Linear Algebra

Peter Petersen

Department of Mathematics, UCLA, Los Angeles CA, 90095
E-mail address: petersen@math.ucla.edu

2000 *Mathematics Subject Classification.* Primary ; Secondary

Contents

Preface

This book covers the aspects of linear algebra that are included in most advanced undergraduate texts. All the usual topics from complex vectors spaces, complex inner products, The Spectral theorem for normal operators, dual spaces, quotient spaces, the minimal polynomial, the Jordan canonical form, and the rational canonical form are explained. A chapter on determinants has been included as the last chapter, but they are not used in the text as a whole. A different approach to linear algebra that doesn't use determinants can be found in [**Axler**].

The expected prerequisites for this book would be a lower division course in matrix algebra. A good reference is for this material is [**Bretscher**].

In the context of other books on linear algebra it is my feeling that this text is about on par in difficulty with books such as [**Axler**], [**Curtis**], [**Halmos**], [**Hoffman-Kunze**], and [**Lang**]. If you want to consider more challenging texts I'd suggest looking at the graduate levels books [**Greub**], [**Roman**], and [**Serre**].

Chapter 1 contains all of the basic material on abstract vectors spaces and linear maps. The dimension formula for linear maps is the theoretical highlight. To facilitate some more concrete developments we cover matrix representations, change of basis, and Gauss elimination. Linear indepence which is usually introduced much earlier in linear algebra only comes towards to end of the chapter. But it is covered in great detail there. We have also included two sections on dual spaces and quotient spaces that can be skipped.

Chapter 2 is concerned with the theory of linear operators. Linear differential equations are used to motivate the introduction of eigenvalues and eigenvectors, but this motivation can be skipped. We then explain how Gauss elimination can be used to compute the eigenvalues as well as the eigenvectors of a matrix. This is used to understand the basics of how and when a linear operator on a finite dimensional space is diagonalizable. We also introduce the minimal polynomial and use it to give the classic characterization of diagonalizable operators. In the latter sections we give a fairly simple proof of the Cayley-Hamilton theorem and the cyclic subspace decomposition. This quickly leads to the Frobenius canonical from. This canonical from is our most general result on how to find a simple matrix representation for a linear map in case it isn't diagonalizable. The last section explains how the Frobenius canonical form implies the Jordan-Chevalley decomposition and the Jordan-Weierstrass canonical form.

Chapter 3 includes material on inner product spaces. The Cauchy-Schwarz inequality and its generalization to Bessel's inequality and how they tie in with orthogonal projections form the theoretical center piece of this chapter. Along the way we cover standard facts about orthonormal bases and their existence through the Gram-Schmidt procedure as well as orthogonal complements and orthogonal projections. The chapter also contains the basic elements of adjoints of linear maps and some of its uses to orthogonal projects as this ties in nicely with orthonormal bases. We end the chapter with a treatment of matrix exponentials and systems of differential equations.

Chapter 4 covers quite a bit of ground on the theory of linear maps between inner product spaces. The most important result is of course The Spectral Theorem for self-adjoint operators. This theorem is used to establish the canonical forms for real and complex normal operators, which then gives the canonical form for unitary, orthogonal and skew-adjoint operators. It should be pointed out that the proof of the Spectral theoem does not depend on whether we use real or complex scalars nor does it rely on the characteristic or minimal polynomials. The reason for ignoring our earlier material on diagonalizability is that it is desirable to have a theory that more easily generalizes to infinite dimensions. The usual proofs that use the characteristic and minimal polynomials are relegated to the exercises. The last sections of the chapter cover the singular value decomposition, the polar decomposition, triangulability of complex linear operators, and quadratic forms and their uses in multivariable calculus.

Chapter 5 covers determinants. At this point it might seem almost useless to introduce the determinant as we have covered the theory without needing it much. While not indispensable, the determinant is rather useful in giving a clean definition for the characteristic polynomial. It is also one of the most important invariants of a finite dimensional operator. It has several nice properties and gives an excellent criterion for when an operator is invertible. It also comes in handy in giving a formula (Cramer's rule) for solutions to linear systems. Finally we discuss its uses in the theory of linear differential equations, in particular in connection with the variation of constants formula for the solution to inhomogeneous equations. We have taken the liberty of defining the determinant of a linear operator through the use of volume forms. Aside from showing that volume forms exist this gives a rather nice way of proving all the properties of determinants without using permutations. It also has the added benefit of automatically giving the permutation formula for the determinant and hence showing that the sign of a permutation is well-defined.

An * after a section heading means that the section is not necessary for the understanding of other sections without an *. We refer to sections in the text by writing out the title in citation marks, e.g., "Dimension and Isomorphism" and if needed we also mention the chapter where the section is located.

Now for how to teach a course using this book. My assumption is that most courses are based on 150 minutes of instruction per week with a problem session or two added . I realize that some courses meet three times while others only two so I won't suggest how much can be covered in a lecture.

First let us suppose that you, like me, teach in the pedagogically impoverished quarter system: It should be possible to teach Chapter 1, sections 2-13 in 5 weeks, being a bit careful about what exactly is covered in sections 12 and 13. Then spend two weeks on Chapter 2, sections 3-5, possibly omitting section 4 covering the minimal polynomial if timing looks tight. Next spend two weeks on Chapter 3 sections 1-5, and finish the course by covering Chapter 4, section 1 as well as exercise 9 in 4.1. This finishes the course with a proof of the Spectral Theorem for self-adjoint operators, although not the proof I'd recommend for a more serious treatment.

Next let us suppose that you teach in a short semester system, as the ones at various private colleges and universities. You could then add two weeks of material by either covering the canonical forms from Chapter 2, sections 6-8 or alternately spend two weeks covering some of the theory of linear operators on inner product spaces from Chapter 4, sections 1-5. In case you have 15 weeks at you disposal it might be possible to cover both of these topics rather than choosing between them.

Finally, should you have two quarters, like we sometimes do here at UCLA, then you can in all likelihood cover virtually the entire text. I'd certainly recommend that you cover all of Chapter 4 and the canonical form sections in Chapter 2, sections 6-8, as well as the chapter on determinants. If time permits it might even be possible to include the sections that cover differential equations: 2.2, 3.7, last part of 4.8, and 5.8.

This book has been used to teach a bridge course on Linear Algebra at UCLA as well as a regular quarter length course. The bridge course was funded by a VIGRE NSF-grant and its purpose was to ensure that incoming graduate students had really learned all of the linear algebra that we expect them to know when starting graduate school. The author would like to thank several UCLA students for suggesting various improvements to the text: Jeremy Brandman, Sam Chamberlain, Timothy Eller, Clark Grubb, Vanessa Idiarte, Yanina Landa, Bryant Mathews, Shervin Mosadeghi, and Danielle O'Donnol.

CHAPTER 1

Basic Theory

In the first chapter we are going to cover the definitions of vector spaces, linear maps, and subspaces. In addition we are introducing several important concepts such as basis, dimension, direct sum, matrix representations of linear maps, and kernel and image for linear maps. We shall prove the dimension theorem for linear maps that relates the dimension of the domain to the dimensions of kernel and image. We give an account of Gauss elimination and how it ties in with the more abstract theory. This will be used to define and compute the characteristic polynomial in chapter 2.

It is important to note that the sections "Row Reduction" and "Linear Independence" contain alternate proofs of some of the important results in this chapter. As such, some people might want to go right to these sections after the discussion on isomorphism in "Dimension and Isomorphism" and then look back at the missed sections.

As induction is going to play a big role in many of the proofs we have chosen to say a few things about that topic in the first section.

1. Induction and Well-ordering*

A fundamental property of the *natural numbers*, i.e., the positive integers $\mathbb{N} = \{1, 2, 3, ...\}$, that will be used throughout the book is the fact that they are *well-ordered*. This means that any non-empty subset $S \subset \mathbb{N}$ has a smallest element $s_{\min} \in S$ such that $s_{\min} \leq s$ for all $s \in S$. Using the natural ordering of the integers, rational numbers, or real numbers we see that this property does not hold for those numbers. For example, the half-open interval $(0, \infty)$ does not have a smallest element.

In order to justify that the positive integers are well-ordered let $S \subset \mathbb{N}$ be non-empty and select $k \in S$. Starting with 1 we can check whether it belongs to S. If it does, then $s_{\min} = 1$. Otherwise check whether 2 belongs to S. If $2 \in S$ and $1 \notin S$, then we have $s_{\min} = 2$. Otherwise we proceed to check whether 3 belongs to S. Continuing in this manner we must eventually find $k_0 \leq k$, such that $k_0 \in S$, but 1, 2, 3, ..., $k_0 - 1 \notin S$. This is the desired minimum: $s_{\min} = k_0$.

We shall use the well-ordering of the natural numbers in several places in this text. A very interesting application is to the proof of The Prime Factorization Theorem: Any integer ≥ 2 is a product of prime numbers. The proof works the following way. Let $S \subset \mathbb{N}$ be the set of numbers which do not admit a prime factorization. If S is empty we are finished, otherwise S contains a smallest element $n = s_{\min} \in S$. If n has no divisors, then it is a prime number and hence has a prime factorization. Thus n must have a divisor $p > 1$. Now write $n = p \cdot q$. Since $p, q < n$ both numbers must have a prime factorization. But then also $n = p \cdot q$ has a prime factorization. This contradicts that S is nonempty.

The second important idea that is tied to the natural numbers is that of *induction*. Sometimes it is also called *mathematical induction* so as not to confuse it with the inductive method from science. The types of results that one can attempt to prove with induction always have a statement that needs to be verified for each number $n \in \mathbb{N}$. Some good examples are

(1) $1+2+3+\cdots+n=\frac{n(n+1)}{2}$.
(2) Every integer ≥ 2 has a prime factorization.
(3) Every polynomial has a root.

The first statement is pretty straight forward to understand. The second is a bit more complicated and we also note that in fact there is only a statement for each integer ≥ 2. This could be finessed by saying that each integer $n+1$, $n \geq 1$ has a prime factorization. This, however, seems too pedantic and also introduces extra and irrelevant baggage by using addition. The third statement is obviously quite different from the other two. For one thing it only stands a chance of being true if we also assume that the polynomials have degree ≥ 1. This gives us the idea of how this can be tied to the positive integers. The statement can be paraphrased as: Every polynomial of degree ≥ 1 has a root. Even then we need to be more precise as x^2+1 does not have any real roots.

In order to explain how induction works abstractly suppose that we have a statement $P(n)$ for each $n \in \mathbb{N}$. Each of the above statements can be used as an example of what $P(n)$ can be. The induction process now works by first insuring that the anchor statement is valid. In other words, we first check that $P(1)$ is true. We then have to establish the *induction step*. This means that we need to show: If $P(n-1)$ is true, then $P(n)$ is also true. The assumption that $P(n-1)$ is true is called the *induction hypothesis*. If we can establish the validity of these two facts then $P(n)$ must be true for all n. This follows from the well-ordering of the natural numbers. Namely, let $S=\{n : P(n) \text{ is false}\}$. If S is empty we are finished, otherwise S has a smallest element $k \in S$. Since $1 \notin S$ we know that $k>1$. But this means that we know that $P(k-1)$ is true. The induction step then implies that $P(k)$ is true as well. This contradicts that S is non-empty.

Let us see if can use this procedure on the above statements. For 1. we begin by checking that $1=\frac{1(1+1)}{2}$. This is indeed true. Next we assume that

$$1+2+3+\cdots+(n-1)=\frac{(n-1)n}{2}$$

and we wish to show that

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}.$$

Using the induction hypothesis we see that

$$\begin{aligned}(1+2+3+\cdots+(n-1))+n &= \frac{(n-1)n}{2}+n \\ &= \frac{(n-1)n+2n}{2} \\ &= \frac{(n+1)n}{2}.\end{aligned}$$

Thus we have shown that $P(n)$ is true provided $P(n-1)$ is true.

For 2. we note that 2 is a prime number and hence has a prime factorization. Next we have to prove that n has a prime factorization if $(n-1)$ does. This, however, does not look like a very promising thing to show. In fact we need a stronger form of induction to get this to work.

The induction step in the stronger version of induction is: If $P(k)$ is true for all $k < n$, then $P(n)$ is also true. Thus the induction hypothesis is much stronger as we assume that all statements prior to $P(n)$ are true. The proof that this form of induction works is virtually identical to the above justification.

Let us see how this stronger version can be used to establish the induction step for 2. Let $n \in \mathbb{N}$, and assume that all integers below n have a prime factorization. If n has no divisors other than 1 and n it must be a prime number and we are finished. Otherwise $n = p \cdot q$ where $p, q < n$. Whence both p and q have prime factorizations by our induction hypothesis. This shows that also n has a prime factorization.

We already know that there is trouble with statement 3. Nevertheless it is interesting to see how an induction proof might break down. First we note that all polynomials of degree 1 look like $ax + b$ and hence have $-\frac{b}{a}$ as a root. This anchors the induction. To show that all polynomials of degree n have a root we need to first decide which of the two induction hypotheses are needed. There really isn't anything wrong by simply assuming that all polynomials of degree $< n$ have a root. In this way we see that at least any polynomial of degree n that is the product of two polynomials of degree $< n$ must have a root. This leaves us with the so-called prime or irreducible polynomials of degree n, namely, those polynomials that are not divisible by polynomials of degree ≥ 1 and $< n$. Unfortunately there isn't much we can say about these polynomials. So induction doesn't seem to work well in this case. All is not lost however. A careful inspection of the "proof" of 3. can be modified to show that any polynomial has a prime factorization. This is studied further in the section "Polynomials" in chapter 2.

The type of statement and induction argument that we will encounter most often in this text is definitely of the third type. That is to say, it certainly will never be of the very basic type seen in statement 1. Nor will it be as easy as in statement 2. In our cases it will be necessary to first find the integer that is used for the induction and even then there will be a whole collection of statements associated with that integer. This is what is happening in the 3rd statement. There we first need to select the degree as our induction integer. Next there are still infinitely many polynomials to consider when the degree is fixed. Finally whether or not induction will work or is the "best" way of approaching the problem might actually be questionable.

The following statement is fairly typical of what we shall see: Every subspace of $\mathbb{R}^n$ admits a basis with $\leq n$ elements. The induction integer is the dimension n and for each such integer there are infinitely many subspaces to be checked. In this case an induction proof will work, but it is also possible to prove the result without using induction.

2. Elementary Linear Algebra

Our first picture of what vectors are and what we can do with them comes from viewing them as geometric objects in the plane. Simply put, a vector is an arrow of some given length drawn in the plane. Such an arrow is also known as an oriented line segment. We agree that vectors that have the same length and orientation are equivalent no matter where they are based. Therefore, if we base them at the origin, then vectors are determined by their endpoints. Using a parallelogram we can add such vectors. We can also multiply them by scalars. If the scalar is negative we are changing the orientation. The size of the scalar determines how much we are scaling the vector, i.e., how much we are changing its length.

This geometric picture can also be taken to higher dimensions. The idea of scaling a vector doesn't change if it lies in space, nor does the idea of how to add vectors, as two vectors must lie either on a line or more generically in a plane. The problem comes when we wish to investigate these algebraic properties further. As an example think about the associative law

$$(x + y) + z = x + (y + z).$$

Clearly the proof of this identity changes geometrically from the plane to space. In fact, if the three vectors do not lie in a plane and therefore span a parallelepiped then the sum of these three vectors regardless of the order in which they are added is the diagonal of this parallelepiped. The picture of what happens when the vectors lie in a plane is simply a projection of the three dimensional picture on to the plane.

The purpose of linear algebra is to clarify these algebraic issues by looking at vectors in a less geometric fashion. This has the added benefit of also allowing other spaces that do not have geometric origins to be included in our discussion. The end result is a somewhat more abstract and less geometric theory, but it has turned out to be truly useful and foundational in almost all areas of mathematics, including geometry, not to mention the physical, natural and social sciences.

Something quite different and interesting happens when we allow for complex scalars. This is seen in the plane itself which we can interpret as the set of complex numbers. Vectors still have the same geometric meaning but we can also "scale" them by a number like $i = \sqrt{-1}$. The geometric picture of what happens when multiplying by i is that the vector's length is unchanged as $|i| = 1$, but it is rotated 90°. Thus it isn't scaled in the usual sense of the word. However, when we define these notions below one will not really see any algebraic difference in what is happening. It is worth pointing out that using complex scalars is not just something one does for the fun of it, it has turned out to be quite convenient and important to allow for this extra level of abstraction. This is true not just within mathematics itself as can be seen when looking at books on quantum mechanics. There complex vector spaces are the "sine qua non" (without which nothing) of the subject.

3. Fields

The "scalars" or numbers used in linear algebra all lie in a *field*. A field is simply a collection of numbers where one has both addition and multiplication. Both operations are associative, commutative etc. We shall mainly be concerned with $\mathbb{R}$ and $\mathbb{C}$, some examples using $\mathbb{Q}$ might be used as well. These three fields satisfy the axioms we list below.

A *field* $\mathbb{F}$ is a set whose elements are called numbers or when used in linear algebra *scalars*. The field contains two different elements 0 and 1 and we can add and multiply numbers. These operations satisfy

(1) The Associative Law:
$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma.$$
(2) The Commutative Law:
$$\alpha + \beta = \beta + \alpha.$$
(3) Addition by 0:
$$\alpha + 0 = \alpha.$$
(4) Existence of Negative Numbers: For each α we can find $-\alpha$ so that
$$\alpha + (-\alpha) = 0.$$
(5) The Associative Law:
$$\alpha(\beta\gamma) = (\alpha\beta)\gamma.$$
(6) The Commutative Law:
$$\alpha\beta = \beta\alpha.$$
(7) Multiplication by 1:
$$\alpha 1 = \alpha.$$
(8) Existence of Inverses: For each $\alpha \neq 0$ we can find α^{-1} so that
$$\alpha\alpha^{-1} = 1.$$

(9) The Distributive Law:

$$\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma.$$

Occasionally we shall also use that the field has *characteristic zero*, this means that

$$n=\overbrace{1+\cdots+1}^{n\text{ times}}\neq 0$$

for all positive integers n. Fields such as $\mathbb{F}_2=\{0,1\}$ where $1+1=0$ clearly do not have characteristic zero. We make the assumption throughout the text that all fields have characteristic zero. In fact, there is little loss of generality in assuming that the fields we work are the usual number fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

There are several important collections of numbers that are not fields:

$$\begin{aligned}\mathbb{N} &= \{1,2,3,....\}\\ &\subset \mathbb{N}_0=\{0,1,2,3,...\}\\ &\subset \mathbb{Z}=\{0,\pm1,\pm2,\pm3,...\}\\ &= \{0,1,-1,2,-2,3,-3,...\}.\end{aligned}$$

4. Vector Spaces

A *vector space* consists of a set of vectors V and a field $\mathbb{F}$. The vectors can be added to yield another vector: if $x,y\in V$, then $x+y\in V$. The scalars can be multiplied with the vectors to yield a new vector: if $\alpha\in\mathbb{F}$ and $x\in V$, then $\alpha x=x\alpha\in V$. The vector space contains a *zero vector* 0, also known as the *origin* of V. It is a bit confusing that we use the same symbol for $0\in V$ and $0\in\mathbb{F}$. It should ways be obvious from the context which zero is used. We shall use the notation that scalars, i.e., elements of $\mathbb{F}$ are denoted by small Greek letters such as $\alpha,\beta,\gamma,...$, while vectors are denoted by small roman letters such as $x,y,z,...$. Addition and scalar multiplication must satisfy the following axioms.

(1) The Associative Law:

$$(x+y)+z=x+(y+z).$$

(2) The Commutative Law:

$$x+y=y+x.$$

(3) Addition by 0:

$$x+0=x.$$

(4) Existence of Negative vectors: For each x we can find $-x$ such that

$$x+(-x)=0.$$

(5) The Associative Law for multiplication by scalars:

$$\alpha(\beta x)=(\alpha\beta)x.$$

(6) The Commutative Law for multiplying by scalars:

$$\alpha x=x\alpha.$$

(7) Multiplication by the unit scalar:

$$1x=x.$$

(8) The Distributive Law when vectors are added:

$$\alpha(x+y)=\alpha x+\alpha y.$$

(9) The Distributive Law when scalars are added:

$$(\alpha+\beta)x=\alpha x+\beta x.$$

The only rule that one might not find elsewhere is $\alpha x = x\alpha$. In fact we could just declare that one is only allowed to multiply by scalars on the left. This, however, is an inconvenient restriction and certainly one that doesn't make sense for many of the concrete vector spaces we will work with. We shall also often write $x-y$ instead of $x+(-y)$.

These axioms lead to several "obvious" facts.

Proposition 1. (1) $0x=0$.
(2) $\alpha 0=0$.
(3) $-1x=-x$.
(4) *If* $\alpha x=0$, *then either* $\alpha=0$ *or* $x=0$.

Proof. By the distributive law

$$0x+0x=(0+0)x=0x.$$

This together with the assocoative law gives us

$$\begin{aligned} 0x &= 0x+(0x-0x) \\ &= (0x+0x)-0x \\ &= 0x-0x \\ &= 0. \end{aligned}$$

The second identity is proved in the same manner.

For the third consider:

$$\begin{aligned} 0 &= 0x \\ &= (1-1)x \\ &= 1x+(-1)x \\ &= x+(-1)x, \end{aligned}$$

adding $-x$ on both sides then yields

$$-x=(-1)x.$$

Finally if $\alpha x=0$ and $\alpha\neq 0$, then we have

$$\begin{aligned} x &= \left(\alpha^{-1}\alpha\right)x \\ &= \alpha^{-1}(\alpha x) \\ &= \alpha^{-1}0 \\ &= 0. \end{aligned}$$

□

With these matters behind us we can relax a bit and start adding, subtracting, and multiplying along the lines we are used to from matrix algebra. Our first construction is to form *linear combinations* of vectors. If $\alpha_1,\dots,\alpha_m\in\mathbb{F}$ and

$x_1, ..., x_m \in V$, then we can multiply each x_i by the scalar α_i and then add up the resulting vectors to form the linear combination

$$x = \alpha_1 x_1 + \cdots + \alpha_m x_m.$$

We also say that x is a linear combination of the x_is.

If we arrange the vectors in a $1 \times m$ row matrix

$$\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix}$$

and the scalars in a column $m \times 1$ matrix we see that the linear combination can be thought of as a matrix product

$$\sum_{i=1}^{m} \alpha_i x_i = \alpha_1 x_1 + \cdots + \alpha_m x_m = \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}.$$

To be completely rigorous we should write the linear combination as a 1×1 matrix $[\alpha_1 x_1 + \cdots + \alpha_m x_m]$ but it seems too pedantic to insist on this. Another curiosity here is that matrix multiplication almost forces us to write

$$x_1 \alpha_1 + \cdots + x_m \alpha_m = \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}.$$

This is one reason why we want to be able to multiply by scalars on both the left and right.

Here are some important examples of vectors spaces.

Example 1. *The most important basic example is undoubtedly the Cartesian n-fold product of the field $\mathbb{F}$.*

$$\begin{aligned} \mathbb{F}^n &= \left\{ \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} : \alpha_1, \ldots, \alpha_n \in \mathbb{F} \right\} \\ &= \{(\alpha_1, \ldots, \alpha_n) : \alpha_1, \ldots, \alpha_n \in \mathbb{F}\}. \end{aligned}$$

Note that the $n \times 1$ and the n-tuple ways of writing these vectors are equivalent. When writing vectors in a line of text the n-tuple version is obviously more convenient. The column matrix version, however, conforms to various other natural choices, as we shall see, and carries some extra meaning for that reason. The i^{th} entry α_i in the vector $x = (\alpha_1, \ldots, \alpha_n)$ is called the i^{th} *coordinate* of x.

Example 2. *The* space of functions *whose domain is some fixed set S and whose values all lie in the field $\mathbb{F}$ is denoted by* $\operatorname{Func}(S, \mathbb{F}) = \{f : S \to \mathbb{F}\}$.

In the special case where $S = \{1, \ldots, n\}$ it is worthwhile noting that

$$\operatorname{Func}(\{1, \ldots, n\}, \mathbb{F}) = \mathbb{F}^n.$$

Thus vectors in $\mathbb{F}^n$ can also be thought of as functions and can be graphed as either an arrow in space or as a histogram type function. The former is of course more geometric, but the latter certainly also has its advantages as collections of numbers in the form of $n \times 1$ matrices don't always look like vectors. In statistics the histogram picture is obviously far more useful. The point here is that the way in which vectors are pictured might be psychologically important, but from an abstract mathematical perspective there is no difference.

There is a slightly more abstract vector space that we can construct out of a general set S *and a vector space* V*. This is the set* $\mathrm{Map}(S,V)$ *of all maps from* S *to* V*. Scalar multiplication and addition are defined as follows*

$$\begin{aligned}(\alpha f)(x) &= \alpha f(x), \\ (f_1+f_2)(x) &= f_1(x)+f_2(x).\end{aligned}$$

The space of functions is in some sense the most general type of vector space as all other vectors spaces are either of this type or *subspaces* of such function spaces. A subspace $M \subset V$ of a vector space is a subset that contains the origin and is closed under both scalar multiplication and vector addition: if $\alpha \in \mathbb{F}$ and $x, y \in M$, then

$$\begin{aligned}\alpha x &\in M, \\ x+y &\in M.\end{aligned}$$

Clearly subspaces of vector spaces are also vector spaces in their own right.

Example 3. *The space of* $n \times m$ *matrices*

$$\begin{aligned}\mathrm{Mat}_{n\times m}(\mathbb{F}) &= \left\{ \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{bmatrix} : \alpha_{ij} \in \mathbb{F} \right\} \\ &= \{(\alpha_{ij}) : \alpha_{ij} \in \mathbb{F}\}.\end{aligned}$$

$n \times m$ *matrices are evidently just a different way of arranging vectors in* $\mathbb{F}^{n\cdot m}$*. This arrangement, as with the column version of vectors in* $\mathbb{F}^n$*, imbues these vectors with some extra meaning that will become evident as we proceed.*

Example 4. *The set of* polynomials *whose coefficients lie in the field* $\mathbb{F}$

$$\mathbb{F}[t] = \left\{ p(t) = a_0 + a_1 t + \cdots + a_k t^k : k \in \mathbb{N}_0, a_0, a_1, ..., a_k \in \mathbb{F} \right\}$$

is also a vector space. If we think of polynomials as functions, then we imagine them as a subspace of $\mathrm{Func}\{\mathbb{F},\mathbb{F}\}$ *. However the fact that a polynomial is determined by its representation as a function depends on the fact that we have a field of characteristic zero! If, for instance,* $\mathbb{F} = \{0,1\}$ *, then the polynomial* t^2+t *vanishes when evaluated at both* 0 *and* 1*. Thus this nontrivial polynomial is, when viewed as a function, the same as* $p(t) = 0$*.*

We could also just record the coefficients. In that case $\mathbb{F}[t]$ *is a subspace of* $\mathrm{Func}(\mathbb{N}_0,\mathbb{F})$ *and consists of those infinite tuples that are zero except at all but a finite number of places.*

If

$$p(t) = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{F}[t],$$

then the largest integer $k \leq n$ *such that* $a_k \neq 0$ *is called the degree of* p*. In other words*

$$p(t) = a_0 + a_1 t + \cdots + a_k t^k$$

and $a_k \neq 0$*. We use the notation* $\deg(p) = k$*.*

Example 5. *The collection of formal power series*

$$\begin{aligned}\mathbb{F}[[t]] &= \left\{ a_0 + a_1 t + \cdots + a_k t^k + \cdots : a_0, a_1, ..., a_k, ... \in \mathbb{F} \right\} \\ &= \left\{ \sum_{i=0}^{\infty} a_i t^i : a_i \in \mathbb{F}, i \in \mathbb{N}_0 \right\}\end{aligned}$$

bears some resemblance to polynomials, but without further discussions on convergence or even whether this makes sense we cannot interpret power series as lying in $\text{Func}(\mathbb{F},\mathbb{F})$. *If, however, we only think about recording the coefficients, then we see that* $\mathbb{F}[[t]] = \text{Func}(\mathbb{N}_0,\mathbb{F})$. *The extra piece of information that both* $\mathbb{F}[t]$ *and* $\mathbb{F}[[t]]$ *carry with them, aside from being vector spaces, is that the elements can also be multiplied. This extra structure will be used in the case of* $\mathbb{F}[t]$. *Powerseries will not play an important role in the sequel. Finally note that* $\mathbb{F}[t]$ *is a subspace of* $\mathbb{F}[[t]]$.

Example 6. *For two (or more) vector spaces* V, W *we can form the (Cartesian) product*

$$V \times W = \{(v,w) : v \in V \text{ and } w \in W\}.$$

Scalar multiplication and addition is defined by

$$\begin{aligned} \alpha(v,w) &= (\alpha v, \alpha w), \\ (v_1,w_1)+(v_2,w_2) &= (v_1+v_2, w_1+w_2). \end{aligned}$$

Note that $V \times W$ *is not in a natural way a subspace in a space of functions or maps.*

4.1. Exercises.

(1) Find a subset $C \subset \mathbb{F}^2$ that is closed under scalar multiplication but not under addition of vectors.
(2) Find a subset $A \subset \mathbb{C}^2$ that is closed under vector addition but not under multiplication by complex numbers.
(3) Find a subset $Q \subset \mathbb{R}$ that is closed under addition but not scalar multiplication.
(4) Let $V = \mathbb{Z}$ be the set of integers with the usual addition as "vector addition". Show that it is not possible to define scalar multiplication by $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ so as to make it into a vector space.
(5) Let V be a real vector space, i.e., a vector space were the scalars are $\mathbb{R}$. The *complexification* of V is defined as $V_{\mathbb{C}} = V \times V$. As in the construction of complex numbers we agree to write $(v,w) \in V_{\mathbb{C}}$ as $v+iw$. Define complex scalar multiplication on $V_{\mathbb{C}}$ and show that it becomes a complex vector space.
(6) Let V be a complex vector space i.e., a vector space were the scalars are $\mathbb{C}$. Define V^* as the complex vector space whose additive structure is that of V but where complex scalar multiplication is given by $\lambda * x = \bar{\lambda}x$. Show that V^* is a complex vector space.
(7) Let P_n be the space of polynomials in $\mathbb{F}[t]$ of degree $\leq n$.
    (a) Show that P_n is a vector space.
    (b) Show that the space of polynomials of degree n is $P_n - P_{n-1}$ and does not form a subspace.
    (c) If $f(t) : \mathbb{F} \to \mathbb{F}$, show that $V = \{p(t) f(t) : p \in P_n\}$ is a subspace of $\text{Func}\{\mathbb{F},\mathbb{F}\}$.
(8) Let $V = \mathbb{C}^{\times} = \mathbb{C} - \{0\}$. Define addition on V by $x \boxplus y = xy$. Define scalar multiplication by $\alpha \boxdot x = e^{\alpha} x$
    (a) Show that if we use $0_V = 1$ and $-x = x^{-1}$, then the first four axioms for a vector space are satisfied.
    (b) Which of the scalar multiplication properties do not hold?

5. Bases

We are now going to introduce one of the most important concepts in linear algebra. Let V be a vector space over $\mathbb{F}$. A *finite basis* for V is a finite collection of vectors $x_1, ..., x_n \in V$ such that each element $x \in V$ can be written as a linear combination

$$x = \alpha_1 x_1 + \cdots + \alpha_n x_n$$

in precisely one way. This means that for each $x \in V$ we can find $\alpha_1, ..., \alpha_n \in \mathbb{F}$ such that

$$x = \alpha_1 x_1 + \cdots + \alpha_n x_n.$$

Moreover, if we have two linear combinations both yielding x

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = x = \beta_1 x_1 + \cdots + \beta_n x_n,$$

then

$$\alpha_1 = \beta_1, ..., \alpha_n = \beta_n.$$

Since each x has a unique linear combination we also refer to it as the *expansion* of x with respect to the basis. In this way we get a well-defined correspondence $V \longleftrightarrow \mathbb{F}^n$ by identifying

$$x = \alpha_1 x_1 + \cdots + \alpha_n x_n$$

with the n-tuple $(\alpha_1, ..., \alpha_n)$. We note that this correspondence preserves scalar multiplication and vector addition since

$$\begin{aligned} \alpha x &= \alpha(\alpha_1 x_1 + \cdots + \alpha_n x_n) \\ &= (\alpha\alpha_1) x_1 + \cdots + (\alpha\alpha_n) x_n, \\ x + y &= (\alpha_1 x_1 + \cdots + \alpha_n x_n) + (\beta_1 x_1 + \cdots + \beta_n x_n) \\ &= (\alpha_1 + \beta_1) x_1 + \cdots + (\alpha_n + \beta_n) x_n. \end{aligned}$$

This means that the choice of basis makes V equivalent to the more concrete vector space $\mathbb{F}^n$. This idea of making abstract vector spaces more concrete by the use of a basis is developed further in "Linear maps as Matrices" and "Dimension and Isomorphism".

We shall later prove that the number of vectors in such a basis for V is always the same. This allows us to define the *dimension* of V over $\mathbb{F}$ to be the number of elements in a basis. Note that the uniqueness condition for the linear combinations guarantees that none of the vectors in a basis can be the zero vector.

Let us consider some basic examples.

Example 7. *In $\mathbb{F}^n$ define the vectors*

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, e_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, ..., e_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

Thus e_i is the vector that is zero in every entry except the i^{th} where it is 1. These vectors evidently form a basis for $\mathbb{F}^n$ since any vector in $\mathbb{F}^n$ has the unique expansion

$$\begin{aligned}\mathbb{F}^n \ni x &= \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} \\ &= \alpha_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \alpha_n \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \\ &= \alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n \\ &= \begin{bmatrix} e_1 & e_2 & \cdots & e_n \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}.\end{aligned}$$

Example 8. *In $\mathbb{F}^2$ consider*

$$x_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, x_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

These two vectors also form a basis for $\mathbb{F}^2$ since we can write

$$\begin{aligned}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} &= (\alpha - \beta) \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} (\alpha - \beta) \\ \beta \end{bmatrix}\end{aligned}$$

To see that these choices are unique observe that the coefficient on x_2 must be β and this then uniquely determines the coefficient in front of x_1.

Example 9. *In $\mathbb{F}^2$ consider the slightly more complicated set of vectors*

$$x_1 = \begin{bmatrix} 1 \\ -1 \end{bmatrix}, x_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

This time we see

$$\begin{aligned}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} &= \frac{\alpha - \beta}{2} \begin{bmatrix} 1 \\ -1 \end{bmatrix} + \frac{\alpha + \beta}{2} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} \frac{\alpha - \beta}{2} \\ \frac{\alpha + \beta}{2} \end{bmatrix}.\end{aligned}$$

Again we can see that the coefficients are unique by observing that the system

$$\begin{aligned}\gamma + \delta &= \alpha, \\ -\gamma + \delta &= \beta\end{aligned}$$

has a unique solution. This is because γ, respectively δ, can be found by subtracting, respectively adding, these two equations.

Example 10. *Likewise the space of matrices $\mathrm{Mat}_{n\times m}(\mathbb{F})$ has a natural basis E_{ij} of nm elements, where E_{ij} is the matrix that is zero in every entry except the $(i,j)^{\text{th}}$ where it is 1.*

If $V = \{0\}$, then we say that V has dimension 0. Another slightly more interesting case that we can cover now is that of one dimensional spaces.

LEMMA 1. *Let V be a vector space over $\mathbb{F}$. If V has a basis with one element, then any other finite basis also has one element.*

PROOF. Let x_1 be a basis for V. If $x \in V$, then $x = \alpha x_1$ for some α. Now suppose that we have $z_1, ..., z_n \in V$, then $z_i = \alpha_i x_1$. If $z_1, ..., z_n$ forms a basis, then none of the vectors are zero and consequently $\alpha_i \neq 0$. Thus for each i we have $x_1 = \alpha_i^{-1} z_i$. Therefore, if $n > 1$, then we have that x_1 can be written in more than one way as a linear combination of $z_1, ..., z_n$. This contradicts the definition of a basis. Whence $n = 1$ as desired. □

The concept of a basis depends quite a lot on the scalars we use. The field of complex numbers $\mathbb{C}$ is clearly a one dimensional vector space when we use $\mathbb{C}$ as the scalar field. To be specific we have that $x_1 = 1$ is a basis for $\mathbb{C}$. If, however, we view $\mathbb{C}$ as a vector space over the reals $\mathbb{R}$, then only real numbers in $\mathbb{C}$ are linear combinations of x_1. Therefore x_1 is no longer a basis when we restrict to real scalars.

It is also possible to have infinite bases. However, some care must be taken in defining this concept as we are not allowed to form infinite linear combinations. We say that a vector space V over $\mathbb{F}$ has a collection $x_i \in V$, where $i \in A$ is some possibly infinite index set, as a basis, if each $x \in V$ is a linear combination of a finite number of the vectors x_i is a unique way. There is, surprisingly, only one important vector space that comes endowed with a natural infinite basis. This is the space $\mathbb{F}[t]$ of polynomials. The collection $x_i = t^i$, $i = 0, 1, 2, ...$ evidently gives us a basis. The other spaces $\mathbb{F}[[t]]$ and $\text{Func}(S, \mathbb{F})$, where S is infinite, do not come with any natural bases. There is a rather subtle theorem which asserts that every vector space must have a basis. It is somewhat beyond the scope of this text to prove this theorem as it depends on *Zorn's lemma* or equivalently the *axiom of choice*. It should also be mentioned that it is a mere existence theorem as it does not give a procedure for constructing infinite bases. In order to get around these nasty points we resort to the trick of saying that a vector space is *infinite dimensional* if it does not admit a finite basis. Note that in the above Lemma we can also show that if V admits a basis with one element then it can't have an infinite basis.

Finally we need to mention some subtleties in the definition of a basis. In most texts a distinction is made between an *ordered* basis $x_1, ..., x_n$ and a basis as a *subset*

$$\{x_1, ..., x_n\} \subset V.$$

There is a fine difference between these two concepts. The collection x_1, x_2 where $x_1 = x_2 = x \in V$ can never be a basis as x can be written as a linear combination of x_1 and x_2 in at least two different ways. As a set, however, we see that $\{x\} = \{x_1, x_2\}$ consists of only one vector and therefore this redundancy has disappeared. Throughout this text we assume that bases are ordered. This is entirely reasonable as most people tend to write down a collection of elements of a set in some, perhaps arbitrary, order. It is also important and convenient to work with ordered bases when time comes to discuss matrix representations. On the few occasions where we shall be working with infinite bases, as with $\mathbb{F}[t]$, they will also be ordered in a natural way using either the natural numbers or the integers.

5.1. Exercises.

(1) Show that $1, t, ..., t^n$ form a basis for P_n.

(2) Show that if $p_0, ..., p_n \in P_n$ satisfy $\deg(p_k) = k$, then they form a basis for P_n.

(3) Find a basis $p_1, ..., p_4 \in P_3$ such that $\deg(p_i) = 3$ for $i = 1, 2, 3, 4$.

(4) For $\alpha \in \mathbb{C}$ consider the subset

$$\mathbb{Q}[\alpha] = \{p(\alpha) : p \in \mathbb{Q}[t]\} \subset \mathbb{C}.$$

Show that

(a) If $\alpha \in \mathbb{Q}$ then $\mathbb{Q}[\alpha] = \mathbb{Q}$

(b) If α is *algebraic*, i.e., it solves an equation $p(\alpha) = 0$ for some $p \in \mathbb{Q}[t]$, then $\mathbb{Q}[\alpha]$ is a field that contains $\mathbb{Q}$. Hint: Show that α must be the root of a polynomial with a nonzero constant term. Use this to find a formula for α^{-1} that depends only on positive powers of α.

(c) If α is *algebraic*, then $\mathbb{Q}[\alpha]$ is a finite dimensional vector space over $\mathbb{Q}$ with a basis $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ for some $n \in \mathbb{N}$. Hint: Let n be the smallest number so that α^n is a linear combination of $1, \alpha, \alpha^2, ..., \alpha^{n-1}$. You must explain why we can find such n.

(d) Show that α is algebraic if and only if $\mathbb{Q}[\alpha]$ is finite dimensional over $\mathbb{Q}$.

(e) We say that α is *transcendental* if it is not algebraic. Show that if α is transcendental then $1, \alpha, \alpha^2, ..., \alpha^n, ...$ form an infinite basis for $\mathbb{Q}[\alpha]$. Thus $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[t]$ represent the same vector space via the substitution $t \longleftrightarrow \alpha$.

(5) Show that

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

span $\mathbb{C}^4$, i.e., every vector on $\mathbb{C}^4$ can be written as a linear combination of these vectors. Which collections of those six vectors form a basis for $\mathbb{C}^4$?

(6) Is it possible to find a basis $x_1, ..., x_n$ for $\mathbb{F}^n$ so that the i^{th} entry for all of the vectors $x_1, ..., x_n$ is zero?

(7) If $e_1, ..., e_n$ is the standard basis for $\mathbb{C}^n$, show that both

$$\begin{aligned} &e_1, ..., e_n, ie_1, ..., ie_n, \text{ and} \\ &e_1, ie_1, ..., e_n, ie_n \end{aligned}$$

form bases for $\mathbb{C}^n$ when viewed as a real vector space.

(8) If $x_1, ..., x_n$ is a basis for the real vector space V, then it is also a basis for the complexification $V_{\mathbb{C}}$ (see the exercises to "Vector Spaces" for the definition of $V_{\mathbb{C}}$).

(9) Find a basis for $\mathbb{R}^3$ where all coordinate entries are ± 1.

(10) A subspace $M \subset \mathrm{Mat}_{n\times n}(\mathbb{F})$ is called a *two-sided ideal* if for all $X \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ and $A \in M$ also $XA, AX \in M$. Show that if $M \neq \{0\}$, then $M = \mathrm{Mat}_{n\times n}(\mathbb{F})$. Hint: Find $A \in M$ such some entry is 1. Then show that we can construct the standard basis for $\mathrm{Mat}_{n\times n}(\mathbb{F})$ by multiplying A by the stardard basis matrices for $\mathrm{Mat}_{n\times n}(\mathbb{F})$ on the left and right.

(11) Let V be a vector space.

(a) Show that $x, y \in V$ form a basis if and only if $x+y, x-y$ form a basis.
(b) Show that $x, y, z \in V$ form a basis if and only if $x+y, y+z, z+x$ form a basis.

6. Linear Maps

A map $L : V \to W$ between vector spaces over the same field $\mathbb{F}$ is said to be *linear* if it preserves scalar multiplication and addition in the following way

$$\begin{aligned} L(\alpha x) &= \alpha L(x), \\ L(x+y) &= L(x) + L(y), \end{aligned}$$

where $\alpha \in \mathbb{F}$ and $x, y \in V$. It is possible to collect these two properties into one condition as follows

$$L(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 L(x_1) + \alpha_2 L(x_2),$$

where $\alpha_1, \alpha_2 \in \mathbb{F}$ and $x_1, x_2 \in V$. More generally we have that L preserves linear combinations in the following way

$$\begin{aligned} L\left(\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}\right) &= L(x_1\alpha_1 + \cdots + x_m\alpha_m) \\ &= L(x_1)\alpha_1 + \cdots + L(x_m)\alpha_m \\ &= \begin{bmatrix} L(x_1) & \cdots & L(x_m) \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} \end{aligned}$$

To prove this simple fact we use induction on m. When $m = 1$, this is simply the fact that L preserves scalar multiplication

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

Assuming the induction hypothesis, that the statement holds for $m-1$, we see that

$$\begin{aligned} L(x_1\alpha_1 + \cdots + x_m\alpha_m) &= L((x_1\alpha_1 + \cdots + x_{m-1}\alpha_{m-1}) + x_m\alpha_m) \\ &= L(x_1\alpha_1 + \cdots + x_{m-1}\alpha_{m-1}) + L(x_m\alpha_m) \\ &= (L(x_1)\alpha_1 + \cdots + L(x_{m-1})\alpha_{m-1}) + L(x_m)\alpha_m \\ &= L(x_1)\alpha_1 + \cdots + L(x_m)\alpha_m. \end{aligned}$$

The important feature of linear maps is that they preserve the operations that are allowed on the spaces we work with. Some extra terminology is often used for linear maps. If the values are the field itself, i.e., $W = \mathbb{F}$, then we also call $L : V \to \mathbb{F}$ a *linear function* or *linear functional*. If $V = W$, then we call $L : V \to V$ a *linear operator*.

Before giving examples we introduce some further notation. The set of all linear maps $\{L : V \to W\}$ is often denoted $\hom(V, W)$. In case we need to specify the scalars we add the field as a subscript $\hom_{\mathbb{F}}(V, W)$. The abbreviation hom stands for *homomorphism*. Homomorphisms are in general maps that preserve whatever algebraic structure that is available. Note that

$$\hom_{\mathbb{F}}(V, W) \subset \operatorname{Map}(V, W)$$

and is a subspace of the latter. Thus $\hom_{\mathbb{F}}(V,W)$ is a vector space over $\mathbb{F}$.

It is easy to see that the composition of linear maps always yields a linear map. Thus, if $L_1 : V_1 \to V_2$ and $L_2 : V_2 \to V_3$ are linear maps, then the composition $L_2 \circ L_1 : V_1 \to V_3$ defined by $L_2 \circ L_1(x) = L_2(L_1(x))$ is again a linear map. We often ignore the composition sign $\circ$ and simply write L_2L_1. An important special situation is that one can "multiply" linear operators $L_1, L_2 : V \to V$ via composition. This multiplication is in general not commutative or abelian as it rarely happens that L_1L_2 and L_2L_1 represent the same map. We shall see many examples of this throughout the text.

Example 11. *Define a map $L : \mathbb{F} \to \mathbb{F}$ by scalar multiplication on $\mathbb{F}$ via $L(x) = \lambda x$ for some $\lambda \in \mathbb{F}$. The distributive law says that the map is additive and the associative law together with the commutative law say that it preserves scalar multiplication. This example can now easily be generalized to scalar multiplication on a vector space V, where we can also define $L(x) = \lambda x$.*

Two special cases are of particular interest. First the identity transformation $1_V : V \to V$ defined by $1_V(x) = x$. This is evidently scalar multiplication by 1. Second we have the zero transformation $0 = 0_V : V \to V$ that maps everything to $0 \in V$ and is simply multiplication by 0. The latter map can also be generalized to a zero map $0 : V \to W$ between different vector spaces. With this in mind we can always write multiplication by λ as the map $\lambda 1_V$ thus keeping track of what it does, where it does it, and finally keeping track of the fact that we think of the procedure as a map.

Expanding on this theme a bit we can, starting with a linear operator $L : V \to V$, use powers of L as well as linear combinations to create new operators on V. For instance, $L^2 - 3 \cdot L + 2 \cdot 1_V$ is defined by

$$\left(L^2 - 3 \cdot L + 2 \cdot 1_V\right)(x) = L(L(x)) - 3L(x) + 2x.$$

We shall often do this in quite general situations. The most general construction comes about by selecting a polynomial $p \in \mathbb{F}[t]$ and considering $p(L)$. If $p = \alpha_k t^k + \cdots + \alpha_1 t + \alpha_0$, then

$$p(L) = \alpha_k L^k + \cdots + \alpha_1 L + \alpha_0 1_V.$$

If we think of $t^0 = 1$ as the degree 0 term in the polynomial then by substituing L we apparently define $L^0 = 1_V$. So still the identity, but the identity in the appropriate set where L lives. Evaluation on $x \in V$ is given by

$$p(L)(x) = \alpha_k L^k(x) + \cdots + \alpha_1 L(x) + \alpha_0 x.$$

Apparently p simply defines a linear combination of the linear operators L^k, ..., L, 1_V and $p(L)(x)$ is a linear combination of the vectors $L^k(x)$, ..., $L(x)$, x.

Example 12. *Fix $x \in V$. Note that the axioms of scalar multiplication also imply that $L : \mathbb{F} \to V$ defined by $L(\alpha) = x\alpha$ is linear.*

Example 13. *Matrix multiplication is the next level of abstraction. Here we let $V = \mathbb{F}^m$ and $W = \mathbb{F}^n$ and L is represented by an $n \times m$ matrix*

$$B = \begin{bmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{bmatrix}.$$

The map is defined using matrix multiplication as follows

$$\begin{aligned} L(x) &= Bx \\ &= \begin{bmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{bmatrix} \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_m \end{bmatrix} \\ &= \begin{bmatrix} \beta_{11}\xi_1 + \cdots + \beta_{1m}\xi_m \\ \vdots \\ \beta_{n1}\xi_1 + \cdots + \beta_{nm}\xi_m \end{bmatrix} \end{aligned}$$

Thus the i^{th} *coordinate of* $L(x)$ *is given by*

$$\sum_{j=1}^{m} \beta_{ij}\xi_j = \beta_{i1}\xi_1 + \cdots + \beta_{im}\xi_m.$$

A similar and very important way of representing this map comes by noting that it creates linear combinations. Write B *as a row matrix of its column vectors*

$$B = \begin{bmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{bmatrix} = \begin{bmatrix} b_1 & \cdots & b_m \end{bmatrix}, \text{ where } b_i = \begin{bmatrix} \beta_{1i} \\ \vdots \\ \beta_{ni} \end{bmatrix}$$

and then observe

$$\begin{aligned} L(x) &= Bx \\ &= \begin{bmatrix} b_1 & \cdots & b_m \end{bmatrix} \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_m \end{bmatrix} \\ &= b_1\xi_1 + \cdots + b_m\xi_m. \end{aligned}$$

Note that, if $m = n$ and the matrix we use is a diagonal matrix with λs down the diagonal and zeros elsewhere, then we obtain the scalar multiplication map $\lambda 1_{\mathbb{F}^n}$. The matrix looks like this

$$\begin{bmatrix} \lambda & 0 & \cdots & 0 \\ 0 & \lambda & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda \end{bmatrix}$$

A very important observation in connection with linear maps defined by matrix multiplication is that composition of linear maps $L : \mathbb{F}^l \to \mathbb{F}^m$ and $K : \mathbb{F}^m \to \mathbb{F}^n$ is given by the matrix product. The maps are defined by matrix multiplication

$$\begin{aligned} L(x) &= Bx, \\ B &= \begin{bmatrix} b_1 & \cdots & b_l \end{bmatrix} \end{aligned}$$

and

$$K(y) = Cy.$$

The composition can now be computed as follows using that K is linear

$$\begin{aligned}(K\circ L)(x) &= K(L(x))\\ &= K(Bx)\\ &= K\left(\begin{bmatrix} b_1 & \cdots & b_l\end{bmatrix}\begin{bmatrix}\xi_1\\ \vdots\\ \xi_l\end{bmatrix}\right)\\ &= \begin{bmatrix} K(b_1) & \cdots & K(b_l)\end{bmatrix}\begin{bmatrix}\xi_1\\ \vdots\\ \xi_l\end{bmatrix}\\ &= \left(\begin{bmatrix} Cb_1 & \cdots & Cb_l\end{bmatrix}\right)\begin{bmatrix}\xi_1\\ \vdots\\ \xi_l\end{bmatrix}\\ &= \left(C\begin{bmatrix} b_1 & \cdots & b_l\end{bmatrix}\right)\begin{bmatrix}\xi_1\\ \vdots\\ \xi_l\end{bmatrix}\\ &= (CB)\,x.\end{aligned}$$

Evidently this all hinges on the fact that the matrix product CB can be defined by

$$\begin{aligned}CB &= C\begin{bmatrix} b_1 & \cdots & b_l\end{bmatrix}\\ &= \begin{bmatrix} Cb_1 & \cdots & Cb_l\end{bmatrix},\end{aligned}$$

a definition that is completely natural if we think of C as a linear map. It should also be noted that we did not use associativity of matrix multiplication in the form $C(Bx) = (CB)\,x$. In fact associativity is a consequence of our calculation.

We can also check things a bit more directly using summation notation. Observe that the i^{th} entry in the composition

$$K\left(L\left(\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_l\end{bmatrix}\right)\right) = \begin{bmatrix}\gamma_{11} & \cdots & \gamma_{1m}\\ \vdots & \ddots & \vdots\\ \gamma_{n1} & \cdots & \gamma_{nm}\end{bmatrix}\left(\begin{bmatrix}\beta_{11} & \cdots & \beta_{1l}\\ \vdots & \ddots & \vdots\\ \beta_{m1} & \cdots & \beta_{ml}\end{bmatrix}\begin{bmatrix}\xi_1\\ \vdots\\ \xi_l\end{bmatrix}\right)$$

satisfies

$$\begin{aligned}\sum_{j=1}^{m}\gamma_{ij}\left(\sum_{s=1}^{l}\beta_{js}\xi_s\right) &= \sum_{j=1}^{m}\sum_{s=1}^{l}\gamma_{ij}\beta_{js}\xi_s\\ &= \sum_{s=1}^{l}\sum_{j=1}^{m}\gamma_{ij}\beta_{js}\xi_s\\ &= \sum_{s=1}^{l}\left(\sum_{j=1}^{m}\gamma_{ij}\beta_{js}\right)\xi_s\end{aligned}$$

were $\left(\sum_{j=1}^{m}\gamma_{ij}\beta_{js}\right)$ represents the (i,s) entry in the matrix product $\left[\gamma_{ij}\right]\left[\beta_{js}\right]$.

EXAMPLE 14. *Note that while scalar multiplication on even the simplest vector space $\mathbb{F}$ is the simplest linear map we can have, there are still several levels of* *complexity here depending on what field we use. Let us consider the map* $L : \mathbb{C} \to \mathbb{C}$ *that is multiplication by* i*, i.e.,* $L(x) = ix$*. If we write* $x = \alpha + i\beta$ *we see that* $L(x) = -\beta + i\alpha$*. Geometrically what we are doing is rotating* x *90°. If we think of* $\mathbb{C}$ *as the plane* $\mathbb{R}^2$ *the map is instead given by the matrix*

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

which is not at all scalar multiplication if we only think in terms of real scalars. Thus a supposedly simple operation with complex numbers is somewhat less simple when we forget complex numbers. What we need to keep in mind is that scalar multiplication with real numbers is simply a form of dilation where vectors are made longer or shorter depending on the scalar. Scalar multiplication with complex numbers is from an abstract algebraic viewpoint equally simple to write down, but geometrically such an operation can involve a rotation from the perspective of a world where only real scalars exist.

EXAMPLE 15. *The* i^{th} *coordinate map* $\mathbb{F}^n \to \mathbb{F}$ *defined by*

$$\begin{aligned} dx_i(x) &= dx_i\left(\begin{bmatrix} \xi_1 \\ \vdots \\ \xi_i \\ \vdots \\ \xi_n \end{bmatrix}\right) \\ &= [0 \cdots 1 \cdots 0] \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_i \\ \vdots \\ \xi_n \end{bmatrix} \\ &= \xi_i. \end{aligned}$$

is a linear map. Here the $1 \times n$ *matrix* $[0 \cdots 1 \cdots 0]$ *is zero everywhere except in the* i^{th} *entry where it is* 1*. The notation* dx_i *is not a mistake, but an incursion from multivariable calculus. While some mystifying words involving infinitesimals often are invoked in connection with such symbols, they have in more advanced and modern treatments of the subject simply been redefined as done here. No mystery at all definitionwise, but it is perhaps no clearer why it has anything to do with integration and differentiation.*

A special piece of notation comes in handy in here. The Kronecker δ symbol is defined as

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

Thus the matrix $[0 \cdots 1 \cdots 0]$ can also be written as

$$\begin{aligned} \begin{bmatrix} 0 & \cdots & 1 & \cdots & 0 \end{bmatrix} &= \begin{bmatrix} \delta_{i1} & \cdots & \delta_{ii} & \cdots & \delta_{in} \end{bmatrix} \\ &= \begin{bmatrix} \delta_{i1} & \cdots & \delta_{in} \end{bmatrix}. \end{aligned}$$

The matrix representing the identity map $1_{\mathbb{F}^n}$ can then we written as

$$\begin{bmatrix} \delta_{11} & \cdots & \delta_{1n} \\ \vdots & \ddots & \vdots \\ \delta_{n1} & \cdots & \delta_{nn} \end{bmatrix}.$$

EXAMPLE 16. *Let us consider the vector space of functions $C^\infty(\mathbb{R},\mathbb{R})$ that have derivatives of all orders. There are several interesting linear operators $C^\infty(\mathbb{R},\mathbb{R}) \to C^\infty(\mathbb{R},\mathbb{R})$*

$$\begin{aligned} D(f)(t) &= \frac{df}{dt}(t), \\ S(f)(t) &= \int_{t_0}^{t} f(s)\,ds, \\ T(f)(t) &= t \cdot f(t). \end{aligned}$$

In a more shorthand fashion we have the differentiation operator $D(f) = f'$, *the* integration operator $S(f) = \int f$, *and the* multiplication operator $T(f) = tf$. *Note that the integration operator is not well-defined unless we use the definite integral and even in that case it depends on the value t_0. These three operators are also defined as operators $\mathbb{R}[t] \to \mathbb{R}[t]$. In this case we usually let $t_0 = 0$ for S. These operators have some interesting relationships. We point out a very intriguing one*

$$DT - TD = 1.$$

To see this simply use Leibniz' rule for differentiating a product to obtain

$$\begin{aligned} D(T(f)) &= D(tf) \\ &= f + tDf \\ &= f + T(D(f)). \end{aligned}$$

With some slight changes the identity $DT - TD = 1$ is the Heisenberg Commutation Law. *This law is important in the verification of* Heisenberg's Uncertainty Principle.

The *trace* is a linear map on square matrices that simply adds the diagonal entries.

$$\begin{aligned} \mathrm{tr} &: \mathrm{Mat}_{n\times n}(\mathbb{F}) \to \mathbb{F}, \\ \mathrm{tr}(A) &= \alpha_{11} + \alpha_{22} + \cdots + \alpha_{nn}. \end{aligned}$$

The trace satisfies the following important commutation relationship.

LEMMA 2. (Invariance of Trace) *If $A \in \mathrm{Mat}_{m\times n}(\mathbb{F})$ and $B \in \mathrm{Mat}_{n\times m}(\mathbb{F})$, then $AB \in \mathrm{Mat}_{m\times m}(\mathbb{F})$, $BA \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ and*

$$\mathrm{tr}(AB) = \mathrm{tr}(BA).$$

PROOF. We write out the matrices

$$A = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix}$$
$$B = \begin{bmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{bmatrix}$$

Thus

$$\begin{aligned} AB &= \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix} \begin{bmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{bmatrix} \\ &= \begin{bmatrix} \alpha_{11}\beta_{11} + \cdots + \alpha_{1n}\beta_{n1} & \cdots & \alpha_{11}\beta_{1m} + \cdots + \alpha_{1n}\beta_{nm} \\ \vdots & \ddots & \vdots \\ \alpha_{m1}\beta_{11} + \cdots + \alpha_{mn}\beta_{n1} & \cdots & \alpha_{m1}\beta_{1m} + \cdots + \alpha_{mn}\beta_{nm} \end{bmatrix} \end{aligned}$$

$$\begin{aligned} BA &= \begin{bmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{bmatrix} \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix} \\ &= \begin{bmatrix} \beta_{11}\alpha_{11} + \cdots + \beta_{1m}\alpha_{m1} & \cdots & \beta_{11}\alpha_{1n} + \cdots + \beta_{1m}\alpha_{mn} \\ \vdots & \ddots & \vdots \\ \beta_{n1}\alpha_{11} + \cdots + \beta_{nm}\alpha_{m1} & \cdots & \beta_{n1}\alpha_{1n} + \cdots + \beta_{nm}\alpha_{mn} \end{bmatrix} \end{aligned}$$

This tells us that $AB \in \mathrm{Mat}_{m\times m}(\mathbb{F})$ and $BA \in \mathrm{Mat}_{n\times n}(\mathbb{F})$. To show the identity note that the (i,i) entry in AB is $\sum_{j=1}^{n} \alpha_{ij}\beta_{ji}$, while the (j,j) entry in BA is $\sum_{i=1}^{m} \beta_{ji}\alpha_{ij}$. Thus

$$\begin{aligned} \operatorname{tr}(AB) &= \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_{ij}\beta_{ji}, \\ \operatorname{tr}(BA) &= \sum_{j=1}^{n}\sum_{i=1}^{m} \beta_{ji}\alpha_{ij}. \end{aligned}$$

By using $\alpha_{ij}\beta_{ji} = \beta_{ji}\alpha_{ij}$ and

$$\sum_{i=1}^{m}\sum_{j=1}^{n} = \sum_{j=1}^{n}\sum_{i=1}^{m}$$

we see that the two traces are equal. □

This allows us to show that *Heisenberg Commutation Law* cannot be true for matrices.

COROLLARY 1. *There are no matrices* $A, B \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ *such that*

$$AB - BA = 1.$$

Proof. By the above Lemma and linearity we have that $\operatorname{tr}(AB - BA) = 0$. On the other hand $\operatorname{tr}(1_{\mathbb{F}^n}) = n$, since the identity matrix has n diagonal entries each of which is 1. □

Observe that we just used the fact that $n \neq 0$ in $\mathbb{F}$, or in other words that $\mathbb{F}$ has characteristic zero. If we allowed ourselves to use the field $\mathbb{F}_2 = \{0, 1\}$ where $1 + 1 = 0$, then we have that $1 = -1$. Thus we can use the matrices

$$\begin{aligned} A &= \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \\ B &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \end{aligned}$$

to get the Heisenberg commutation law satisfied:

$$\begin{aligned} AB - BA &= \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

We have two further linear maps. Consider $V = \operatorname{Func}(S, \mathbb{F})$ and select $s_0 \in S$, then the *evaluation map* $\operatorname{ev}_{s_0} : \operatorname{Func}(S, \mathbb{F}) \to \mathbb{F}$ defined by $\operatorname{ev}_{s_0}(f) = f(s_0)$ is linear. More generally we have the *restriction map* for $T \subset S$ defined as a linear maps $\operatorname{Func}(S, \mathbb{F}) \to \operatorname{Func}(T, \mathbb{F})$, by mapping f to $f|_T$. The notation $f|_T$ means that we only consider f as mapping from T into $\mathbb{F}$. In other words we have forgotten that f maps all of S into $\mathbb{F}$ and only remembered what it did on T.

Linear maps play a big role in multivariable calculus and are used in a number of ways to clarify and understand certain constructions. The fact that linear algebra is the basis for multivariable calculus should not be surprising as linear algebra is merely a generalization of vector algebra.

Let $F : \Omega \to \mathbb{R}^n$ be a differentiable function defined on some open domain $\Omega \subset \mathbb{R}^m$. The differential of F at $x_0 \in \Omega$ is a linear map $DF_{x_0} : \mathbb{R}^m \to \mathbb{R}^n$ that can be defined via the limiting process

$$DF_{x_0}(h) = \lim_{t \to 0} \frac{F(x_0 + th) - F(x_0)}{t}.$$

Note that $x_0 + th$ describes a line parametrized by t passing through x_0 and points in the direction of h. This definition tells us that DF_{x_0} preserves scalar multiplication as

$$\begin{aligned} DF_{x_0}(\alpha h) &= \lim_{t\to 0}\frac{F(x_0+t\alpha h)-F(x_0)}{t} \\ &= \alpha\lim_{t\to 0}\frac{F(x_0+t\alpha h)-F(x_0)}{t\alpha} \\ &= \alpha\lim_{t\alpha\to 0}\frac{F(x_0+t\alpha h)-F(x_0)}{t\alpha} \\ &= \alpha\lim_{s\to 0}\frac{F(x_0+sh)-F(x_0)}{s} \\ &= \alpha DF_{x_0}(h). \end{aligned}$$

Additivity is another matter however. Thus one often reverts to the trick of saying that F is differentiable at x_0 provided we can find a linear map $L:\mathbb{R}^m\to\mathbb{R}^n$ satisfying

$$\lim_{|h|\to 0}\frac{|F(x_0+h)-F(x_0)-L(h)|}{|h|}=0$$

One then proves that such a linear map must be unique and then renames it $L=DF_{x_0}$. In case F is continuously differentiable, DF_{x_0} is also given by the $n\times m$ matrix of partial derivatives

$$\begin{aligned} DF_{x_0}(h) &= DF_{x_0}\left(\begin{bmatrix} h_1 \\ \vdots \\ h_m\end{bmatrix}\right) \\ &= \begin{bmatrix} \frac{\partial F_1}{\partial x_1} & \cdots & \frac{\partial F_1}{\partial x_m} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_n}{\partial x_1} & \cdots & \frac{\partial F_n}{\partial x_m}\end{bmatrix}\begin{bmatrix} h_1 \\ \vdots \\ h_m\end{bmatrix} \\ &= \begin{bmatrix} \frac{\partial F_1}{\partial x_1}h_1+\cdots+\frac{\partial F_1}{\partial x_m}h_m \\ \vdots \\ \frac{\partial F_n}{\partial x_1}h_1+\cdots+\frac{\partial F_n}{\partial x_m}h_m\end{bmatrix} \end{aligned}$$

One of the main ideas in differential calculus (of several variables) is that linear maps are simpler to work with and that they give good local approximations to differentiable maps. This can be made more precise by observing that we have the *first order approximation*

$$\begin{aligned} F(x_0+h) &= F(x_0)+DF_{x_0}(h)+o(h), \\ \lim_{|h|\to 0}\frac{|o(h)|}{|h|} &= 0 \end{aligned}$$

One of the goals of differential calculus is to exploit knowledge of the linear map DF_{x_0} and then use this first order approximation to get a better understanding of the map F itself.

In case $f:\Omega\to\mathbb{R}$ is a function one often sees the differential of f defined as the expression

$$df=\frac{\partial f}{\partial x_1}dx_1+\cdots+\frac{\partial f}{\partial x_m}dx_m.$$

Having now interpreted dx_i as a linear function we then observe that df itself is a linear function whose matrix description is given by

$$\begin{aligned} df(h) &= \frac{\partial f}{\partial x_1} dx_1(h) + \cdots + \frac{\partial f}{\partial x_m} dx_m(h) \\ &= \frac{\partial f}{\partial x_1} h_1 + \cdots + \frac{\partial f}{\partial x_m} h_m \\ &= \begin{bmatrix} \frac{\partial f}{\partial x_1} & \cdots & \frac{\partial f}{\partial x_m} \end{bmatrix} \begin{bmatrix} h_1 \\ \vdots \\ h_m \end{bmatrix}. \end{aligned}$$

More generally, if we write

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_n \end{bmatrix},$$

then

$$DF_{x_0} = \begin{bmatrix} dF_1 \\ \vdots \\ dF_n \end{bmatrix}$$

with the understanding that

$$DF_{x_0}(h) = \begin{bmatrix} dF_1(h) \\ \vdots \\ dF_n(h) \end{bmatrix}.$$

Note how this conforms nicely with the above matrix representation of the differential.

6.1. Exercises.

(1) Let V, W be vector spaces over $\mathbb{Q}$. Show that any *additive* map $L : V \to W$, i.e.,

$$L(x_1 + x_2) = L(x_1) + L(x_2),$$

is linear.

(2) Show that $D : \mathbb{F}[t] \to \mathbb{F}[t]$ defined by

$$D(\alpha_0 + \alpha_1 t + \cdots + \alpha_n t^n) = \alpha_1 + 2\alpha_2 t + \cdots + n\alpha_n t^{n-1}$$

is a linear map.

(3) If $L : V \to V$ is a linear operator, then $K : \mathbb{F}[t] \to \hom(V, V)$ defined by $K(p) = p(L)$ is a linear map.

(4) If $T : V \to W$ is a linear operator, and $\tilde{V}$ is a vector space, then right multiplication

$$R_T : \hom\left(W, \tilde{V}\right) \to \hom\left(V, \tilde{V}\right)$$

defined by $R_T(K) = K \circ T$ and left multiplication

$$L_T : \hom\left(\tilde{V}, V\right) \to \hom\left(\tilde{V}, W\right)$$

defined by $L_T(K) = T \circ K$ are linear operators.

(5) If $A \in \text{Mat}_{n\times n}(\mathbb{F})$ is upper triangular, i.e., $\alpha_{ij} = 0$ for $i > j$ or

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{nn} \end{bmatrix},$$

and $p(t) \in \mathbb{F}[t]$, then $p(A)$ is also upper triangular and the diagonal entries are $p(\alpha_{ii})$, i.e.,

$$p(A) = \begin{bmatrix} p(\alpha_{11}) & * & \cdots & * \\ 0 & p(\alpha_{22}) & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p(\alpha_{nn}) \end{bmatrix}.$$

(6) Let $t_1, ..., t_n \in \mathbb{R}$ and define

$$\begin{aligned} L &: C^\infty(\mathbb{R},\mathbb{R}) \to \mathbb{R}^n \\ L(f) &= (f(t_1), ..., f(t_n)). \end{aligned}$$

Show that L is linear.

(7) Let $t_0 \in \mathbb{R}$ and define

$$\begin{aligned} L &: C^\infty(\mathbb{R},\mathbb{R}) \to \mathbb{R}^n \\ L(f) &= \left(f(t_0), (Df)(t_0), ..., \left(D^{n-1}f\right)(t_0)\right). \end{aligned}$$

Show that L is linear.

(8) Let $A \in \text{Mat}_{n\times n}(\mathbb{R})$ be symmetric, i.e., the (i,j) entry is the same as the (j,i) entry. Show that $A = 0$ if and only if $\text{tr}\left(A^2\right) = 0$.

(9) For each $n \geq 2$ find $A \in \text{Mat}_{n\times n}(\mathbb{F})$ such that $A \neq 0$, but $\text{tr}\left(A^k\right) = 0$ for all $k = 1, 2, ...$

(10) Find $A \in \text{Mat}_{2\times 2}(\mathbb{R})$ such that $\text{tr}\left(A^2\right) < 0$.

7. Linear Maps as Matrices

We saw above that quite a lot of linear maps can be defined using matrices. In this section we shall reverse this construction and show that all abstractly defined linear maps between finite dimensional vector spaces come from some basic matrix constructions.

To warm up we start with the simplest situation.

Lemma 3. *Assume V is one dimensional over $\mathbb{F}$, then any $L : V \to V$ is of the form $L = \lambda 1_V$.*

Proof. Assume x_1 is a basis. Then $L(x_1) = \lambda x_1$ for some $\lambda \in \mathbb{F}$. Now any $x = \alpha x_1$ so $L(x) = L(\alpha x_1) = \alpha L(x_1) = \alpha\lambda x_1 = \lambda x$ as desired. □

This gives us a very simple canonical form for linear maps in this elementary situation. The rest of the section tries to explain how one can generalize this to vector spaces with finite bases.

Possibly the most important abstractly defined linear map comes from considering linear combinations. We fix a vector space V over $\mathbb{F}$ and select $x_1, ..., x_m \in V$.

Then we have a linear map

$$\begin{aligned} L &: \mathbb{F}^m \to V \\ L\left(\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}\right) &= \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} \\ &= x_1\alpha_1 + \cdots + x_m\alpha_m. \end{aligned}$$

The fact that it is linear follows from knowing that $L : \mathbb{F} \to V$ defined by $L(\alpha) = \alpha x$ is linear together with the fact that sums of linear maps are linear. We shall denote this map by its row matrix

$$L = \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix},$$

where the entries are vectors. Using the standard basis $e_1, ..., e_m$ for $\mathbb{F}^m$ we observe that the entries x_i (think of them as column vectors) satisfy

$$L(e_i) = \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} e_i = x_i.$$

Thus the vectors that form the columns for the matrix for L are the images of the basis vectors for $\mathbb{F}^m$. With this in mind we can show

LEMMA 4. *Any linear map $L : \mathbb{F}^m \to V$ is of the from*

$$L = \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix}$$

where $x_i = L(e_i)$.

PROOF. Define $L(e_i) = x_i$ and use linearity of L to see that

$$\begin{aligned} L\left(\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}\right) &= L\left(\begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}\right) \\ &= L(e_1\alpha_1 + \cdots + e_m\alpha_m) \\ &= L(e_1)\alpha_1 + \cdots + L(e_m)\alpha_m \\ &= \begin{bmatrix} L(e_1) & \cdots & L(e_m) \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} \\ &= \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}. \end{aligned}$$

□

In case we specialize to the situation where $V = \mathbb{F}^n$ the vectors $x_1, ..., x_m$ really are $n \times 1$ column matrices. If we write them accordingly

$$x_i = \begin{bmatrix} \beta_{1i} \\ \vdots \\ \beta_{ni} \end{bmatrix},$$

then

$$\begin{aligned}
\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix}\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} &= x_1\alpha_1 + \cdots + x_m\alpha_m \\
&= \begin{bmatrix} \beta_{11} \\ \vdots \\ \beta_{n1} \end{bmatrix}\alpha_1 + \cdots + \begin{bmatrix} \beta_{1m} \\ \vdots \\ \beta_{nm} \end{bmatrix}\alpha_m \\
&= \begin{bmatrix} \beta_{11}\alpha_1 \\ \vdots \\ \beta_{n1}\alpha_1 \end{bmatrix} + \cdots + \begin{bmatrix} \beta_{1m}\alpha_m \\ \vdots \\ \beta_{nm}\alpha_m \end{bmatrix} \\
&= \begin{bmatrix} \beta_{11}\alpha_1 + \cdots + \beta_{1m}\alpha_m \\ \vdots \\ \beta_{n1}\alpha_1 + \cdots + \beta_{nm}\alpha_m \end{bmatrix} \\
&= \begin{bmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{bmatrix}\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}.
\end{aligned}$$

Hence any linear map $\mathbb{F}^m \to \mathbb{F}^n$ is given by matrix multiplication, and the columns of the matrix are the images of the basis vectors of $\mathbb{F}^m$.

We can also use this to study maps $V \to W$ as long as we have bases $e_1, ..., e_m$ for V and $f_1, ..., f_n$ for W. Each $x \in V$ has a unique expansion

$$x = \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix}\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}.$$

So if $L : V \to W$ is linear, then

$$\begin{aligned}
L(x) &= L\left(\begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix}\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}\right) \\
&= \begin{bmatrix} L(e_1) & \cdots & L(e_m) \end{bmatrix}\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} \\
&= \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix}\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix},
\end{aligned}$$

where $x_i = L(e_i)$. In effect we have proven that

$$L \circ \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix} = \begin{bmatrix} L(e_1) & \cdots & L(e_m) \end{bmatrix}$$

if we interpret

$$\begin{aligned}
\begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix} &: \mathbb{F}^m \to V, \\
\begin{bmatrix} L(e_1) & \cdots & L(e_m) \end{bmatrix} &: \mathbb{F}^m \to W
\end{aligned}$$

as linear maps.

Expanding $L(e_i) = x_i$ with respect to the basis for W gives us

$$x_i = \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} \begin{bmatrix} \beta_{1i} \\ \vdots \\ \beta_{ni} \end{bmatrix}$$

and

$$\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} = \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} \begin{bmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{bmatrix}.$$

This gives us the *matrix representation* for a linear map $V \to W$ with respect to the specified bases.

$$\begin{aligned} L(x) &= \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} \\ &= \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} \begin{bmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}. \end{aligned}$$

We will often use the terminology

$$[L] = \begin{bmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{bmatrix}$$

for the matrix representing L. The way to remember the formula for $[L]$ is to use

$$\begin{aligned} L \circ \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix} &= \begin{bmatrix} L(e_1) & \cdots & L(e_m) \end{bmatrix} \\ &= \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} [L]. \end{aligned}$$

In the special case where $L : V \to V$ is a linear operator one usually only selects one basis $e_1, ..., e_n$. In this case we get the relationship

$$\begin{aligned} L \circ \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} &= \begin{bmatrix} L(e_1) & \cdots & L(e_n) \end{bmatrix} \\ &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} [L] \end{aligned}$$

for the matrix representation.

Example 17. *Let*

$$P_n = \{\alpha_0 + \alpha_1 t + \cdots + \alpha_n t^n : \alpha_0, \alpha_1, ..., \alpha_n \in \mathbb{F}\}$$

be the space of polynomials of degree $\leq n$ *and* $D : V \to V$ *the differentiation operator*

$$D(\alpha_0 + \alpha_1 t + \cdots + \alpha_n t^n) = \alpha_1 + \cdots + n\alpha_n t^{n-1}.$$

If we use the basis $1, t, ..., t^n$ *for* V *then we see that*

$$D\left(t^k\right) = kt^{k-1}$$

and thus the $(n+1)\times(n+1)$ *matrix representation is computed via*

$$\begin{aligned} & \left[\begin{array}{ccccc} D(1) & D(t) & D\left(t^2\right) & \cdots & D(t^n) \end{array}\right] \\ = & \left[\begin{array}{ccccc} 0 & 1 & 2t & \cdots & nt^{n-1} \end{array}\right] \\ = & \left[\begin{array}{ccccc} 1 & t & t^2 & \cdots & t^n \end{array}\right] \left[\begin{array}{ccccc} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 2 & \cdots & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & n \\ 0 & 0 & 0 & \cdots & 0 \end{array}\right]. \end{aligned}$$

EXAMPLE 18. *Next consider the maps* $T,S:P_n\to P_{n+1}$ *defined by*

$$\begin{aligned} T\left(\alpha_0+\alpha_1 t+\cdots+\alpha_n t^n\right) &= \alpha_0 t+\alpha_1 t^2+\cdots+\alpha_n t^{n+1}, \\ S\left(\alpha_0+\alpha_1 t+\cdots+\alpha_n t^n\right) &= \alpha_0 t+\frac{\alpha_1}{2}t^2+\cdots+\frac{\alpha_n}{n+1}t^{n+1}. \end{aligned}$$

This time the image space and domain are not the same but the choices for basis are at least similar. We get the $(n+2)\times(n+1)$ *matrix representations*

$$\begin{aligned} & \left[\begin{array}{ccccc} T(1) & T(t) & T\left(t^2\right) & \cdots & T(t^n) \end{array}\right] \\ = & \left[\begin{array}{ccccc} t & t^2 & t^3 & \cdots & t^{n+1} \end{array}\right] \\ = & \left[\begin{array}{cccccc} 1 & t & t^2 & t^3 & \cdots & t^{n+1} \end{array}\right] \left[\begin{array}{ccccc} 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{array}\right] \end{aligned}$$

$$\begin{aligned} & \left[\begin{array}{ccccc} S(1) & S(t) & S\left(t^2\right) & \cdots & S(t^n) \end{array}\right] \\ = & \left[\begin{array}{ccccc} t & \frac{1}{2}t^2 & \frac{1}{3}t^3 & \cdots & \frac{1}{n+1}t^{n+1} \end{array}\right] \\ = & \left[\begin{array}{cccccc} 1 & t & t^2 & t^3 & \cdots & t^{n+1} \end{array}\right] \left[\begin{array}{ccccc} 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & \frac{1}{2} & 0 & \cdots & 0 \\ 0 & 0 & \frac{1}{3} & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & \frac{1}{n} \end{array}\right] \end{aligned}$$

Doing a matrix representation of a linear map that is already given as a matrix can get a little confusing, but the procedure is obviously the same.

EXAMPLE 19. *Let*

$$L=\left[\begin{array}{cc} 1 & 1 \\ 0 & 2 \end{array}\right]:\mathbb{F}^2\to\mathbb{F}^2$$

and consider the basis

$$x_1=\left[\begin{array}{c} 1 \\ 0 \end{array}\right], x_2=\left[\begin{array}{c} 1 \\ 1 \end{array}\right].$$

Then

$$L(x_1) = x_1,$$
$$L(x_2) = \begin{bmatrix} 2 \\ 2 \end{bmatrix} = 2x_2.$$

So

$$\begin{bmatrix} L(x_1) & L(x_2) \end{bmatrix} = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

Example 20. *Let*

$$L = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} : \mathbb{F}^2 \to \mathbb{F}^2$$

and consider the basis

$$x_1 = \begin{bmatrix} 1 \\ -1 \end{bmatrix}, x_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Then

$$L(x_1) = \begin{bmatrix} 0 \\ -2 \end{bmatrix} = x_1 - x_2,$$
$$L(x_2) = \begin{bmatrix} 2 \\ 2 \end{bmatrix} = 2x_2.$$

So

$$\begin{bmatrix} L(x_1) & L(x_2) \end{bmatrix} = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix}.$$

Example 21. *Let*

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{F})$$

and consider

$$\begin{aligned} L_A &: \mathrm{Mat}_{2\times 2}(\mathbb{F}) \to \mathrm{Mat}_{2\times 2}(\mathbb{F}) \\ L_A(X) &= AX. \end{aligned}$$

We use the basis E_{ij} for $\mathrm{Mat}_{n\times n}(\mathbb{F})$ where the ij entry in E_{ij} is 1 and all other entries are zero. Next order the basis $E_{11}, E_{21}, E_{12}, E_{22}$. This means that we think of $\mathrm{Mat}_{2\times 2}(\mathbb{F}) \approx \mathbb{F}^4$ were the columns are stacked on top of each other with the first column being the top most. With this choice of basis we note that

$$\begin{aligned} & \begin{bmatrix} L_A(E_{11}) & L_A(E_{21}) & L_A(E_{12}) & L_A(E_{22}) \end{bmatrix} \\ = & \begin{bmatrix} AE_{11} & AE_{21} & AE_{12} & AE_{22} \end{bmatrix} \\ = & \begin{bmatrix} \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \begin{bmatrix} 0 & c \\ 0 & d \end{bmatrix} \end{bmatrix} \\ = & \begin{bmatrix} E_{11} & E_{21} & E_{12} & E_{22} \end{bmatrix} \begin{bmatrix} a & c & 0 & 0 \\ b & d & 0 & 0 \\ 0 & 0 & a & c \\ 0 & 0 & b & d \end{bmatrix} \end{aligned}$$

Thus L_A has the block diagonal form

$$\begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}$$

This problem easily generalizes to the case of $n \times n$ *matrices, where* L_A *will have a block diagonal form that looks like*

$$\begin{bmatrix} A & 0 & \cdots & 0 \\ 0 & A & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{bmatrix}$$

EXAMPLE 22. *Let* $L : \mathbb{F}^n \to \mathbb{F}^n$ *be a linear map which maps basis vectors to basis vectors. Thus* $L(e_j) = e_{\sigma(j)}$, *where*

$$\sigma : \{1, ..., n\} \to \{1, ..., n\}.$$

If σ *is one-to-one and onto then it is called a* permutation. *Apparently it permutes the elements of* $\{1, ..., n\}$. *The corresponding linear map is denoted* L_σ. *The matrix representation of* L_σ *can be computed from the simple relationship* $L_\sigma(e_j) = e_{\sigma(j)}$. *Thus the* j^{th} *column has zeros everywhere except for a* 1 *in the* $\sigma(j)$ *entry. This means that* $[L_\sigma] = [\delta_{i,\sigma(j)}]$. *The matrix* $[L_\sigma]$ *is also known as a* permutation matrix.

EXAMPLE 23. *Let* $L : V \to V$ *be a linear map whose matrix representation with respect to the basis* x_1, x_2 *is given by*

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}.$$

We wish to compute the matrix representation of $K = 2L^2 + 3L - 1_V$. *We know that*

$$\begin{bmatrix} L(x_1) & L(x_2) \end{bmatrix} = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

or equivalently

$$\begin{aligned} L(x_1) &= x_1, \\ L(x_2) &= 2x_1 + x_2. \end{aligned}$$

Thus

$$\begin{aligned} K(x_1) &= 2L(L(x_1)) + 3L(x_1) - 1_V(x_1) \\ &= 2L(x_1) + 3x_1 - x_1 \\ &= 2x_1 + 3x_1 - x_1 \\ &= 4x_1, \\ K(x_2) &= 2L(L(x_2)) + 3L(x_2) - 1_V(x_2) \\ &= 2L(2x_1 + x_2) + 3(2x_1 + x_2) - x_2 \\ &= 2(2x_1 + (2x_1 + x_2)) + 3(2x_1 + x_2) - x_2 \\ &= 14x_1 + 4x_2, \end{aligned}$$

and

$$\begin{bmatrix} K(x_1) & K(x_2) \end{bmatrix} = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} 1 & 14 \\ 0 & 4 \end{bmatrix}.$$

7.1. Exercises.

(1) (a) Show that t^3, t^3+t^2, t^3+t^2+t, t^3+t^2+t+1 form a basis for P_3.
(b) Compute the image of $(1,2,3,4)$ under the coordinate map

$$\begin{bmatrix} t^3 & t^3+t^2 & t^3+t^2+t & t^3+t^2+t+1 \end{bmatrix} : \mathbb{F}^4 \to P_3$$

(c) Find the vector in $\mathbb{F}^4$ whose image is $4t^3+3t^2+2t+1$.

(2) Find the matrix representation for $D : P_3 \to P_3$ with respect to the basis t^3, t^3+t^2, t^3+t^2+t, t^3+t^2+t+1.

(3) Find the matrix representation for

$$D^2 + 2D + 1 : P_3 \to P_3$$

with respect to the standard basis $1, t, t^2, t^3$.

(4) If $L : V \to V$ is a linear operator on a finite dimensional vector space and $p(t) \in \mathbb{F}[t]$, then the matrix representations for L and $p(L)$ with respect to some fixed basis are related by $[p(L)] = p([L])$.

(5) Consider the two linear maps $L, K : P_n \to \mathbb{C}^{n+1}$ defined by

$$\begin{aligned} L(f) &= (f(t_0), ..., f(t_n)) \\ K(f) &= (f(t_0), (Df)(t_0), ..., (D^n f)(t_0)). \end{aligned}$$

(a) Find a basis $p_0, ..., p_n$ for P_n such that $K(p_i) = e_i$, where $e_1, ..., e_n$ is the canonical basis for $\mathbb{C}^{n+1}$.
(b) Provided $t_0, ..., t_n$ are distinct find a basis $q_0, ..., q_n$ for P_n such that $L(q_i) = e_i$.

(6) Let

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

and consider the linear map $R_A : \mathrm{Mat}_{2\times 2}(\mathbb{F}) \to \mathrm{Mat}_{2\times 2}(\mathbb{F})$ defined by $R_A(X) = XA$. Compute the matrix representation of this linear maps with respect to the basis

$$\begin{aligned} E_{11} &= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \\ E_{21} &= \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \\ E_{12} &= \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \\ E_{22} &= \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

(7) Compute a matrix representation for $L : \mathrm{Mat}_{2\times 2}(\mathbb{F}) \to \mathrm{Mat}_{1\times 2}(\mathbb{F})$ defined by $L(X) = \begin{bmatrix} 1 & -1 \end{bmatrix} X$.

(8) Let $A \in \mathrm{Mat}_{n\times m}(\mathbb{F})$ and E_{ij} the matrix that has 1 in the ij entry and is zero elsewhere.
(a) If $E_{ij} \in \mathrm{Mat}_{k\times n}(\mathbb{F})$, then $E_{ij}A \in \mathrm{Mat}_{k\times m}(\mathbb{F})$ is the matrix whose i^{th} row is the j^{th} row of A and all other entries are zero.
(b) If $E_{ij} \in \mathrm{Mat}_{n\times k}(\mathbb{F})$, then $AE_{ij} \in \mathrm{Mat}_{n\times k}(\mathbb{F})$ is the matrix whose j^{th} column is the i^{th} column of A and all other entries are zero.

(9) Let e_1, e_2 be the standard basis for $\mathbb{C}^2$ and consider the two real bases e_1, e_2, ie_1, ie_2 and e_1, ie_1, e_2, ie_2. If $\lambda = \alpha + i\beta$ is a complex number, then compute the real matrix representations for $\lambda 1_{\mathbb{C}^2}$ with respect to both bases.

(10) If $L : V \to V$ has a lower triangular representation with respect to the basis $x_1, ..., x_n$, then it has an upper triangular representation with respect to $x_n, ..., x_1$.

(11) Let V and W be vector spaces with bases $e_1, ..., e_m$ and $f_1, ..., f_n$ respectively. Define $E_{ij} \in \hom(V, W)$ as the linear map that sends e_j to f_i and all other e_ks go to zero, i.e., $E_{ij}(e_k) = \delta_{jk} f_i$.
  (a) Show that the matrix representation for E_{ij} is 1 in the ij entry and 0 otherwise.
  (b) Show that E_{ij} form a basis for $\hom(V, W)$.
  (c) If $L \in \hom(V, W)$, then $L = \sum_{i,j} \alpha_{ij} E_{ij}$. Show that $[L] = [\alpha_{ij}]$ with respect to these bases.

8. Dimension and Isomorphism

We are now almost ready to prove that the number of elements in a basis for a fixed vector space is always the same.

Two vector spaces V and W over $\mathbb{F}$ are said to be *isomorphic* if we can find linear maps $L : V \to W$ and $K : W \to V$ such that $LK = 1_W$ and $KL = 1_V$. One can also describe the equations $LK = 1_W$ and $KL = 1_V$ in an interesting little diagram of maps

$$\begin{array}{ccc} V & \xrightarrow{L} & W \\ \uparrow 1_V & & \uparrow 1_W \\ V & \xleftarrow{K} & W \end{array}$$

where the vertical arrows are the identity maps.

We also say that a linear map $L : V \to W$ is an *isomorphism* if we can find $K : W \to V$ such that $LK = 1_W$ and $KL = 1_V$.

Note that if V_1 and V_2 are isomorphic and V_2 and V_3 are isomorphic, then also V_1 and V_3 must be isomorphic by composition of the given isomorphisms.

Recall that a map $f : S \to T$ between sets is *one-to-one* or *injective* if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$. A better name for this concept is two-to-two as pointed out by R. Arens, since injective maps evidently take two distinct points to two distinct points. We say that $f : S \to T$ is *onto* or *surjective* if every $y \in T$ is of the form $y = f(x)$ for some $x \in S$. In others words $f(S) = T$. A map that is both one-to-one and onto is said to be bijective. Such a map always has an inverse f^{-1} defined via $f^{-1}(y) = x$ if $f(x) = y$. Note that for each $y \in T$ such an x exists since f is onto and that this x is unique since f is one-to-one. The relationship between f and f^{-1} is $f \circ f^{-1}(y) = y$ and $f^{-1} \circ f(x) = x$. Observe that $f^{-1} : T \to S$ is also a bijection and has inverse $\left(f^{-1}\right)^{-1} = f$.

Lemma 5. *V and W are* isomorphic *if and only if there is a bijective linear map $L : V \to W$.*

The "if and only if" part asserts that the two statements

- V and W are *isomorphic.*
- There is a bijective linear map $L : V \to W$.

are equivalent. In other words, if one statement is true, then so is the other. To establish the Lemma it is therefore necessary to prove two things, namely, that the first statement implies the second and that the second implies the first.

PROOF. If V and W are isomorphic, then we can find linear maps $L : V \to W$ and $K : W \to V$ so that $LK = 1_W$ and $KL = 1_V$. Then for any $y \in W$

$$y = 1_W(y) = L(K(y)).$$

Thus $y = L(x)$ if $x = K(y)$. This means L is onto. If $L(x_1) = L(x_2)$ then

$$x_1 = 1_V(x_1) = KL(x_1) = KL(x_2) = 1_V(x_2) = x_2.$$

Showing that L is one-to-one.

Conversely assume $L : V \to W$ is linear and a bijection. Then we have an inverse map L^{-1} that satisfies $L \circ L^{-1} = 1_W$ and $L^{-1} \circ L = 1_V$. In order for this inverse to be allowable as K we need to check that it is linear. Thus select $\alpha_1, \alpha_2 \in \mathbb{F}$ and $y_1, y_2 \in W$. Let $x_i = L^{-1}(y_i)$ so that $L(x_i) = y_i$. Then we have

$$\begin{aligned}
L^{-1}(\alpha_1 y_1 + \alpha_2 y_2) &= L^{-1}(\alpha_1 L(x_1) + \alpha_2 L(x_2)) \\
&= L^{-1}(L(\alpha_1 x_1 + \alpha_2 x_2)) \\
&= 1_V(\alpha_1 x_1 + \alpha_2 x_2) \\
&= \alpha_1 x_1 + \alpha_2 x_2 \\
&= \alpha_1 L^{-1}(y_1) + \alpha_2 L^{-1}(y_2)
\end{aligned}$$

as desired. □

Recall that a finite basis for V over $\mathbb{F}$ consists of a collection of vectors $x_1, ..., x_n \in V$ so that each x has a unique expansion $x = x_1\alpha_1 + \cdots + x_n\alpha_n$, $\alpha_1, ..., \alpha_n \in \mathbb{F}$. This means that the linear map

$$\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} : \mathbb{F}^n \to V$$

is a bijection and hence by the above Lemma an isomorphism. We saw in the last section that any linear map $\mathbb{F}^m \to V$ must be of this form. In particular, any isomorphism $\mathbb{F}^m \to V$ gives rise to a basis for V. Since $\mathbb{F}^n$ is our prototype for an n-dimensional vector space over $\mathbb{F}$ it is natural to say that a vector space has dimension n if it is isomorphic to $\mathbb{F}^n$. As we have just seen, this is equivalent to saying that V has a basis consisting of n vectors. The only problem is that we don't know if two spaces $\mathbb{F}^m$ and $\mathbb{F}^n$ can be isomorphic when $m \neq n$. This is taken care of next.

THEOREM 1. (Uniqueness of Dimension) *If $\mathbb{F}^m$ and $\mathbb{F}^n$ are isomorphic over $\mathbb{F}$, then $n = m$.*

PROOF. Suppose we have $L : \mathbb{F}^m \to \mathbb{F}^n$ and $K : \mathbb{F}^n \to \mathbb{F}^m$ such that $LK = 1_{\mathbb{F}^n}$ and $KL = 1_{\mathbb{F}^m}$. In "Linear maps as Matrices" we showed that the linear maps L and K are represented by matrices, i.e., $L \in \mathrm{Mat}_{n\times m}(\mathbb{F})$ and $K \in \mathrm{Mat}_{m\times n}(\mathbb{F})$. Thus we have

$$\begin{aligned}
n &= \mathrm{tr}(1_{\mathbb{F}^n}) \\
&= \mathrm{tr}(LK) \\
&= \mathrm{tr}(KL) \\
&= \mathrm{tr}(1_{\mathbb{F}^m}) \\
&= m.
\end{aligned}$$

□

This proof has the defect of only working when the field has characteristic 0. The result still holds in the more general situation where the characteristic is nonzero. Other more standard proofs that work in these more general situations can be found in "Linear Independence" and "Row Reduction".

We can now unequivocally denote and define the *dimension* of a vector space V over $\mathbb{F}$ as $\dim_{\mathbb{F}} V = n$ if V is isomorphic to $\mathbb{F}^n$. In case V is not isomorphic to any $\mathbb{F}^n$ we say that V is *infinite dimensional* and write $\dim_{\mathbb{F}} V = \infty$.

Note that some vector spaces allow for several choices of scalars and the choice of scalars can have a rather drastic effect on what the dimension is. For example $\dim_{\mathbb{C}} \mathbb{C} = 1$, while $\dim_{\mathbb{R}} \mathbb{C} = 2$. If we consider $\mathbb{R}$ as a vector space over $\mathbb{Q}$ something even worse happens: $\dim_{\mathbb{Q}} \mathbb{R} = \infty$. This is because $\mathbb{R}$ is not countably infinite, while all of the vector spaces $\mathbb{Q}^n$ are countably infinite. More precisely, it is possible to find a bijective map $f : \mathbb{N} \to \mathbb{Q}^n$, but, as first observed by G. Cantor, there is no bijective map $f : \mathbb{N} \to \mathbb{R}$. Thus the reason why $\dim_{\mathbb{Q}} \mathbb{R} = \infty$ is not solely a question of linear algebra but a more fundamental one of having bijective maps between sets.

COROLLARY 2. *If V and W are finite dimensional vector spaces over $\mathbb{F}$, then $\hom_{\mathbb{F}}(V, W)$ is also finite dimensional and*

$$\dim_{\mathbb{F}} \hom_{\mathbb{F}}(V, W) = (\dim_{\mathbb{F}} W) \cdot (\dim_{\mathbb{F}} V)$$

PROOF. By choosing bases for V and W we showed in "Linear Maps as Matrices" that there is a natural map

$$\hom_{\mathbb{F}}(V, W) \to \mathrm{Mat}_{(\dim_{\mathbb{F}} W) \times (\dim_{\mathbb{F}} V)}(\mathbb{F}) \simeq \mathbb{F}^{(\dim_{\mathbb{F}} W) \cdot (\dim_{\mathbb{F}} V)}.$$

This map is both one-to-one and onto as the matrix representation uniquely determines the linear map and every matrix yields a linear map. Finally one easily checks that the map is linear. □

In the special case where $V = W$ and we have a basis for the n-dimensional space V the linear isomorphism

$$\hom_{\mathbb{F}}(V, V) \longleftrightarrow \mathrm{Mat}_{n \times n}(\mathbb{F})$$

also preserves composition and products. Thus for $L, K : V \to V$ we have

$$[LK] = [L][K].$$

The extra product structure on the two vector spaces $\hom_{\mathbb{F}}(V, V)$ and $\mathrm{Mat}_{n \times n}(\mathbb{F})$ make these spaces into so called *algebras*. Algebras are simply vector spaces that in addition have a product structure. This product structure must satisfy the associative law, the distributive law, and also commute with scalar multiplication. Unlike a field it is not required that all nonzero elements have inverses. The above isomorphism is what we call an algebra isomorphism.

8.1. Exercises.

(1) Let $L, K : V \to V$ satisfy $L \circ K = 0$. Is it true that $K \circ L = 0$?
(2) Let $L : V \to W$ be a linear map. Show that L is an isomorphism if and only if it maps a basis for V to a basis for W.

(3) If V is finite dimensional show that V and $\hom_{\mathbb{F}}(V,\mathbb{F})$ have the same dimension and hence are isomorphic. Conclude that for each $x \in V - \{0\}$ there exists $L \in \hom_{\mathbb{F}}(V,\mathbb{F})$ such that $L(x) \neq 0$. For infinite dimensional spaces such as $\mathbb{R}$ over $\mathbb{Q}$ it is much less clear that this is true.

(4) Consider the map

$$K : V \to \hom_{\mathbb{F}}(\hom_{\mathbb{F}}(V,\mathbb{F}),\mathbb{F})$$

defined by the fact that

$$K(x) \in \hom_{\mathbb{F}}(\hom_{\mathbb{F}}(V,\mathbb{F}),\mathbb{F})$$

is the linear functional on $\hom_{\mathbb{F}}(V,\mathbb{F})$ such that

$$K(x)(L) = L(x), \text{ for } L \in \hom_{\mathbb{F}}(V,\mathbb{F}).$$

Show that this map is one-to-one when V is finite dimensional.

(5) Let $V \neq \{0\}$ be finite dimensional and assume that

$$L_1, ..., L_n : V \to V$$

are linear operators. Show that if $L_1 \circ \cdots \circ L_n = 0$, then L_i is not one-to-one for some $i = 1, ..., n$.

(6) Let $t_0, ..., t_n \in \mathbb{R}$ be distinct and consider $P_n \subset \mathbb{C}[t]$. Define $L : P_n \to \mathbb{C}^{n+1}$ by $L(p) = (p(t_0), ..., p(t_n))$. Show that L is an isomorphism. (This problem will be easier to solve later in the text.)

(7) Let $t_0 \in \mathbb{F}$ and consider $P_n \subset \mathbb{F}[t]$. Show that $L : P_n \to \mathbb{F}^{n+1}$ defined by

$$L(p) = (p(t_0), (Dp)(t_0), ..., (D^n p)(t_0))$$

is an isomorphism. Hint: Think of a Taylor expansion at t_0.

(8) Let V be finite dimensional. Show that, if $L_1, L_2 : \mathbb{F}^n \to V$ are isomorphisms, then for any $L : V \to V$ we have

$$\operatorname{tr}\left(L_1^{-1} \circ L \circ L_1\right) = \operatorname{tr}\left(L_2^{-1} \circ L \circ L_2\right).$$

This means we can define $\operatorname{tr}(L)$. Hint: Try not to use explicit matrix representations.

(9) If V and W are finite dimensional and $L_1 : V \to W$ and $L_2 : W \to V$ are linear, then show that

$$\operatorname{tr}(L_1 \circ L_2) = \operatorname{tr}(L_2 \circ L_1)$$

(10) Construct an isomorphism $V \to \hom_{\mathbb{F}}(\mathbb{F}, V)$.

(11) Let V be a complex vector space. Is the identity map $V \to V^*$ an isomorphism? (See exercises to "Vector Spaces" for a definition of V^*).

(12) Assume that V and W are finite dimensional. Define

$$\begin{aligned} \hom_{\mathbb{F}}(V,W) &\to \hom_{\mathbb{F}}(\hom_{\mathbb{F}}(W,V),\mathbb{F}), \\ L &\to [A \to \operatorname{tr}(A \circ L)]. \end{aligned}$$

Thus the linear map $L : V \to W$ is mapped to a linear map $\hom_{\mathbb{F}}(W,V) \to \mathbb{F}$, that simply takes $A \in \hom_{\mathbb{F}}(W,V)$ to $\operatorname{tr}(A \circ L)$. Show that this map is an isomorphism.

(13) Show that $\dim_{\mathbb{R}} \operatorname{Mat}_{n\times n}(\mathbb{C}) = 2n^2$, while $\dim_{\mathbb{R}} \operatorname{Mat}_{2n\times 2n}(\mathbb{R}) = 4n^2$. Conclude that there must be matrices in $\operatorname{Mat}_{2n\times 2n}(\mathbb{R})$ that do not come from complex matrices in $\operatorname{Mat}_{n\times n}(\mathbb{C})$. Find an example of a matrix in $\operatorname{Mat}_{2\times 2}(\mathbb{R})$ that does not come from $\operatorname{Mat}_{1\times 1}(\mathbb{C})$.

(14) For $A = [\alpha_{ij}] \in \mathrm{Mat}_{n\times m}(\mathbb{F})$ define the *transpose* $A^t = [\beta_{ij}] \in \mathrm{Mat}_{m\times n}(\mathbb{F})$ by $\beta_{ij} = \alpha_{ji}$. Thus A^t is gotten from A by reflecting in the diagonal entries.
- (a) Show that $A \to A^t$ is a linear map which is also an isomorphism whose inverse is given by $B \to B^t$.
- (b) If $A \in \mathrm{Mat}_{n\times m}(\mathbb{F})$ and $B \in \mathrm{Mat}_{m\times n}(\mathbb{F})$ show that $(AB)^t = B^t A^t$.
- (c) Show that if $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ is invertible, i.e., there exists $A^{-1} \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ such that
$$AA^{-1} = A^{-1}A = 1_{\mathbb{F}^n},$$
then A^t is also invertible and $(A^t)^{-1} = (A^{-1})^t$.

9. Matrix Representations Revisited

While the number of elements in a basis is always the same, there is unfortunately not a clear choice of a basis for many abstract vector spaces. This necessitates a discussion on the relationship between expansions of vectors in different bases.

Using the idea of isomorphism in connection with a choice of basis we can streamline the procedure for expanding vectors and constructing the matrix representation of a linear map.

Fix a linear map $L : V \to W$ and bases $e_1, ..., e_m$ for V and $f_1, ..., f_n$ for W. One can then encode all of the necessary information in a diagram of maps

$$\begin{array}{ccc} V & \xrightarrow{L} & W \\ \uparrow & & \uparrow \\ \mathbb{F}^m & \xrightarrow{[L]} & \mathbb{F}^n \end{array}$$

In this diagram the top horizontal arrow represents L and the bottom horizontal arrow represents the matrix for L interpreted as a linear map $[L] : \mathbb{F}^m \to \mathbb{F}^n$. The two vertical arrows are the basis isomorphisms defined by the choices of bases for V and W, i.e.,

$$\begin{array}{rcl} \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix} & : & \mathbb{F}^m \to V, \\ \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} & : & \mathbb{F}^n \to W. \end{array}$$

Thus we have the formulae relating L and $[L]$

$$\begin{array}{rcl} L & = & \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} \circ [L] \circ \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix}^{-1}, \\ [L] & = & \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix}^{-1} \circ L \circ \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix}. \end{array}$$

Note that a basis isomorphism

$$\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} : \mathbb{F}^m \to \mathbb{F}^m$$

is a matrix

$$\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \in \mathrm{Mat}_{m\times m}(\mathbb{F})$$

provided we write the vectors $x_1, ..., x_m$ as column vectors. As such, the map can be inverted using the standard matrix inverse. That said, it is not an easy problem to invert matrices or linear maps in general.

It is important to be aware of the fact that different bases will yield different matrix representations. To see what happens abstractly let us assume that we have two bases $x_1, ..., x_n$ and $y_1, ..., y_n$ for a vector space V. If we think of $x_1, ..., x_n$ as a basis for the domain and $y_1, ..., y_n$ as a basis for the image, then the identity map $1_V : V \to V$ has a matrix representation that is computed via

$$\begin{aligned}\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} &= \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} \begin{bmatrix} \beta_{11} & \cdots & \beta_{1n} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nn} \end{bmatrix} \\ &= \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} B.\end{aligned}$$

The matrix B, being the matrix representation for an isomorphism, is itself invertible and we see that by multiplying by B^{-1} on the right we obtain

$$\begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} B^{-1}.$$

This is the matrix representation for $1_V^{-1} = 1_V$ when we switch the bases around. Differently stated we have

$$\begin{aligned} B &= \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix}^{-1} \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}, \\ B^{-1} &= \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^{-1} \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix}. \end{aligned}$$

We now check what happens to a vector $x \in V$

$$\begin{aligned} x &= \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \\ &= \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} \begin{bmatrix} \beta_{11} & \cdots & \beta_{1n} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nn} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}. \end{aligned}$$

Thus, if we know the coordinates for x with respect to $x_1, ..., x_n$, then we immediately obtain the coordinates for x with respect to $y_1, ..., y_n$ by changing

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

to

$$\begin{bmatrix} \beta_{11} & \cdots & \beta_{1n} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nn} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}.$$

We can evidently also go backwards using the inverse B^{-1} rather than B.

EXAMPLE 24. *In* $\mathbb{F}^2$ *let* e_1, e_2 *be the standard basis and* $y_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $y_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$. *Then* B_1^{-1} *is easily found using*

$$\begin{aligned} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} y_1 & y_2 \end{bmatrix} \\ &= \begin{bmatrix} e_1 & e_2 \end{bmatrix} B_1^{-1} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} B_1^{-1} \\ &= B_1^{-1} \end{aligned}$$

B_1 *itself requires solving*

$$\begin{aligned} \begin{bmatrix} e_1 & e_2 \end{bmatrix} &= \begin{bmatrix} y_1 & y_2 \end{bmatrix} B_1, \text{ or} \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} B_1. \end{aligned}$$

Thus

$$\begin{aligned} B_1 &= \begin{bmatrix} y_1 & y_2 \end{bmatrix}^{-1} \\ &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} \\ &= \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

EXAMPLE 25. *In* $\mathbb{F}^2$ *let* $x_1 = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$, $x_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ *and* $y_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $y_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$. *Then* B_2 *is found by*

$$\begin{aligned} B_2 &= \begin{bmatrix} y_1 & y_2 \end{bmatrix}^{-1} \begin{bmatrix} x_1 & x_2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 2 & 0 \\ -1 & 1 \end{bmatrix} \end{aligned}$$

and

$$B_2^{-1} = \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 1 \end{bmatrix}.$$

Recall that we know

$$\begin{aligned} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} &= \alpha e_1 + \beta e_2 \\ &= \frac{\alpha - \beta}{2} x_1 + \frac{\alpha + \beta}{2} x_2 \\ &= (\alpha - \beta) y_1 + \beta y_2. \end{aligned}$$

Thus it should be true that

$$\begin{bmatrix} (\alpha - \beta) \\ \beta \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} \frac{\alpha-\beta}{2} \\ \frac{\alpha+\beta}{2} \end{bmatrix},$$

which indeed is the case.

Now suppose that we have a linear operator $L : V \to V$. It will have matrix representations with respect to both bases. First let us do this in a diagram of maps

$$\begin{array}{ccc} \mathbb{F}^n & \xrightarrow{A_1} & \mathbb{F}^n \\ \downarrow & & \downarrow \\ V & \xrightarrow{L} & V \\ \uparrow & & \uparrow \\ \mathbb{F}^n & \xrightarrow{A_2} & \mathbb{F}^n \end{array}$$

Here the downward arrows come form the isomorphism

$$\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} : \mathbb{F}^n \to V$$

and the upward arrows are

$$\begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} : \mathbb{F}^n \to V.$$

Thus

$$\begin{aligned} L &= \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} A_1 \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^{-1} \\ L &= \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} A_2 \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix}^{-1} \end{aligned}$$

We wish to discover what the relationship between A_1 and A_2 is. To figure this out we simply note that

$$\begin{aligned} \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} A_1 \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^{-1} &= L \\ &= \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} A_2 \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix}^{-1}. \end{aligned}$$

Hence

$$\begin{aligned} A_1 &= \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^{-1} \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} A_2 \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix}^{-1} \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \\ &= B^{-1} A_2 B. \end{aligned}$$

To memorize this formula keep in mind that B transforms from the $x_1, ..., x_n$ basis to the $y_1, ..., y_n$ basis while B^{-1} reverses this process. The matrix product $B^{-1}A_2B$ then indicates that starting from the right we have gone from $x_1, ..., x_n$ to $y_1, ..., y_n$ then used A_2 on the $y_1, ..., y_n$ basis and then transformed back from the $y_1, ..., y_n$ basis to the $x_1, ..., x_n$ basis in order to find what A_1 does with respect to the $x_1, ..., x_n$ basis.

Example 26. *We have the representations for*

$$L = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$$

with respect to the three bases we just studied earlier in "Linear Maps as Matrices"

$$\begin{bmatrix} L(e_1) & L(e_2) \end{bmatrix} = \begin{bmatrix} e_1 & e_2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix},$$

$$\begin{bmatrix} L(x_1) & L(x_2) \end{bmatrix} = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix},$$

$$\begin{bmatrix} L(y_1) & L(y_2) \end{bmatrix} = \begin{bmatrix} y_1 & y_2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

Using the changes of basis calculated above we can check the following relationships

$$\begin{aligned}\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} &= B_1 \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} B_1^{-1} \\ &= \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\end{aligned}$$

$$\begin{aligned}\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} &= B_2 \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} B_2^{-1} \\ &= \begin{bmatrix} 2 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 1 \end{bmatrix}\end{aligned}$$

One can more generally consider $L : V \to W$ and see what happens if we change bases in both V and W. The analysis is similar as long as we keep in mind that there are four bases in play. The key diagram evidently looks like

$$\begin{array}{ccc} \mathbb{F}^m & \xrightarrow{A_1} & \mathbb{F}^n \\ \downarrow & & \downarrow \\ V & \xrightarrow{L} & W \\ \uparrow & & \uparrow \\ \mathbb{F}^m & \xrightarrow{A_2} & \mathbb{F}^n \end{array}$$

One of the goals in the study of linear operators or just square matrices is to find a suitable basis that makes the matrix representation as simple as possible. This is a rather complicated theory which the rest of the book will try to uncover.

9.1. Exercises.

(1) Let $V = \{\alpha \cos(t) + \beta \sin(t) : \alpha, \beta \in \mathbb{C}\}$.
   (a) Show that $\cos(t), \sin(t)$ and $\exp(it), \exp(-it)$ both form a basis for V.
   (b) Find the change of basis matrix.
   (c) Find the matrix representation of $D : V \to V$ with respect to both bases and check that the change of basis matrix gives the correct relationship between these two matrices.

(2) Let
$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} : \mathbb{R}^2 \to \mathbb{R}^2$$
and consider the basis
$$x_1 = \begin{bmatrix} 1 \\ -1 \end{bmatrix}, x_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$
   (a) Compute the matrix representation of A with respect to x_1, x_2.
   (b) Compute the matrix representation of A with respect to $\frac{1}{\sqrt{2}}x_1$, $\frac{1}{\sqrt{2}}x_2$.
   (c) Compute the matrix representation of A with respect to x_1, $x_1 + x_2$.

(3) Let e_1, e_2 be the standard basis for $\mathbb{C}^2$ and consider the two real bases e_1, e_2, ie_1, ie_2 and e_1, ie_1, e_2, ie_2. If $\lambda = \alpha + i\beta$ is a complex number compute the real matrix representations for $\lambda 1_{\mathbb{C}^2}$ with respect to both bases. Show that the two matrices are related via the change of basis formula.

(4) If $x_1, ..., x_n$ is a basis for V, then what is the change of basis matrix from $x_1, ..., x_n$ to $x_n, ..., x_1$? How does the matrix representation of an operator on V change with this change of basis?
(5) Let $L : V \to V$ be a linear operator, $p(t) \in \mathbb{F}[t]$ a polynomial and $K : V \to W$ an isomorphism. Show that
$$p\left(K \circ L \circ K^{-1}\right) = K \circ p(L) \circ K^{-1}.$$
(6) Let A be a permutation matrix. Will the matrix representation for A still be a permutation matrix in a different basis?
(7) What happens to the matrix representation of a linear map if the change of basis matrix is a permutation matrix?

10. Subspaces

A nonempty subset $M \subset V$ of a vector space V is said to be a *subspace* if it is closed under addition and scalar multiplication:

$$\begin{aligned} x, y \in M &\implies x + y \in M, \\ \alpha \in \mathbb{F} \text{ and } x \in M &\implies \alpha x \in M \end{aligned}$$

Note that since $M \neq \emptyset$ we can find $x \in M$, this means that $0 = 0 \cdot x \in M$. It is clear that subspaces become vector spaces in their own right and this without any further checking of the axioms.

The two properties for a subspace can be combined into one property as follows

$$\alpha_1, \alpha_2 \in \mathbb{F} \text{ and } x_1, x_2 \in M \implies \alpha_1 x_1 + \alpha_2 x_2 \in M$$

Any vector space always has two *trivial subspaces*, namely, V and $\{0\}$. Some more interesting examples come below.

EXAMPLE 27. *Let M_i be the i^{th} coordinate axis in $\mathbb{F}^n$, i.e., the set consisting of the vectors where all but the i^{th} coordinate are zero. Thus*

$$M_i = \{(0, ..., 0, \alpha_i, 0, ..., 0) : \alpha_i \in \mathbb{F}\}.$$

EXAMPLE 28. *Polynomials in $\mathbb{F}[t]$ of degree $\leq n$ form a subspace denoted P_n.*

EXAMPLE 29. *Continuous functions $C^0([a,b], \mathbb{R})$ on an interval $[a,b] \subset \mathbb{R}$ is evidently a subspace of* $\text{Func}([a,b], \mathbb{R})$. *Likewise the space of functions that have derivatives of all orders is a subspace*

$$C^\infty([a,b], \mathbb{R}) \subset C^0([a,b], \mathbb{R}).$$

If we regard polynomials as functions on $[a,b]$ then we have that

$$\mathbb{R}[t] \subset C^\infty([a,b], \mathbb{R}).$$

EXAMPLE 30. *Solutions to simple types of equations often form subspaces:*

$$\left\{3\alpha_1 - 2\alpha_2 + \alpha_3 = 0 : (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{F}^3\right\}.$$

However something like

$$\left\{3\alpha_1 - 2\alpha_2 + \alpha_3 = 1 : (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{F}^3\right\}$$

does not yield a subspace as it doesn't contain the origin.

Example 31. *There are other interesting examples of subspaces of* $C^{\infty}(\mathbb{R},\mathbb{C})$. *If* $\omega>0$ *is some fixed number then we consider*

$$C_{\omega}^{\infty}(\mathbb{R},\mathbb{C})=\{f\in C^{\infty}(\mathbb{R},\mathbb{C}):f(t)=f(t+\omega)\text{ for all }t\in\mathbb{R}\}.$$

These are the periodic functions *with period* ω. *Note that*

$$\begin{aligned} f(t) &= \exp(i2\pi t/\omega) \\ &= \cos(2\pi t/\omega)+i\sin(2\pi t/\omega) \end{aligned}$$

is an example of a periodic function.

Subspaces allow for a generalized type of calculus. That is, we can "add" and "multiply" them to form other subspaces. However, it isn't possible to find inverses for either operation. If $M,N\subset V$ are subspaces then we can form two new subspaces, the *sum* and the *intersection*:

$$\begin{aligned} M+N &= \{x+y:x\in M\text{ and }y\in N\}, \\ M\cap N &= \{x:x\in M\text{ and }x\in N\}. \end{aligned}$$

It is certainly true that both of these sets contain the origin. The intersection is most easily seen to be a subspace so let us check the sum. If $\alpha\in\mathbb{F}$ and $x\in M$, $y\in N$, then we have $\alpha x\in M$, $\alpha y\in N$ so

$$\alpha x+\alpha y=\alpha(x+y)\in M+N.$$

In this way we see that $M+N$ is closed under scalar multiplication. To check that it is closed under addition is equally simple.

We can think of $M+N$ as addition of subspaces and $M\cap N$ as a kind of multiplication. The element that acts as zero for addition is the trivial subspace $\{0\}$ as $M+\{0\}=M$, while $M\cap V=M$ implies that V is the identity for intersection. Beyond this, it is probably not that useful to think of these subspace operations as arithmetic operations, e.g, the distributive law does not hold.

If $S\subset V$ is a subset of a vector space, then the *span* of S is defined as

$$\operatorname{span}(S)=\bigcap_{S\subset M\subset V}M,$$

where $M\subset V$ is always a subspace of V. Thus the span is the intersection of all subspaces that contain S. This is a subspace of V and must in fact be the smallest subspace containing S. We immediately get the following elementary properties.

Proposition 2. *Let* V *be a vector space and* $S,T\subset V$ *subsets.*

(1) *If* $S\subset T$, *then* $\operatorname{span}(S)\subset\operatorname{span}(T)$.
(2) *If* $M\subset V$ *is a subspace, then* $\operatorname{span}(M)=M$.
(3) $\operatorname{span}(\operatorname{span}(S))=\operatorname{span}(S)$.
(4) $\operatorname{span}(S)=\operatorname{span}(T)$ *if and only if* $S\subset\operatorname{span}(T)$ *and* $T\subset\operatorname{span}(S)$.

Proof. The first property is obvious from the definition of span.

To prove the second property we first note that we always have that $S\subset\operatorname{span}(S)$. In particular $M\subset\operatorname{span}(M)$. On the other hand as M is a subspace that contains M it must also follow that $\operatorname{span}(M)\subset M$.

The third property follows from the second as $\operatorname{span}(S)$ is a subspace.

To prove the final property we first observe that if $\operatorname{span}(S)\subset\operatorname{span}(T)$, then $S\subset\operatorname{span}(T)$. Thus it is clear that if $\operatorname{span}(S)=\operatorname{span}(T)$, then $S\subset\operatorname{span}(T)$ and $T\subset\operatorname{span}(S)$. Conversely we have from the first and third properties that if $S \subset \operatorname{span}(T)$, then $\operatorname{span}(S) \subset \operatorname{span}(\operatorname{span}(T)) = \operatorname{span}(T)$. This shows that if $S \subset \operatorname{span}(T)$ and $T \subset \operatorname{span}(S)$, then $\operatorname{span}(S) = \operatorname{span}(T)$. □

The following lemma gives an alternate and very convenient description of the span.

LEMMA 6. (Characterization of $\operatorname{span}(M)$) *Let $S \subset V$ be a nonempty subset of M. Then* $\operatorname{span}(S)$ *consists of all linear combinations of vectors in S.*

PROOF. Let C be the set of all linear combinations of vectors in S. Since $\operatorname{span}(S)$ is a subspace it must be true that $C \subset \operatorname{span}(S)$. Conversely if $x, y \in C$, then we note that also $\alpha x + \beta y$ is a linear combination of vectors from S. Thus $\alpha x + \beta y \in C$ and hence C is a subspace. This means that $\operatorname{span}(S) \subset C$. □

We say that M and N have *trivial intersection* provided $M \cap N = \{0\}$, i.e., their intersection is the trivial subspace. We say that M and N are *transversal* provided $M + N = V$. Both concepts are important in different ways. Transversality also plays a very important role in the more advanced subject of differentiable topology. Differentiable topology is the study of maps and spaces through a careful analysis of differentiable functions.

If we combine the two concepts of transversality and trivial intersection we arrive at another important idea. Two subspaces are said to be *complementary* if they are transversal and have trivial intersection.

LEMMA 7. *Two subspaces $M, N \subset V$ are complementary if and only if each vector $z \in V$ can be written as $z = x + y$, where $x \in M$ and $y \in N$ in one and only one way.*

Before embarking on the proof let us explain the use of "one and only one". The idea is first that z can be written like that in (at least) one way, the second part is that this is the only way in which to do it. In other words having found x and y so that $z = x + y$ there can't be any other ways in which to decompose z into a sum of elements from M and N.

PROOF. First assume that M and N are complementary. Since $V = M + N$ we know that $z = x + y$ for some $x \in M$ and $y \in N$. If we have

$$x_1 + y_1 = z = x_2 + y_2$$

where $x_1, x_2 \in M$ and $y_1, y_2 \in N$, then by moving each of x_2 and y_1 to the other side we get

$$M \ni x_1 - x_2 = y_2 - y_1 \in N.$$

This means that

$$x_1 - x_2 = y_2 - y_1 \in M \cap N = \{0\}$$

and hence that

$$x_1 - x_2 = y_2 - y_1 = 0.$$

Thus $x_1 = x_2$ and $y_1 = y_2$ and we have established that z has the desired unique decomposition.

Conversely assume that any $z = x + y$, for unique $x \in M$ and $y \in N$. First we see that this means $V = M + N$. To see that $M \cap N = \{0\}$ we simply select $z \in M \cap N$. Then $z = z + 0 = 0 + z$ where $z \in M, 0 \in N$ and $0 \in M, z \in N$. Since such decompositions are assumed to be unique we must have that $z = 0$ and hence $M \cap N = \{0\}$. □

When we have two complementary subsets $M, N \subset V$ we also say that V is a *direct sum* of M and N and we write this symbolically as $V = M \oplus N$. The special sum symbol indicates that indeed $V = M + N$ and also that the two subspaces have trivial intersection. Using what we have learned so far about subspaces we get a result that is often quite useful.

COROLLARY 3. *Let $M, N \subset V$ be subspaces. If $M \cap N = \{0\}$, then*

$$M + N = M \oplus N$$

and

$$\dim(M + N) = \dim(M) + \dim(N)$$

We also have direct sum decompositions for more than two subspaces. If $M_1, ..., M_k \subset V$ are subspaces we say that V is a direct sum of $M_1, ..., M_k$ and write

$$V = M_1 \oplus \cdots \oplus M_k$$

provided any vector $z \in V$ can be decomposed as

$$\begin{aligned} z &= x_1 + \cdots + x_k, \\ x_1 &\in M_1, ..., x_k \in M_k \end{aligned}$$

in one and only one way.

Here are some examples of direct sums.

EXAMPLE 32. *The prototypical example of a direct sum comes from the plane. Where $V = \mathbb{R}^2$ and*

$$M = \{(x, 0) : x \in \mathbb{R}\}$$

is the 1^{st} coordinate axis and

$$N = \{(0, y) : y \in \mathbb{R}\}$$

the 2^{nd} coordinate axis.

EXAMPLE 33. *Direct sum decompositions are by no means unique, as can be seen using $V = \mathbb{R}^2$ and*

$$M = \{(x, 0) : x \in \mathbb{R}\}$$

and

$$N = \{(y, y) : y \in \mathbb{R}\}$$

the diagonal. We can easily visualize and prove that the intersection is trivial. As for transversality just observe that

$$(x, y) = (x - y, 0) + (y, y).$$

EXAMPLE 34. *We also have the direct sum decomposition*

$$\mathbb{F}^n = M_1 \oplus \cdots \oplus M_n,$$

where

$$M_i = \{(0, ..., 0, \alpha_i, 0, ..., 0) : \alpha_i \in \mathbb{F}\}.$$

EXAMPLE 35. *Here is a more abstract example that imitates the first. Partition the set*

$$\{1,2,...,n\} = \{i_1,...,i_k\} \cup \{j_1,...,j_{n-k}\}$$

into two complementary sets. Let

$$\begin{aligned} V &= \mathbb{F}^n, \\ M &= \left\{(\alpha_1,...,\alpha_n) \in \mathbb{F}^n : \alpha_{j_1} = \cdots = \alpha_{j_{n-k}} = 0\right\}, \\ N &= \{(\alpha_1,...,\alpha_n) : \alpha_{i_1} = \cdots = \alpha_{i_k} = 0\}. \end{aligned}$$

Thus

$$\begin{aligned} M &= M_{i_1} \oplus \cdots \oplus M_{i_k}, \\ N &= M_{j_1} \oplus \cdots \oplus M_{j_{n-k}}, \end{aligned}$$

and $\mathbb{F}^n = M \oplus N$. *Note that* M *is isomorphic to* $\mathbb{F}^k$ *and* N *to* $\mathbb{F}^{n-k}$, *but with different indices for the axes. Thus we have the more or less obvious decomposition:* $\mathbb{F}^n = \mathbb{F}^k \times \mathbb{F}^{n-k}$. *Note, however, that when we use* $\mathbb{F}^k$ *rather than* M *we do not think of* $\mathbb{F}^k$ *as a subspace of* $\mathbb{F}^n$ *as vectors in* $\mathbb{F}^k$ *are* k*-tuples of the form* $(\alpha_{i_1},...,\alpha_{i_k})$. *Thus there is a subtle difference between writing* $\mathbb{F}^n$ *as a product or direct sum.*

EXAMPLE 36. *Another very interesting decomposition is that of separating functions into odd and even parts. Recall that a function* $f : \mathbb{R} \to \mathbb{R}$ *is said to be odd, respectively even, if* $f(-t) = -f(t)$, *respectively* $f(-t) = f(t)$. *Note that constant functions are even, while functions whose graphs are lines through the origin are odd. We denote the subsets of odd and even functions by* $\mathrm{Func}^{\mathrm{odd}}(\mathbb{R},\mathbb{R})$ *and* $\mathrm{Func}^{\mathrm{ev}}(\mathbb{R},\mathbb{R})$. *It is easily seen that these subsets are subspaces. Also* $\mathrm{Func}^{\mathrm{odd}}(\mathbb{R},\mathbb{R}) \cap \mathrm{Func}^{\mathrm{ev}}(\mathbb{R},\mathbb{R}) = \{0\}$ *since only the zero function can be both odd and even. Finally any* $f \in \mathrm{Func}(\mathbb{R},\mathbb{R})$ *can be decomposed as follows*

$$\begin{aligned} f(t) &= f_{\mathrm{ev}}(t) + f_{\mathrm{odd}}(t), \\ f_{\mathrm{ev}}(t) &= \frac{f(t) + f(-t)}{2}, \\ f_{\mathrm{odd}}(t) &= \frac{f(t) - f(-t)}{2}. \end{aligned}$$

A specific example of such a decomposition is

$$\begin{aligned} e^t &= \cosh(t) + \sinh(t), \\ \cosh(t) &= \frac{e^t + e^{-t}}{2}, \\ \sinh(t) &= \frac{e^t - e^{-t}}{2}. \end{aligned}$$

If we consider complex valued functions $\mathrm{Func}(\mathbb{R},\mathbb{C})$ *we still have the same concepts of even and odd and also the desired direct sum decomposition. Here, another similar and very interesting decomposition is the Euler formula*

$$\begin{aligned} e^{it} &= \cos(t) + i\sin(t) \\ \cos(t) &= \frac{e^{it} + e^{-it}}{2}, \\ \sin(t) &= \frac{e^{it} - e^{-it}}{2i}. \end{aligned}$$

Some interesting questions come to mind with the definitions encountered here. What is the relationship between $\dim_{\mathbb{F}} M$ and $\dim_{\mathbb{F}} V$ for a subspace $M \subset V$? Do all subspaces have a complement? Are there some relationships between subspaces and linear maps?

At this point we can show that subspaces of finite dimensional vector spaces do have complements. This result will be used to prove several other important theorems in the chapter.

THEOREM 2. (Existence of Complements) *Let $M \subset V$ be a subspace and assume that $V = \operatorname{span}\{x_1, ..., x_n\}$. If $M \neq V$, then it is possible to choose $x_{i_1}, ..., x_{i_k}$ such that*

$$V = M \oplus \operatorname{span}\{x_{i_1}, ..., x_{i_k}\}$$

PROOF. Successively choose $x_{i_1}, ..., x_{i_k}$ such that

$$\begin{array}{rcl} x_{i_1} & \notin & M, \\ x_{i_2} & \notin & M + \operatorname{span}\{x_{i_1}\}, \\ & \vdots & \\ x_{i_k} & \notin & M + \operatorname{span}\left\{x_{i_1}, ..., x_{i_{k-1}}\right\}. \end{array}$$

This process can be continued until

$$V = M + \operatorname{span}\{x_{i_1}, ..., x_{i_k}\}$$

and since

$$\operatorname{span}\{x_1, ..., x_n\} = V$$

we know that this will happen for some $k \leq n$. It now only remains to be seen that

$$\{0\} = M \cap \operatorname{span}\{x_{i_1}, ..., x_{i_k}\}.$$

To check this suppose that

$$x \in M \cap \operatorname{span}\{x_{i_1}, ..., x_{i_k}\}$$

and write

$$x = \alpha_{i_1} x_{i_1} + \cdots + \alpha_{i_k} x_{i_k} \in M.$$

If $\alpha_{i_1} = \cdots = \alpha_{i_k} = 0$, there is nothing to worry about. Otherwise we can find the largest l so that $\alpha_{i_l} \neq 0$. Then

$$\frac{1}{\alpha_{i_l}} x = \frac{\alpha_{i_1}}{\alpha_{i_l}} x_{i_1} + \cdots + \frac{\alpha_{i_{l-1}}}{\alpha_{i_l}} x_{i_{l-1}} + x_{i_l} \in M$$

which implies the contradictory statement that

$$x_{i_l} \in M + \operatorname{span}\left\{x_{i_1}, ..., x_{i_{l-1}}\right\}.$$

□

This theorem shows that $\dim(M) \leq \dim(V)$ as long as we know that both M and V are finite dimensional. To see this, first select a basis $y_1, ..., y_l$ for M and then $x_{i_1}, ..., x_{i_k}$ as a basis for a complement to M using a basis $x_1, ..., x_n$ for V. Putting these two bases together will then yield a basis $y_1, ..., y_l, x_{i_1}, ..., x_{i_k}$ for V. Thus $l + k = \dim(V)$, which shows that $l = \dim(M) \leq \dim(V)$. Thus the important point lies in showing that M is finite dimensional. We will establish this in the next section.

10.1. Exercises.

(1) Show that
$$S=\left\{L:\mathbb{R}^3\to\mathbb{R}^2:L(1,2,3)=0,\ \ (2,3)=L(x)\ \text{ for some } x\in\mathbb{R}^2\right\}$$
is not a subspace of $\hom\left(\mathbb{R}^3,\mathbb{R}^2\right)$. How many linear maps are there in S?

(2) Find a one dimensional complex subspace $M\subset\mathbb{C}^2$ such that $\mathbb{R}^2\cap M=\{0\}$.

(3) Let $L:V\to W$ be a linear map and $N\subset W$ a subspace. Show that
$$L^{-1}(N)=\{x\in V:L(x)\in N\}$$
is a subspace of V.

(4) Is it true that subspaces satisfy the distributive law
$$M\cap(N_1+N_2)=M\cap N_1+M\cap N_2?$$

(5) Show that if V is finite dimensional, then $\hom(V,V)$ is a direct sum of the two subspaces $M=\operatorname{span}\{1_V\}$ and $N=\{L:\operatorname{tr}L=0\}$.

(6) Show that $\mathrm{Mat}_{n\times n}(\mathbb{R})$ is the direct sum of the following three subspaces (you also have to show that they are subspaces)
$$\begin{aligned} I &= \operatorname{span}\{1_{\mathbb{R}^n}\},\\ S_0 &= \left\{A:\operatorname{tr}A=0\text{ and }A^t=A\right\},\\ A &= \left\{A:A^t=-A\right\}. \end{aligned}$$

(7) Let $M_1,...,M_k\subsetneq V$ be proper subspaces of a finite dimensional vector space and $N\subset V$ a subspace. Show that if $N\subset M_1\cup\cdots\cup M_k$, then $N\subset M_i$ for some i. Conclude that if N is not contained in any of the M_is, then we can find $x\in N$ such that $x\notin M_1,...,x\notin M_k$.

(8) Assume that $V=N\oplus M$ and that $x_1,...,x_k$ form a basis for M while $x_{k+1},...,x_n$ form a basis for N. Show that $x_1,...,x_n$ is a basis for V.

(9) An *affine subspace* $A\subset V$ of a vector space is a subspace such that *affine linear combinations* of vectors in A lie in A, i.e., if $\alpha_1+\cdots+\alpha_n=1$ and $x_1,...,x_n\in A$, then $\alpha_1x_1+\cdots+\alpha_nx_n\in A$.
   (a) Show that A is an affine subspace if and only if there is a point $x_0\in V$ and a subspace $M\subset V$ such that
   $$A=x_0+M=\{x_0+x:x\in M\}.$$
   (b) Show that A is an affine subspace if and only if there is a subspace $M\subset V$ with the properties: 1) if $x,y\in A$, then $x-y\in M$ and 2) if $x\in A$ and $z\in M$, then $x+z\in A$.
   (c) Show that the subspaces constructed in parts a. and b. are equal.
   (d) Show that the set of monic polynomials of degree n in P_n, i.e., the coefficient in front of t^n is 1, is an affine subspace with $M=P_{n-1}$.

(10) Show that the two spaces below are subspaces of $C^\infty_{2\pi}(\mathbb{R},\mathbb{R})$ that are not equal to each other
$$\begin{aligned} V_1 &= \{b_1\sin(t)+b_2\sin(2t)+b_3\sin(3t):b_1,b_2,b_3\in\mathbb{R}\},\\ V_2 &= \left\{b_1\sin(t)+b_2\sin^2(t)+b_3\sin^3(t):b_1,b_2,b_3\in\mathbb{R}\right\}. \end{aligned}$$

(11) Let $T\subset C^\infty_{2\pi}(\mathbb{R},\mathbb{C})$ be the space of complex trigonometric polynomials, i.e., the space of functions of the form
$$a_0+a_1\cos t+\cdots+a_k\cos^k t+b_1\sin t+\cdots+b_k\sin^k t,$$

where $a_0, ..., a_k, b_1, ..., b_k \in \mathbb{C}$.

(a) Show that T is also equal to the space of functions of the form

$$\alpha_0 + \alpha_1 \cos t + \cdots + \alpha_k \cos(kt) + \beta_1 \sin t + \cdots + \beta_k \sin(kt)$$

where $\alpha_0, ..., \alpha_k, \beta_1, ..., \beta_k \in \mathbb{C}$.

(b) Show that T is also equal to the space of function of the form

$$c_{-k} \exp(-ikt) + \cdots + c_{-1} \exp(-it) + c_0 + c_1 \exp(it) + \cdots + c_k \exp(ikt),$$

where $c_{-k}, ..., c_k \in \mathbb{C}$.

(12) If $M \subset V$ and $N \subset W$ are subspaces, then $M \times N \subset V \times W$ is also a subspace.

(13) If $A \in \text{Mat}_{n \times n}(\mathbb{F})$ has $\text{tr}(A) = 0$, show that

$$A = A_1 B_1 - B_1 A_1 + \cdots + A_m B_m - B_m A_m$$

for suitable $A_i, B_i \in \text{Mat}_{n \times n}(\mathbb{F})$. Hint: Show that

$$M = \text{span}\{XY - YX : X, Y \in \text{Mat}_{n \times n}(\mathbb{F})\}$$

has dimension $n^2 - 1$ by exhibiting a suitable basis.

(14) Let $L : V \to W$ be a linear map and consider the graph

$$G_L = \{(x, L(x)) : x \in V\} \subset V \times W.$$

(a) Show that G_L is a subspace.

(b) Show that the map $V \to G_L$ that sends x to $(x, L(x))$ is an isomorphism.

(c) Show that L is one-to-one if and only if the projection $P_W : V \times W \to W$ is one-to-one when restricted to G_L.

(d) Show that L is onto if and only if the projection $P_W : V \times W \to W$ is onto when restricted to G_L.

(e) Show that a subspace $N \subset V \times W$ is the graph of a linear map $K : V \to W$ if and only if the projection $P_V : V \times W \to V$ is an isomorphism when restricted to N.

(f) Show that a subspace $N \subset V \times W$ is the graph of a linear map $K : V \to W$ if and only if $V \times W = N \oplus (\{0\} \times W)$.

11. Linear Maps and Subspaces

Linear maps generate a lot of interesting subspaces and can also be used to understand certain important aspects of subspaces. Conversely the subspaces associated to a linear map give us crucial information as to whether the map is one-to-one or onto.

Let $L : V \to W$ be a linear map between vector spaces. The *kernel* or *nullspace* of L is

$$\ker(L) = \text{N}(L) = \{x \in V : L(x) = 0\} = L^{-1}(0).$$

The *image* or *range* of L is

$$\text{im}(L) = \text{R}(L) = L(V) = \{y \in W : y = L(x) \text{ for some } x \in V\}.$$

Both of these spaces are subspaces.

Lemma 8. $\ker(L)$ *is a subspace of* V *and* $\text{im}(L)$ *is a subspace of* W.

Proof. Assume that $\alpha_1, \alpha_2 \in \mathbb{F}$ and that $x_1, x_2 \in \ker(L)$, then

$$L(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 L(x_1) + \alpha_2 L(x_2) = 0.$$

More generally, if we only assume $x_1, x_2 \in V$, then we have

$$\alpha_1 L(x_1) + \alpha_2 L(x_2) = L(\alpha_1 x_1 + \alpha_2 x_2) \in \operatorname{im}(L).$$

This proves the claim. □

The same proof shows that $L(M) = \{L(x) : x \in M\}$ is a subspace of W when M is a subspace of V.

Lemma 9. *L is one-to-one if and only if* $\ker(L) = \{0\}$.

Proof. We know that $L(0 \cdot 0) = 0 \cdot L(0) = 0$, so if L is one-to-one we have that $L(x) = 0 = L(0)$ implies that $x = 0$. Hence $\ker(L) = \{0\}$. Conversely assume that $\ker(L) = \{0\}$. If $L(x_1) = L(x_2)$, then linearity of L tells us that $L(x_1 - x_2) = 0$. Then $\ker(L) = \{0\}$ implies $x_1 - x_2 = 0$, which shows that $x_1 = x_2$. □

If we have a direct sum decomposition $V = M \oplus N$, then we can construct what is called the *projection* of V onto M along N. The map $E : V \to V$ is defined as follows. For $z \in V$ we write $z = x + y$ for unique $x \in M$, $y \in N$ and define

$$E(z) = x.$$

Thus $\operatorname{im}(E) = M$ and $\ker(E) = N$. Note that

$$(1_V - E)(z) = z - x = y.$$

This means that $1_V - E$ is the projection of V onto N along M. So the decomposition $V = M \oplus N$, gives us similar decomposition of 1_V using these two projections: $1_V = E + (1_V - E)$.

Using all of the examples of direct sum decompositions we get several examples of projections. Note that each projection E onto M leads in a natural way to a linear map $P : V \to M$. This map has the same definition $P(z) = P(x + y) = x$, but it is not E as it is not defined as an operator $V \to V$. It is perhaps pedantic to insist on having different names but note that as it stands we are not allowed to compose P with itself as it doesn't map into V.

We are now ready to establish several extremely important results relating linear maps, subspaces and dimensions.

Recall that complements to a fixed subspace are usually not unique, however, they do have the same dimension as the next result shows.

Lemma 10. (Uniqueness of Complements) *If $V = M_1 \oplus N = M_2 \oplus N$, then M_1 and M_2 are isomorphic.*

Proof. Let $P : V \to M_2$ be the projection whose kernel is N. We contend that the map $P|_{M_1} : M_1 \to M_2$ is an isomorphism. The kernel can be computed as

$$\begin{aligned} \ker(P|_{M_1}) &= \{x \in M_1 : P(x) = 0\} \\ &= \{x \in V_1 : P(x) = 0\} \cap M_1 \\ &= N \cap M_1 \\ &= \{0\}. \end{aligned}$$

To check that the map is onto select $x_2 \in M_2$. Next write $x_2 = x_1 + y_1$, where $x_1 \in M_1$ and $y_1 \in N$. Then

$$\begin{aligned} x_2 &= P(x_2) \\ &= P(x_1 + y_1) \\ &= P(x_1) + P(y_1) \\ &= P(x_1) \\ &= P|_{M_1}(x_1). \end{aligned}$$

This establishes the claim. □

THEOREM 3. (The Subspace Theorem) *Assume that V is finite dimensional and that $M \subset V$ is a subspace. Then M is finite dimensional and*

$$\dim_{\mathbb{F}} M \leq \dim_{\mathbb{F}} V.$$

Moreover if $V = M \oplus N$, then

$$\dim_{\mathbb{F}} V = \dim_{\mathbb{F}} M + \dim_{\mathbb{F}} N.$$

PROOF. If $M = V$ we are finished. Otherwise select a basis $x_1, ..., x_m$ for V. Then after using the basis to extract a complement to M in V we have that

$$\begin{aligned} V &= M \oplus \operatorname{span}\{x_{i_1}, ..., x_{i_k}\}, \\ V &= \operatorname{span}\{x_{j_1}, ..., x_{j_l}\} \oplus \operatorname{span}\{x_{i_1}, ..., x_{i_k}\}, \end{aligned}$$

where $k + l = m$ and

$$\{1, ..., n\} = \{j_1, ..., j_l\} \cup \{i_1, ..., i_k\}.$$

The previous result then shows that M and $\operatorname{span}\{x_{j_1}, ..., x_{j_l}\}$ are isomorphic. Thus

$$\dim_{\mathbb{F}} M = l < m.$$

In addition we see that if $V = M \oplus N$, then the previous result also shows that

$$\dim_{\mathbb{F}} N = k.$$

This proves the theorem. □

THEOREM 4. (The Dimension Formula) *Let V be finite dimensional and $L : V \to W$ a linear map, then* $\operatorname{im}(L)$ *is finite dimensional and*

$$\dim_{\mathbb{F}} V = \dim_{\mathbb{F}} \ker(L) + \dim_{\mathbb{F}} \operatorname{im}(L).$$

PROOF. We know that $\dim_{\mathbb{F}} \ker(L) \leq \dim_{\mathbb{F}} V$ and that it has a complement $N \subset V$ of dimension $k = \dim_{\mathbb{F}} V - \dim_{\mathbb{F}} \ker(L)$. Since $N \cap \ker(L) = \{0\}$ the linear map L must be one-to-one when restricted to N. Thus $L|_N : N \to \operatorname{im}(L)$ is an isomorphism. This proves the theorem. □

The number $\operatorname{nullity}(L) = \dim_{\mathbb{F}} \ker(L)$ is called the *nullity* of L and $\operatorname{rank}(L) = \dim_{\mathbb{F}} \operatorname{im}(L)$ is known as the *rank* of L.

COROLLARY 4. *If M is a subspace of V and* $\dim_{\mathbb{F}} M = \dim_{\mathbb{F}} V = n < \infty$, *then $M = V$.*

PROOF. If $M \neq V$ there must be a complement of dimension > 0. This gives us a contradiction with The Subspace Theorem. □

Corollary 5. *Assume that* $L : V \to W$ *and* $\dim_{\mathbb{F}} V = \dim_{\mathbb{F}} W = n < \infty$. *Then* L *is an isomorphism if either* $\text{nullity}(L) = 0$ *or* $\text{rank}(L) = n$.

Proof. The dimension theorem shows that if either $\text{nullity}(L) = 0$ or $\text{rank}(L) = n$, then also $\text{rank}(L) = n$ or $\text{nullity}(L) = 0$. Thus showing that L is an isomorphism. □

Knowing that the vector spaces are abstractly isomorphic can therefore help us in checking when a given linear map might be an isomorphism.

Many of these results are not true in infinite dimensional spaces. The differentiation operator $D : C^\infty(\mathbb{R}, \mathbb{R}) \to C^\infty(\mathbb{R}, \mathbb{R})$ is onto and has a kernel consisting of all constant functions. The multiplication operator $T : C^\infty(\mathbb{R}, \mathbb{R}) \to C^\infty(\mathbb{R}, \mathbb{R})$ on the other hand is one-to-one but is not onto as $T(f)(0) = 0$ for all $f \in C^\infty(\mathbb{R}, \mathbb{R})$.

Corollary 6. *If* $L : V \to W$ *is a linear map between finite dimensional spaces, then we can find bases* $e_1, ..., e_m$ *for* V *and* $f_1, ..., f_n$ *for* W *so that*

$$\begin{aligned} L(e_1) &= f_1, \\ &\vdots \\ L(e_k) &= f_k, \\ L(e_{k+1}) &= 0, \\ &\vdots \\ L(e_m) &= 0, \end{aligned}$$

where $k = \text{rank}(L)$.

Proof. Simply decompose $V = \ker(L) \oplus M$. Then choose a basis $e_1, ..., e_k$ for M and a basis $e_{k+1}, ..., e_m$ for $\ker(L)$. Combining these two bases gives us a basis for V. Then define $f_1 = L(e_1), ..., f_k = L(e_k)$. Since $L|_M : M \to \text{im}(L)$ is an isomorphism this implies that $f_1, ..., f_k$ form a basis for $\text{im}(L)$. We then get the desired basis for W by letting $f_{k+1}, ..., f_n$ be a basis for a complement to $\text{im}(L)$ in W. □

While this certainly gives the nicest possible matrix representation for L it isn't very useful. The complete freedom one has in the choice of both bases somehow also means that aside from the rank no other information is encoded in the matrix. The real goal will be to find the best matrix for a linear operator $L : V \to V$ with respect to one basis. In the general situation $L : V \to W$ we will have something more to say in case V and W are inner product spaces and the bases are orthonormal.

Finally it is worth mentioning that projections as a class of linear operators on V can be characterized in a surprisingly simple manner.

Theorem 5. (Characterization of Projections) *Projections all satisfy the functional relationship* $E^2 = E$. *Conversely any* $E : V \to V$ *that satisfies* $E^2 = E$ *is a projection.*

Proof. First assume that E is the prjection onto M along N coming from $V = M \oplus N$. If $z = x + y \in M \oplus N$, then

$$\begin{aligned} E^2(z) &= E(E(z)) \\ &= E(x) \\ &= E(z). \end{aligned}$$

Conversely assume that $E^2 = E$, then $E(x) = x$ provided $x \in \operatorname{im}(E)$. Thus we have

$$\begin{aligned} \operatorname{im}(E) \cap \ker(E) &= \{0\}, \text{ and} \\ \operatorname{im}(E) + \ker(E) &= \operatorname{im}(E) \oplus \ker(E) \end{aligned}$$

From The Dimension Theorem we also have that

$$\dim(\operatorname{im}(E)) + \dim(\ker(E)) = \dim(V).$$

This shows that $\operatorname{im}(E) + \ker(E)$ is a subspace of dimension $\dim(V)$ and hence all of V. Finally if we write $z = x + y$, $x \in \operatorname{im}(E)$ and $y \in \ker(E)$, then $E(x+y) = E(x) = x$, so E is the projection onto $\operatorname{im}(E)$ along $\ker(E)$. □

In this way we have shown that there is a natural identification between direct sum decompositions and projections, i.e., maps satisfying $E^2 = E$.

11.1. Exercises.

(1) Let $L, K : V \to V$ satisfy $L \circ K = 1_V$.
   (a) If V is finite dimensional, then $K \circ L = 1_V$.
   (b) If V is infinite dimensional give an example where $K \circ L \neq 1_V$.

(2) Let $M \subset V$ be a k-dimensional subspace of an n-dimensional vector space. Show that any isomorphism $L : M \to \mathbb{F}^k$ can be extended to an isomorphism $\hat{L} : V \to \mathbb{F}^n$, such that $\hat{L}|_M = L$. Here we have identified $\mathbb{F}^k$ with the subspace in $\mathbb{F}^n$ where the last $n - k$ coordinates are zero.

(3) Let $L : V \to W$ be a linear map.
   (a) If L has rank k show that it can be factored through $\mathbb{F}^k$, i.e., we can find $K_1 : V \to \mathbb{F}^k$ and $K_2 : \mathbb{F}^k \to W$ such that $L = K_2 K_1$.
   (b) Show that any matrix $A \in \operatorname{Mat}_{n\times m}(\mathbb{F})$ of rank k can be factored $A = BC$, where $B \in \operatorname{Mat}_{n\times k}(\mathbb{F})$ and $C \in \operatorname{Mat}_{k\times m}(\mathbb{F})$.
   (c) Conclude that any rank 1 matrix $A \in \operatorname{Mat}_{n\times m}(\mathbb{F})$ looks like

$$A = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \begin{bmatrix} \beta_1 & \cdots & \beta_m \end{bmatrix}.$$

(4) If $L_1 : V_1 \to V_2$ and $L_2 : V_2 \to V_3$ are linear show.
   (a) $\operatorname{im}(L_2 \circ L_1) \subset \operatorname{im}(L_2)$. In particular, if $L_2 \circ L_1$ is onto then so is L_2.
   (b) $\ker(L_1) \subset \ker(L_2 \circ L_1)$. In particular, if $L_2 \circ L_1$ is one-to-one then so is L_1.
   (c) Give an example where $L_2 \circ L_1$ is an isomorphism but L_1 and L_2 are not.
   (d) What happens in c. if we assume that the vector spaces all have the same dimension?
   (e) Show that

$$\begin{aligned} \operatorname{rank}(L_1) + \operatorname{rank}(L_2) - \dim(V_2) &\leq \operatorname{rank}(L_2 \circ L_1) \\ &\leq \min\{\operatorname{rank}(L_1), \operatorname{rank}(L_2)\}. \end{aligned}$$

   (f) Show that

$$\begin{aligned} \max\{\dim(\ker L_1), \dim(\ker L_2)\} &\leq \dim(\ker L_2 \circ L_1) \\ &\leq \dim(\ker L_1) + \dim(\ker L_2) \end{aligned}$$

(5) Let $L : V \to V$ be a linear operator on a finite dimensional vector space.
  (a) Show that $L = \lambda 1_V$ if and only if $L(x) \in \operatorname{span}\{x\}$ for all $x \in V$.
  (b) Show that $L = \lambda 1_V$ if and only if $L \circ K = K \circ L$ for all $K \in \hom(V, V)$.
  (c) Show that $L = \lambda 1_V$ if and only if $L \circ K = K \circ L$ for all isomorphisms $K : V \to V$.

(6) Show that two 2-dimensional subspaces of a 3-dimensional vector space must have a nontrivial intersection.

(7) *(Dimension formula for subspaces)* Let $M_1, M_2 \subset V$ be subspaces of a finite dimensional vector space. Show that

$$\dim(M_1 \cap M_2) + \dim(M_1 + M_2) = \dim(M_1) + \dim(M_2).$$

Conclude that if M_1 and M_2 are transverse then $M_1 \cap M_2$ has the "expected" dimension $(\dim(M_1) + \dim(M_2)) - \dim V$. Hint: Use the dimension formula on the linear map $L : M_1 \times M_2 \to V$ defined by $L(x_1, x_2) = x_1 - x_2$. Alternatively select a suitable basis for $M_1 + M_2$ by starting with a basis for $M_1 \cap M_2$.

(8) Let $M \subset V$ be a subspace. Show that the subset of $\hom_{\mathbb{F}}(V, W)$ consisting of maps that vanish on M is a subspace of dimension $\dim_{\mathbb{F}} W \cdot (\dim_{\mathbb{F}} V - \dim_{\mathbb{F}} M)$.

(9) Let $M_1, M_2 \subset V$ be subspaces of a finite dimensional vector space.
  (a) If $M_1 \cap M_2 = \{0\}$ and $\dim(M_1) + \dim(M_2) \geq \dim V$, then $V = M_1 \oplus M_2$.
  (b) If $M_1 + M_2 = V$ and $\dim(M_1) + \dim(M_2) \leq \dim V$, then $V = M_1 \oplus M_2$.

(10) Let $A \in \mathrm{Mat}_{n \times l}(\mathbb{F})$ and consider $L_A : \mathrm{Mat}_{l \times m}(\mathbb{F}) \to \mathrm{Mat}_{n \times m}(\mathbb{F})$ defined by $L_A(X) = AX$. Find the kernel and image of this map.

(11) Let

$$0 \overset{L_0}{\to} V_1 \overset{L_1}{\to} V_2 \overset{L_2}{\to} \cdots \overset{L_{n-1}}{\to} V_n \overset{L_n}{\to} 0$$

be a sequence of linear maps such that $\operatorname{im}(L_i) \subset \ker(L_{i+1})$ for $i = 0, 1, ..., n-1$. Note that L_0 and L_n are both the trivial linear maps with image $\{0\}$. Show that

$$\sum_{i=1}^{n} (-1)^i \dim V_i = \sum_{i=1}^{n} (-1)^i (\dim(\ker(L_i)) - \dim(\operatorname{im}(L_{i-1}))).$$

Hint: First try the case where $n = 2$.

(12) Show that the matrix

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

as a linear map satisfies $\ker(L) = \operatorname{im}(L)$.

(13) Show that

$$\begin{bmatrix} 0 & 0 \\ \alpha & 1 \end{bmatrix}$$

defines a projection for all $\alpha \in \mathbb{F}$. Compute the kernel and image.

(14) For any integer $n > 1$ give examples of linear maps $L : \mathbb{C}^n \to \mathbb{C}^n$ such that
  (a) $\mathbb{C}^n = \ker(L) \oplus \operatorname{im}(L)$ is a nontrivial direct sum decomposition.
  (b) $\{0\} \neq \ker(L) \subset \operatorname{im}(L)$.

(15) For $P_n \subset \mathbb{R}[t]$ and $2(n+1)$ points $a_0 < b_0 < a_1 < b_1 < \cdots < a_n < b_n$ consider the map $L : P_n \to \mathbb{R}^{n+1}$ defined by

$$L(p) = \begin{bmatrix} \frac{1}{b_0 - a_0} \int_{a_0}^{b_0} p(t)\, dt \\ \vdots \\ \frac{1}{b_n - a_n} \int_{a_n}^{b_n} p(t)\, dt \end{bmatrix}.$$

Show that L is a linear isomorphism.

12. Linear Independence

In this section we shall finally study the concepts of linear dependence and independence as well as how they tie in with kernels and images of linear maps.

Assume that $L : \mathbb{F}^m \to V$ is the linear map defined by $\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix}$. We say that $x_1, ..., x_m$ are *linearly independent* if $\ker(L) = \{0\}$. In other words $x_1, ..., x_m$ are linearly independent if

$$x_1\alpha_1 + \cdots + x_m\alpha_m = 0$$

implies that

$$\alpha_1 = \cdots = \alpha_m = 0.$$

The image of the map L can be identified with $\operatorname{span}\{x_1, ..., x_m\}$ and is described as

$$\{x_1\alpha_1 + \cdots + x_m\alpha_m : \alpha_1, ..., \alpha_m \in \mathbb{F}\}.$$

Note that $x_1, ..., x_m$ is a basis precisely when $\ker(L) = \{0\}$ and $\operatorname{span}\{x_1, ..., x_m\} = V$. The notions of kernel and image therefore enter our investigations of dimension in a very natural way. Finally we say that $x_1, ..., x_m$ are *linearly dependent* if they are not linearly independent, i.e., we can find $\alpha_1, ..., \alpha_m \in \mathbb{F}$ not all zero so that $x_1\alpha_1 + \cdots + x_m\alpha_m = 0$. In the next section we shall see how Gauss elimination helps us decide when a selection of vectors in $\mathbb{F}^n$ is linearly dependent or independent.

We give here a characterization of linear dependence that is quite useful in both concrete and abstract situations.

Lemma 11. (Characterization of Linear Dependence) *Let $x_1, ..., x_n \in V$. Then $x_1, ..., x_n$ is linearly dependent if and only if either $x_1 = 0$, or we can find a smallest $k \geq 2$ such that x_k is a linear combination of $x_1, ..., x_{k-1}$.*

Proof. First observe that if $x_1 = 0$, then $1x_1 = 0$ is a nontrivial linear combination. Next if

$$x_k = \alpha_1 x_1 + \cdots + \alpha_{k-1} x_{k-1},$$

then we also have a nontrivial linear combination

$$\alpha_1 x_1 + \cdots + \alpha_{k-1} x_{k-1} + (-1)\, x_k = 0.$$

Conversely, assume that $x_1, ..., x_n$ are linearly dependent. Select a nontrivial linear combination such that

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 0.$$

Then we can pick k so that $\alpha_k \neq 0$ and $\alpha_{k+1} = \cdots = \alpha_n = 0$. If $k = 1$, then we must have $x_1 = 0$ and we are finished. Otherwise

$$x_k = -\frac{\alpha_1}{\alpha_k} x_1 - \cdots - \frac{\alpha_{k-1}}{\alpha_k} x_{k-1}.$$

Thus the set of ks with the property that x_k is a linear combination of $x_1, ..., x_{k-1}$ is a nonempty set that contains some integer ≥ 2. Now simply select the smallest integer in this set to get the desired choice for k. □

This immediately leads us to the following criterion for linear independence.

COROLLARY 7. (Characterization of Linear Independence) *Let $x_1, ..., x_n \in V$. Then $x_1, ..., x_n$ is linearly independent if and only if $x_1 \neq 0$ and for each $k \geq 2$ we have*

$$x_k \notin \operatorname{span}\{x_1, ..., x_{k-1}\}.$$

EXAMPLE 37. *Let $A \in \operatorname{Mat}_{n \times n}(\mathbb{F})$ be an upper triangular matrix with k nonzero entries on the diagonal. We claim that the rank of A is $\geq k$. Select the k column vectors $x_1, ..., x_k$ that correspond to the nonzero diagonal entries from left to right. Thus $x_1 \neq 0$ and*

$$x_l \notin \operatorname{span}\{x_1, ..., x_{l-1}\}$$

since x_l has a nonzero entry that lies below all of the nonzero entries for $x_1, ..., x_{l-1}$. Using the dimension formula we see that $\dim(\ker(A)) \leq n - k$.

It is possible for A to have rank $> k$. Consider, e.g.,

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

This matrix has rank 2, but only one nonzero entry on the diagonal.

Recall from "Subspaces" that we can choose complements to a subspace by selecting appropriate vectors from a set that spans the vector space.

COROLLARY 8. *If $V = \operatorname{span}\{x_1, ..., x_n\}$, then we can select*

$$x_{i_1}, ..., x_{i_k} \in \{x_1, ..., x_n\}$$

forming a basis for V.

PROOF. We use $M = \{0\}$ and select $x_{i_1}, ..., x_{i_k}$ such that

$$\begin{aligned} x_{i_1} &\neq 0, \\ x_{i_2} &\notin \operatorname{span}\{x_{i_1}\}, \\ &\vdots \\ x_{i_k} &\notin \operatorname{span}\{x_{i_1}, ..., x_{i_{k-1}}\}, \\ V &= \operatorname{span}\{x_{i_1}, ..., x_{i_k}\}. \end{aligned}$$

The previous corollary then shows that x_{i_1}, ..., x_{i_k} are linearly independent. □

A more traditional method for establishing that all bases for a vector space have the same number of elements is based on the following classical result, often called simply the *Replacement Theorem*.

THEOREM 6. (Steinitz Replacement) *Let $y_1, ..., y_m \in V$ be linearly independent and $V = \operatorname{span}\{x_1, ..., x_n\}$. Then $m \leq n$ and V has a basis of the form y_1, ..., y_m, x_{i_1}, ..., x_{i_l} where $l \leq n - m$.*

PROOF. First observe that we know we can find $x_{i_1}, ..., x_{i_l}$ such that $\operatorname{span}\{x_{i_1}, ..., x_{i_l}\}$ is a complement to $M = \operatorname{span}\{y_1, ..., y_m\}$. Thus y_1, ..., y_m, x_{i_1}, ..., x_{i_l} must form a basis for V.

The fact that $m \leq \dim(V)$ follows from the Subspace Theorem and that $n \geq \dim(V)$ from the above result. This also shows that $l \leq n - m$.

It is, however, possible to give a more direct argument that does not use the Subspace Theorem. Instead we use a simple algorithm and the proof of the above corollary.

Observe that y_1, x_1, ..., x_n are linearly dependent as y_1 is a linear combination of x_1, ..., x_n. As $y_1 \neq 0$ this shows that some x_i is a linear combination of the previous vectors. Thus also

$$\operatorname{span}\{y_1, x_1, ..., x_{i-1}, x_{i+1}, ..., x_n\} = V.$$

Now repeat the argument with y_2 in place of y_1 and y_1, x_1, ..., x_{i-1}, x_{i+1}, ..., x_n in place of x_1, ..., x_n. Thus

$$y_2, y_1, x_1, ..., x_{i-1}, x_{i+1}, ..., x_n$$

is linearly dependent and since y_2, y_1 are linearly independent some x_j is a linear combination of the previous vectors. Continuing in this fashion we get a set of n vectors

$$y_m, ..., y_1, x_{j_1}, ...x_{j_{n-m}}$$

that spans V. Finally we can use the above corollary to eliminate vectors to obtain a basis. Since y_m, ..., y_1 are linearly independent we can do this by just trowing away vectors from x_{j_1}, ..., $x_{j_{n-m}}$. □

This theorem leads us to a new proof of the fact that any two bases must contain the same number of elements. It also shows that a linearly independent collection of vectors contains fewer vectors than a basis, while a spanning set contains more elements than a basis.

Finally we can prove a remarkable threom for matrices, that we shall revisit many more times in this text.. The *column rank* of a matrix is the dimension of the column space, i.e., the space spanned by the column vectors. In other words, it is the maximal number of linearly independent column vectors. This is also the dimension of the image of the matrix viewed as a linear map. Similarly the *row rank* is the dimension of the row space, i.e., the space spanned by the row vectors. This is the dimension of the image of the transposed matrix.

THEOREM 7. (The Rank Theorem) *Any $n \times m$ matrix has the property that the row rank is equal to the column rank.*

PROOF. Let $A \in \operatorname{Mat}_{n\times m}(\mathbb{F})$ and x_1, ..., $x_r \in \mathbb{F}^n$ be a basis for the column space of A. Next write the columns of A as linear combinations of this basis

$$\begin{aligned} A &= \begin{bmatrix} x_1 & \cdots & x_r \end{bmatrix} \begin{bmatrix} \beta_{11} & & \beta_{1m} \\ & & \\ \beta_{r1} & & \beta_{rm} \end{bmatrix} \\ &= \begin{bmatrix} x_1 & \cdots & x_r \end{bmatrix} B \end{aligned}$$

By taking transposes we see that

$$A^t = B^t \begin{bmatrix} x_1 & \cdots & x_r \end{bmatrix}^t.$$

But this shows that the columns of A^t, i.e., the rows of A, are linear combinations of the r vectors that form the columns of B^t

$$\begin{bmatrix} \beta_{11} \\ \vdots \\ \beta_{1m} \end{bmatrix}, ..., \begin{bmatrix} \beta_{r1} \\ \vdots \\ \beta_{rm} \end{bmatrix}$$

Thus the row space is spanned by r vectors. This shows that there can't be more than r linearly independent rows.

A similar argument shows that the reverse inequality also holds. □

There is a very interesting example associated to the rank theorem..

EXAMPLE 38. *Let $t_1, ..., t_n \in \mathbb{F}$ be distinct. We claim that the vectors*

$$\begin{bmatrix} 1 \\ t_1 \\ \vdots \\ t_1^{n-1} \end{bmatrix}, ..., \begin{bmatrix} 1 \\ t_n \\ \vdots \\ t_n^{n-1} \end{bmatrix}$$

are a basis for $\mathbb{F}^n$. To show this we have to show that the rank of the corresponding matrix

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ t_1 & t_2 & & t_n \\ \vdots & & & \vdots \\ t_1^{n-1} & t_2^{n-1} & \cdots & t_n^{n-1} \end{bmatrix}$$

is n. The simplest way to do this is by considering the row rank. If the rows are linearly dependent, then we can find $\alpha_0, ..., \alpha_{n-1} \in \mathbb{F}$ so that

$$\alpha_0 \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} + \alpha_1 \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{bmatrix} + \cdots + \alpha_{n-1} \begin{bmatrix} t_1^{n-1} \\ t_2^{n-1} \\ \vdots \\ t_n^{n-1} \end{bmatrix} = 0.$$

Thus the polynomial

$$p(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_{n-1} t^{n-1}$$

has $t_1, ..., t_n$ as roots. In other words we have a polynomial of degree $\leq n-1$ with n roots. This is not possible unless $\alpha_1 = \cdots = \alpha_{n-1} = 0$ (see also "Polynomials" in chapter 2).

The criteria for linear dependence lead to an important result about the powers of a linear operator. Before going into that we observe that there is a connection between polynomials and linear combinations of powers of a linear operator. Let $L : V \to V$ be a linear operator on an n-dimensional vector space. If

$$p(t) = \alpha_k t^k + \cdots + \alpha_1 t + \alpha_0 \in \mathbb{F}[t],$$

then

$$p(L) = \alpha_k L^k + \cdots + \alpha_1 L + \alpha_0 1_V$$

is a linear combination of

$$L^k, ..., L, 1_V.$$

Conversely any linear combination of L^k, ..., L, 1_V must look like this.

Since hom (V,V) has dimension n^2 it follows that 1_V, L, L^2, ..., L^{n^2} are linearly dependent. This means that we can find a smallest positive integer $k \leq n^2$ such that 1_V, L, L^2, ..., L^k are linearly dependent. Thus 1_V, L, L^2, ..., L^l are linearly independent for $l < k$ and

$$L^k \in \text{span}\left\{1_V, L, L^2, ..., L^{k-1}\right\}.$$

In the next chapter we shall show that $k \leq n$. The fact that

$$L^k \in \text{span}\left\{1_V, L, L^2, ..., L^{k-1}\right\}$$

means that we have a polynomial

$$\mu_L(t) = t^k + \alpha_{k-1}t^{k-1} + \cdots + \alpha_1 t + \alpha_0$$

such that

$$\mu_L(L) = 0.$$

This is the so called *minimal polynomial* for L. Apparently there is no polynomial of smaller degree that has L as a root.

Recall that we characterized projections as linear operators that satisfy $L^2 = L$ (see "Linear Maps and Subspaces"). Thus nontrivial projections are precisely the operators whose minimal polynomial is $\mu_L(t) = t^2 - t$. Note that teow trivial projections 1_V and 0_V have minimal polynomials $\mu_{1_V} = t - 1$ and $\mu_{0_V} = t$.

Example 39. *Let*

$$\begin{aligned} A &= \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} \\ B &= \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix} \\ C &= \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & i \end{bmatrix} \end{aligned}$$

We note that A is not proportional to 1_V, while

$$\begin{aligned} A^2 &= \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}^2 \\ &= \begin{bmatrix} \lambda^2 & 2\lambda \\ 0 & \lambda^2 \end{bmatrix} \\ &= 2\lambda \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} - \lambda^2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

Thus

$$\mu_A(t) = t^2 - 2\lambda t + \lambda^2 = (t-\lambda)^2.$$

The calculation for B is similar and evidently yields the same minimal polynomial

$$\mu_B(t) = t^2 - 2\lambda t + \lambda^2 = (t-\lambda)^2.$$

Finally for C we note that

$$C^2 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

Thus

$$\mu_C(t) = t^2 + 1.$$

In the theory of differential equations it is also important to understand when functions are linearly independent. We start with vector valued functions $x_1(t), \ldots,$ $x_k(t) : I \to \mathbb{F}^n$, where I is any set, but usually an interval. These k functions are linearly independent provided they are linearly independent at just one point $t_0 \in I$. In other words if the k vectors $x_1(t_0), \ldots, x_k(t_0) \in \mathbb{F}^n$ are linearly independent then the functions are also linearly independent. The converse statement is not true in general. To see why this is we give a specific example.

EXAMPLE 40. *It is an important fact from analysis that there are functions* $\phi(t) \in C^\infty(\mathbb{R}, \mathbb{R})$ *such that*

$$\phi(t) = \begin{cases} 0 & t \leq 0 \\ 1 & t \geq 1 \end{cases}$$

these can easily be pictured, but it takes some work to construct them. Given this function we consider $x_1, x_2 : \mathbb{R} \to \mathbb{R}^2$ *defined by*

$$\begin{aligned} x_1(t) &= \begin{bmatrix} \phi(t) \\ 0 \end{bmatrix}, \\ x_2(t) &= \begin{bmatrix} 0 \\ \phi(-t) \end{bmatrix}. \end{aligned}$$

When $t \leq 0$ *we have that* $x_1 = 0$ *so the two functions are linearly dependent on* $(-\infty, 0]$. *When* $t \geq 0$, *we have that* $x_2(t) = 0$ *so the functions are also linearly dependent on* $[0, \infty)$. *Now assume that we can find* $\lambda_1, \lambda_2 \in \mathbb{R}$ *such that*

$$\lambda_1 x_1(t) + \lambda_2 x_2(t) = 0 \text{ for all } t \in \mathbb{R}.$$

If $t \geq 1$, *this implies that*

$$\begin{aligned} 0 &= \lambda_1 x_1(t) + \lambda_2 x_2(t) \\ &= \lambda_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \lambda_2 \begin{bmatrix} 0 \\ 0 \end{bmatrix} \\ &= \lambda_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix}. \end{aligned}$$

Thus $\lambda_1 = 0$. *Similarly we have for* $t \leq -1$

$$\begin{aligned} 0 &= \lambda_1 x_1(t) + \lambda_2 x_2(t) \\ &= \lambda_1 \begin{bmatrix} 0 \\ 0 \end{bmatrix} + \lambda_2 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \lambda_2 \begin{bmatrix} 1 \\ 0 \end{bmatrix}. \end{aligned}$$

So $\lambda_2 = 0$. *This shows that the two functions* x_1 *and* x_2 *are linearly independent as functions on* $\mathbb{R}$ *even though they are linearly dependent for each* $t \in \mathbb{R}$.

Next we want to study what happens in the spacial case where $n = 1$, i.e., we have functions $x_1(t), \ldots, x_k(t) : I \to \mathbb{F}$. In this case the above strategy for determining linear independence at a point completely fails as the values lie in a one dimensional vector space. We can, however, construct auxiliary vector valued functions by taking derivatives. In order to be able to take derivatives we have to assume either that $I = \mathbb{F}$ and $x_i \in \mathbb{F}[t]$ are polynomials with the formal derivatives defined as in exercise 2 in "Linear Maps" or that $I \subset \mathbb{R}$ is an interval, $\mathbb{F} = \mathbb{C}$, and $x_i \in C^{\infty}(I, \mathbb{C})$. In either case we can then construct new vector valued functions $z_1, ..., z_k : I \to \mathbb{F}^k$ by listing x_i and its first $k-1$ derivatives in column form

$$z_i(t) = \begin{bmatrix} x_i(t) \\ (Dx_i)(t) \\ \\ \left(D^{k-1}x_i\right)(t) \end{bmatrix}$$

First we claim that $x_1, ..., x_k$ are linearly dependent if and only if $z_1, ..., z_k$ are linearly dependent. This quite simple and depends on the fact that D^n is linear. We only need to observe that

$$\begin{aligned} \alpha_1 z_1 + \cdots + \alpha_k z_k &= \alpha_1 \begin{bmatrix} x_1 \\ Dx_1 \\ \vdots \\ D^{k-1}x_1 \end{bmatrix} + \cdots + \alpha_k \begin{bmatrix} x_k \\ Dx_k \\ \vdots \\ D^{k-1}x_k \end{bmatrix} \\ &= \begin{bmatrix} \alpha_1 x_1 \\ \alpha_1 Dx_1 \\ \vdots \\ \alpha_1 D^{k-1}x_1 \end{bmatrix} + \cdots + \begin{bmatrix} \alpha_k x_k \\ \alpha_k Dx_k \\ \vdots \\ \alpha_k D^{k-1}x_k \end{bmatrix} \\ &= \begin{bmatrix} \alpha_1 x_1 + \cdots + \alpha_k x_k \\ \alpha_1 Dx_1 + \cdots + \alpha_k Dx_k \\ \vdots \\ \alpha_1 D^{k-1}x_1 + \cdots + \alpha_k D^{k-1}x_k \end{bmatrix} \\ &= \begin{bmatrix} \alpha_1 x_1 + \cdots + \alpha_k x_k \\ D(\alpha_1 x_1 + \cdots + \alpha_k x_k) \\ \vdots \\ D^{k-1}(\alpha_1 x_1 + \cdots + \alpha_k x_k) \end{bmatrix}. \end{aligned}$$

Thus $\alpha_1 z_1 + \cdots + \alpha_k z_k = 0$ if and only if $\alpha_1 x_1 + \cdots + \alpha_k x_k = 0$. This shows the claim. Let us now see how this works in action.

EXAMPLE 41. *Let $x_i(t) = \exp(\lambda_i t)$, where $\lambda_i \in \mathbb{C}$ are distinct. Then*

$$z_i(t) = \begin{bmatrix} \exp(\lambda_i t) \\ \lambda_i \exp(\lambda_i t) \\ \vdots \\ \lambda_i^{k-1} \exp(\lambda_i t) \end{bmatrix} = \begin{bmatrix} 1 \\ \lambda_i \\ \vdots \\ \lambda_i^{k-1} \end{bmatrix} \exp(\lambda_i t).$$

Thus $\exp(\lambda_1 t), ..., \exp(\lambda_k t)$ are linearly independent as we saw above that the vectors

$$\begin{bmatrix} 1 \\ \lambda_1 \\ \vdots \\ \lambda_1^{k-1} \end{bmatrix}, ..., \begin{bmatrix} 1 \\ \lambda_k \\ \vdots \\ \lambda_k^{k-1} \end{bmatrix}$$

are linearly independent.

EXAMPLE 42. *Let* $x_k(t) = \cos(kt)$, $k = 0, 1, 2, ..., n$. *In this case direct check will involve a matrix that has both cosines and sines in alternating rows. Instead we can use Euler's formula that*

$$x_k(t) = \cos(kt) = \frac{1}{2}e^{ikt} - \frac{1}{2}e^{-ikt}.$$

We know from the previous exercise that the $2n+1$ *functions* $\exp(ikt)$, $k = 0, \pm 1, ..., \pm n$ *are linearly independent. Thus the original* $n+1$ *cosine functions are also linearly independent.*

Note that if we added the n *sine functions* $y_k(t) = \sin(kt)$, $k = 1, ..., n$ *we have* $2n+1$ *cosine and sine functions that also become linearly independent.*

12.1. Exercises.

(1) *(Characterization of Linear Independence)* Show that $x_1, ..., x_n$ are linearly independent in V if and only if

$$\text{span}\{x_1, ..., \hat{x}_i, ..., x_n\} \neq \text{span}\{x_1, ..., x_n\}$$

for all $i = 1, ..., n$.

(2) *(Characterization of Linear Independence)* Show that $x_1, ..., x_n$ are linearly independent in V if and only if

$$\text{span}\{x_1, ..., x_n\} = \text{span}\{x_1\} \oplus \cdots \oplus \text{span}\{x_n\}.$$

(3) Assume that we have nonzero vectors $x_1, ..., x_k \in V$ and a direct sum of subspaces

$$M_1 + \cdots + M_k = M_1 \oplus \cdots \oplus M_k.$$

Show that if $x_i \in M_i$, then $x_1, ..., x_k$ are linearly independent.

(4) Show that $t^3 + t^2 + 1, t^3 + t^2 + t, t^3 + t + 2$ are linearly independent in P_3. Which of the standard basis vectors $1, t, t^2, t^3$ can be added to this collection to create a basis for P_3?

(5) If $p_0(t), ..., p_n(t) \in \mathbb{F}[t]$ all have degree $\leq n$ and all vanish at t_0, then they are linearly dependent.

(6) Assume that we have two fields $\mathbb{F} \subset \mathbb{L}$, such as $\mathbb{R} \subset \mathbb{C}$.
   (a) If $x_1, ..., x_m$ form a basis for $\mathbb{F}^m$, then they also form a basis for $\mathbb{L}^m$.
   (b) If $x_1, ..., x_k$ are linearly independent in $\mathbb{F}^m$, then they are also linearly independent in $\mathbb{L}^m$.
   (c) If $x_1, ..., x_k$ are linearly dependent in $\mathbb{F}^m$, then they are also linearly dependent in $\mathbb{L}^m$.
   (d) If $x_1, ..., x_k \in \mathbb{F}^m$, then

$$\dim_{\mathbb{F}} \text{span}_{\mathbb{F}}\{x_1, ..., x_k\} = \dim_{\mathbb{L}} \text{span}_{\mathbb{L}}\{x_1, ..., x_k\}.$$

   (e) If $M \subset \mathbb{F}^m$ is a subspace, then

$$M = \text{span}_{\mathbb{L}}(M) \cap \mathbb{F}^m.$$

   (f) Let $A \in \text{Mat}_{n \times m}(\mathbb{F})$. Then $A : \mathbb{F}^m \to \mathbb{F}^n$ is one-to-one (resp. onto) if and only if $A : \mathbb{L}^m \to \mathbb{L}^n$ is one-to-one (resp. onto).

(7) Show that $\dim_{\mathbb{F}} V \leq n$ if and only if every collection of $n+1$ vectors is linearly dependent.

(8) Assume that $x_1, ..., x_k$ span V and that $L : V \to V$ is a linear map that is not one-to-one. Show that $L(x_1), ..., L(x_k)$ are linearly dependent.

(9) If $x_1, ..., x_k$ are linearly dependent, then $L(x_1), ..., L(x_k)$ are linearly dependent.
(10) If $L(x_1), ..., L(x_k)$ are linearly independent, then $x_1, ..., x_k$ are linearly independent.
(11) Let $A \in \text{Mat}_{n \times m}(\mathbb{F})$ and assume that $y_1, ..., y_m \in V$

$$\begin{bmatrix} y_1 & \cdots & y_m \end{bmatrix} = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} A$$

where $x_1, ..., x_n$ form a basis for V.
   (a) Show that $y_1, ..., y_m$ span V if and only if A has rank n. Conclude that $m \geq n$.
   (b) Show that $y_1, ..., y_m$ are linearly independent if and only if $\ker(A) = \{0\}$. Conclude that $m \leq n$.
   (c) Show that $y_1, ..., y_m$ form a basis for V if and only if A is invertible. Conclude that $m = n$.

13. Row Reduction

In this section we give a brief and rigorous outline of the standard procedures involved in solving systems of linear equations. The goal in the context of what we have already learned is to find a way of computing the image and kernel of a linear map that is represented by a matrix. Along the way we shall reprove that the dimension is well-defined as well as the dimension formula for linear maps.

The usual way of writing n equations with m variables is

$$\begin{array}{ccc} a_{11}x_1 + \cdots + a_{1m}x_m & = & b_1 \\ \vdots & \vdots & \vdots \\ a_{n1}x_1 + \cdots + a_{nm}x_m & = & b_n \end{array}$$

where the variables are $x_1, ..., x_m$. The goal is to understand for which choices of constants a_{ij} and b_i such systems can be solved and then list all the solutions. To conform to our already specified notation we change the system so that it looks like

$$\begin{array}{ccc} \alpha_{11}\xi_1 + \cdots + \alpha_{1m}\xi_m & = & \beta_1 \\ \vdots & \vdots & \vdots \\ \alpha_{n1}\xi_1 + \cdots + \alpha_{nm}\xi_m & = & \beta_n \end{array}$$

In matrix form this becomes

$$\begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{bmatrix} \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$$

and can be abbreviated to

$$Ax = b.$$

As such we can easily use the more abstract language of linear algebra to address some general points.

PROPOSITION 3. *Let $L : V \to W$ be a linear map.*

(1) *$L(x) = b$ can be solved if and only if $b \in \text{im}(L)$.*
(2) *If $L(x_0) = b$ and $x \in \ker(L)$, then $L(x + x_0) = b$.*
(3) *If $L(x_0) = b$ and $L(x_1) = b$, then $x_0 - x_1 \in \ker(L)$.*

Therefore, we can find all solutions to $L(x) = b$ provided we can find the kernel $\ker(L)$ and just one solution x_0. Note that the kernel consists of the solutions to what we call the *homogeneous system*: $L(x) = 0$.

With this behind us we are now ready to address the issue of how to make the necessary calculations that allow us to find a solution to

$$\begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{bmatrix} \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$$

The usual method is through *elementary row operations*. To keep things more conceptual think of the actual linear equations

$$\begin{array}{ccc} \alpha_{11}\xi_1 + \cdots + \alpha_{1m}\xi_m & = & \beta_1 \\ \vdots & \vdots & \vdots \\ \alpha_{n1}\xi_1 + \cdots + \alpha_{nm}\xi_m & = & \beta_n \end{array}$$

and observe that we can perform the following three operations without changing the solutions to the equations:

(1) Interchanging equations (or rows).
(2) Adding a multiple of an equation (or row) to a different equation (or row).
(3) Multiplying an equation (or row) by a nonzero number.

Using these operations one can put the system in *row echelon form*. This is most easily done by considering the *augmented matrix*, where the variables have disappeared

$$\left[\begin{array}{ccc|c} \alpha_{11} & \cdots & \alpha_{1m} & \beta_1 \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} & \beta_n \end{array}\right]$$

and then performing the above operations, now on rows, until it takes the special form where

(1) The first nonzero entry in each row is normalized to be 1. This is also called the *leading* 1 for the row.
(2) The leading 1s appear in echelon form, i.e., as we move down along the rows the leading 1s will appear farther to the right.

The method by which we put a matrix into row echelon form is called *Gauss elimination*. Having put the system into this simple form one can then solve it by starting from the last row or equation.

When doing the process on A itself we denote the resulting row echelon matrix by A_{ref}. There are many ways of doing row reductions so as to come up with a row echelon form for A and it is quite likely that one ends up with different echelon forms. To see why consider

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

This matrix is clearly in row echelon form. However we can subtract the second row from the first row to obtain a new matrix which is still in row echelon form:

$$\begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

It is now possible to use the last row to arrive at

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The important information about A_{ref} is the placement of the leading 1 in each row and this placement will always be the same for any row echelon form. To get a unique row echelon form we need to reduce the matrix using *Gauss-Jordan elimination*. This process is what we just performed on the above matrix A. The idea is to first arrive at some row echelon form A_{ref} and then starting with the second row eliminate all entries above the leading 1, this is then repeated with row three, etc. In this way we end up with a matrix that is still in row echelon form, but also has the property that all entries below and above the leading 1 in each row are zero. We say that such a matrix is in *reduced row echelon form.* If we start with a matrix A, then the resulting reduced row echelon form is denoted A_{rref}. For example, if we have

$$A_{\text{ref}} = \begin{bmatrix} 0 & 1 & 4 & 1 & 0 & 3 & -1 \\ 0 & 0 & 0 & 1 & -2 & 5 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

then we can reduce further to get a new reduced row echelon form

$$A_{\text{rref}} = \begin{bmatrix} 0 & 1 & 4 & 0 & 2 & -2 & 0 \\ 0 & 0 & 0 & 1 & -2 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The row echelon form and reduced row echelon form of a matrix can more abstractly be characterized as follows. Suppose that we have an $n \times m$ matrix $A = \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix}$, where $x_1, ..., x_m \in \mathbb{F}^n$ correspond to the columns of A. Let $e_1, ..., e_n \in \mathbb{F}^n$ be the canonical basis. The matrix is in row echelon form if we can find $1 \leq j_1 < \cdots < j_k \leq m$, where $k \leq n$, such that

$$x_{j_s} = e_s + \sum_{i<s} \alpha_{ij_s} e_i$$

for $s = 1, ..., k$. For all other indices j we have

$$\begin{aligned} x_j &= 0, \text{ if } j < j_1, \\ x_j &\in \operatorname{span}\{e_1, ..., e_s\}, \text{ if } j_s < j < j_{s+1}, \\ x_j &\in \operatorname{span}\{e_1, ..., e_k\}, \text{ if } j_k < j. \end{aligned}$$

Moreover, the matrix is in reduced row echelon form if in addition we assume that

$$x_{j_s} = e_s.$$

Below we shall prove that the reduced row echelon form of a matrix is unique, but before doing so it is convenient to reinterpret the row operations as matrix multiplication.

Let $A \in \mathrm{Mat}_{n\times m}(\mathbb{F})$ be the matrix we wish to row reduce. The row operations we have described can be accomplished by multiplying A by certain invertible $n\times n$ matrices on the left. These matrices are called *elementary matrices*. The define these matrices we use the standard basis matrices E_{kl} where the kl entry is 1 while all other entries are 0. The matrix product $E_{kl}A$ is a matrix whose k^{th} row is the l^{th} row of A and all other rows vanish.

(1) Interchanging rows k and l: This can be accomplished by the matrix multiplication $I_{kl}A$, where

$$\begin{aligned} I_{kl} &= E_{kl} + E_{lk} + \sum_{i\neq k,l} E_{ii} \\ &= E_{kl} + E_{lk} + 1_{\mathbb{F}^n} - E_{kk} - E_{ll} \end{aligned}$$

or in other words the ij entries α_{ij} in I_{kl} satisfy $\alpha_{kl} = \alpha_{lk} = 1$, $\alpha_{ii} = 1$ if $i \neq k, l$, and $\alpha_{ij} = 0$ otherwise. Note that $I_{kl} = I_{lk}$ and $I_{kl}I_{lk} = 1_{\mathbb{F}^n}$. Thus I_{kl} is invertible.

(2) Multiplying row l by $\alpha \in \mathbb{F}$ and adding it to row $k \neq l$. This can be accomplished via $R_{kl}(\alpha)A$, where

$$R_{kl}(\alpha) = 1_{\mathbb{F}^n} + \alpha E_{kl}$$

or in other words the ij entries α_{ij} in $R_{kl}(\alpha)$ look like $\alpha_{ii} = 1$, $\alpha_{kl} = \alpha$, and $\alpha_{ij} = 0$ otherwise. This time we note that $R_{kl}(\alpha)R_{kl}(-\alpha) = 1_{\mathbb{F}^n}$.

(3) Multiplying row k by $\alpha \in \mathbb{F} - \{0\}$. This can be accomplished by $M_k(\alpha)A$, where

$$\begin{aligned} M_k(\alpha) &= \alpha E_{kk} + \sum_{i\neq k} E_{ii} \\ &= 1_{\mathbb{F}^n} + (\alpha - 1)E_{kk} \end{aligned}$$

or in other words the ij entries α_{ij} of $M_k(\alpha)$ are $\alpha_{kk} = \alpha$, $\alpha_{ii} = 1$ if $i \neq k$, and $\alpha_{ij} = 0$ otherwise. Clearly $M_k(\alpha)M_k(\alpha^{-1}) = 1_{\mathbb{F}^n}$.

Performing row reductions on A is now the same as doing a matrix multiplication PA, where $P \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ is a product of the elementary matrices. Note that such P are invertible and that P^{-1} is also a product of elementary matrices. The elementary 2×2 matrices look like.

$$\begin{aligned} I_{12} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ R_{12}(\alpha) &= \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}, \\ R_{21}(\alpha) &= \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix}, \\ M_1(\alpha) &= \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix}, \\ M_2(\alpha) &= \begin{bmatrix} 1 & 0 \\ 0 & \alpha \end{bmatrix}. \end{aligned}$$

If we multiply these matrices onto A from the left we obtain the desired operations:

$$I_{12}A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} = \begin{bmatrix} \alpha_{21} & \alpha_{22} \\ \alpha_{11} & \alpha_{12} \end{bmatrix}$$

$$R_{12}(\alpha) A = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} = \begin{bmatrix} \alpha_{11} + \alpha\alpha_{21} & \alpha_{12} + \alpha\alpha_{22} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}$$

$$R_{21}(\alpha) A = \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix} \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha\alpha_{11} + \alpha_{21} & \alpha\alpha_{12} + \alpha_{22} \end{bmatrix}$$

$$M_1(\alpha) A = \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} = \begin{bmatrix} \alpha\alpha_{11} & \alpha\alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}$$

$$M_2(\alpha) A = \begin{bmatrix} 1 & 0 \\ 0 & \alpha \end{bmatrix} \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha\alpha_{21} & \alpha\alpha_{22} \end{bmatrix}$$

We can now move on to the important result mentioned above.

THEOREM 8. (Uniqueness of Reduced Row Echelon Form) *The reduced row echelon form of an $n \times m$ matrix is unique.*

PROOF. Let $A \in \mathrm{Mat}_{n\times m}(\mathbb{F})$ and assume that we have two reduced row echelon forms

$$\begin{aligned} PA &= \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix}, \\ QA &= \begin{bmatrix} y_1 & \cdots & y_m \end{bmatrix}, \end{aligned}$$

where $P, Q \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ are invertible. In particular, we have that

$$R \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} = \begin{bmatrix} y_1 & \cdots & y_m \end{bmatrix}$$

where $R \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ is invertible. We shall show that $x_i = y_i$, $i = 1, ..., m$ by induction on n.

First observe that if $A = 0$, then there is nothing to prove. If $A \neq 0$, then both of the reduced row echelon forms have to be nontrivial. Then we have that

$$\begin{aligned} x_{i_1} &= e_1, \\ x_i &= 0 \text{ for } i < i_1 \end{aligned}$$

and

$$\begin{aligned} y_{j_1} &= e_1, \\ y_i &= 0 \text{ for } i < j_1. \end{aligned}$$

The relationship $Rx_i = y_i$ shows that $y_i = 0$ if $x_i = 0$. Thus $j_1 \geq i_1$. Similarly the relationship $y_i = R^{-1}x_i$ shows that $x_i = 0$ if $y_i = 0$. Hence also $j_1 \leq i_1$. Thus $i_1 = j_1$ and $x_{i_1} = e_1 = y_{j_1}$. This implies that $Re_1 = e_1$ and $R^{-1}e_1 = e_1$. In other words

$$R = \begin{bmatrix} 1 & 0 \\ 0 & R' \end{bmatrix}$$

where $R' \in \mathrm{Mat}_{(n-1)\times(n-1)}(\mathbb{F})$ is invertible. In the special case where $n = 1$, we are finished as we have shown that $R = [1]$ in that case. This anchors our induction. We can now assume that the induction hypothesis is that all $(n-1) \times m$ matrices have unique reduced row echelon forms.

If we define $x_i', y_i' \in \mathbb{F}^{n-1}$ as the last $n-1$ entries in x_i and y_i, i.e.,

$$\begin{aligned} x_i &= \begin{bmatrix} \xi_{1i} \\ x_i' \end{bmatrix}, \\ y_i &= \begin{bmatrix} \upsilon_{1i} \\ y_i' \end{bmatrix}, \end{aligned}$$

then we see that $\begin{bmatrix} x_1' & \cdots & x_m' \end{bmatrix}$ and $\begin{bmatrix} y_1' & \cdots & y_m' \end{bmatrix}$ are still in reduced row echelon form. Moreover, the relationship

$$\begin{bmatrix} y_1 & \cdots & y_m \end{bmatrix} = R \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix}$$

now implies that

$$\begin{aligned} \begin{bmatrix} \upsilon_{11} & \cdots & \upsilon_{1m} \\ y_1' & \cdots & y_m' \end{bmatrix} &= \begin{bmatrix} y_1 & \cdots & y_m \end{bmatrix} \\ &= R \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & R' \end{bmatrix} \begin{bmatrix} \xi_{11} & \cdots & \xi_{1m} \\ x_1' & \cdots & x_m' \end{bmatrix} \\ &= \begin{bmatrix} \xi_{11} & \cdots & \xi_{1m} \\ R'x_1' & \cdots & R'x_m' \end{bmatrix} \end{aligned}$$

Thus

$$R' \begin{bmatrix} x_1' & \cdots & x_m' \end{bmatrix} = \begin{bmatrix} y_1' & \cdots & y_m' \end{bmatrix}.$$

The induction hypothesis now implies that $x_i' = y_i'$. This combined with

$$\begin{aligned} \begin{bmatrix} y_1 & \cdots & y_m \end{bmatrix} &= \begin{bmatrix} \upsilon_{11} & \cdots & \upsilon_{1m} \\ y_1' & \cdots & y_m' \end{bmatrix} \\ &= \begin{bmatrix} \xi_{11} & \cdots & \xi_{1m} \\ R'x_1' & \cdots & R'x_m' \end{bmatrix} \\ &= \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \end{aligned}$$

shows that $x_i = y_i$ for all $i = 1, ..., m$. □

We are now ready to explain how the reduced row echelon form can be used to identify the kernel and image of a matrix. Along the way we shall reprove some of our earlier results. Suppose that $A \in \mathrm{Mat}_{n \times m}(\mathbb{F})$ and

$$\begin{aligned} PA &= A_{\mathrm{rref}} \\ &= \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix}, \end{aligned}$$

where we can find $1 \le j_1 < \cdots < j_k \le m$, such that

$$\begin{aligned} x_{j_s} &= e_s \text{ for } i = 1, ..., k \\ x_j &= 0, \text{ if } j < j_1, \\ x_j &\in \operatorname{span}\{e_1, ..., e_s\}, \text{ if } j_s < j < j_{s+1}, \\ x_j &\in \operatorname{span}\{e_1, ..., e_k\}, \text{ if } j_k < j. \end{aligned}$$

Finally let $i_1 < \cdots < i_{m-k}$ be the indices complementary to $j_1, .., j_k$, i.e.,

$$\{1, ..., m\} = \{j_1, .., j_k\} \cup \{i_1, ..., i_{m-k}\}.$$

We are first going to study the kernel of A. Since P is invertible we see that $Ax = 0$ if and only if $A_{\mathrm{rref}} x = 0$. Thus we need only study the equation $A_{\mathrm{rref}} x = 0$. If we let $x = (\xi_1, ..., \xi_m)$, then the nature of the equations $A_{\mathrm{rref}} x = 0$ will tell us that

$(\xi_1, ..., \xi_m)$ are uniquely determined by $\xi_{i_1}, ..., \xi_{i_{m-k}}$. To see why this is we note that if we have $A_{\text{rref}} = [\alpha_{ij}]$, then the reduced row echelon form tells us that

$$\begin{aligned} \xi_{j_1} + \alpha_{1i_1}\xi_{i_1} + \cdots + \alpha_{1i_{m-k}}\xi_{i_{m-k}} &= 0, \\ &\vdots \\ \xi_{j_k} + \alpha_{ki_1}\xi_{i_1} + \cdots + \alpha_{ki_{m-k}}\xi_{i_{m-k}} &= 0, \end{aligned}$$

Thus $\xi_{j_1}, ..., \xi_{j_k}$ have explicit formulas in terms of $\xi_{i_1}, ..., \xi_{i_{m-k}}$. We actually get a bit more information: If we take $(\alpha_1, ..., \alpha_{m-k}) \in \mathbb{F}^{m-k}$ and construct the unique solution $x = (\xi_1, ..., \xi_m)$ such that $\xi_{i_1} = \alpha_1$, ..., $\xi_{i_{m-k}} = \alpha_{m-k}$ then we have actually constructed a map

$$\begin{aligned} \mathbb{F}^{m-k} &\to \ker(A_{\text{rref}}) \\ (\alpha_1, ..., \alpha_{m-k}) &\to (\xi_1, ..., \xi_m). \end{aligned}$$

We have just seen that this map is onto. The construction also gives us explicit formulas for $\xi_{j_1}, ..., \xi_{j_k}$ that are linear in $\xi_{i_1} = \alpha_1$, ..., $\xi_{i_{m-k}} = \alpha_{m-k}$. Thus the map is linear. Finally if $(\xi_1, ..., \xi_m) = 0$, then we clearly also have $(\alpha_1, ..., \alpha_{m-k}) = 0$, so the map is one-to-one. All in all it is a linear isomorphism.

This leads us to the following result.

THEOREM 9. (Uniqueness of Dimension) *Let* $A \in \text{Mat}_{n\times m}(\mathbb{F})$, *if* $n < m$, *then* $\ker(A) \neq \{0\}$. *Consequently* $\mathbb{F}^n$ *and* $\mathbb{F}^m$ *are not isomorphic.*

PROOF. Using the above notation we have $k \leq n < m$. Thus $m - k > 0$. From what we just saw this implies $\ker(A) = \ker(A_{\text{rref}}) \neq \{0\}$. In particular it is not possible for A to be invertible. This shows that $\mathbb{F}^n$ and $\mathbb{F}^m$ cannot be isomorphic. □

Having now shown that the dimension of a vector space is well-defined we can then establish the dimension formula. Part of the proof of this theorem is to identify a basis for the image of a matrix. Note that this proof does not depend on the result that subspaces of finite dimensional vector spaces are finite dimensional. In fact for the subspaces under consideration, namely, the kernel and image, it is part of the proof to show that they are finite dimensional.

THEOREM 10. (The Dimension Formula) *Let* $A \in \text{Mat}_{n\times m}(\mathbb{F})$, *then*

$$m = \dim(\ker(A)) + \dim(\text{im}(A)).$$

PROOF. We use the above notation. We just saw that $\dim(\ker(A)) = m - k$, so it remains to check why $\dim(\text{im}(A)) = k$?

If

$$A = \begin{bmatrix} y_1 & \cdots & y_m \end{bmatrix},$$

then we have $y_i = P^{-1}x_i$, where

$$A_{\text{rref}} = \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix}.$$

We know that each

$$x_j \in \text{span}\{e_1, ..., e_k\} = \text{span}\{x_{j_1}, ..., x_{j_k}\},$$

thus we have that

$$y_j \in \text{span}\{y_{j_1}, ..., y_{j_k}\}.$$

Moreover, as P is invertible we see that $y_{j_1}, ..., y_{j_k}$ must be linearly independent as $e_1, ..., e_k$ are linearly independent. This proves that $y_{j_1}, ..., y_{j_k}$ form a basis for $\operatorname{im}(A)$. □

COROLLARY 9. (Subspace Theorem) *Let $M \subset \mathbb{F}^n$ be a subspace. Then M is finite dimensional and* $\dim(M) \leq n$.

PROOF. Recall from "Subspaces" that every subspace $M \subset \mathbb{F}^n$ has a complement. This means that we can construct a projection as in "Linear Maps and Subspaces" that has M as kernel. This means that M is the kernel for some $A \in \operatorname{Mat}_{n\times n}(\mathbb{F})$. Thus the previous theorem implies the claim. □

It might help to see an example of how the above constructions work.

EXAMPLE 43. *Suppose that we have a 4×7 matrix*

$$A = \begin{bmatrix} 0 & 1 & 4 & 1 & 0 & 3 & -1 \\ 0 & 0 & 0 & 1 & -2 & 5 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Then

$$A_{\text{rref}} = \begin{bmatrix} 0 & 1 & 4 & 0 & 2 & -2 & 0 \\ 0 & 0 & 0 & 1 & -2 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Thus $j_1 = 2$, $j_2 = 4$, and $j_3 = 7$. The complementary indices are $i_1 = 1$, $i_2 = 3$, $i_3 = 5$, and $i_4 = 6$. Hence

$$\operatorname{im}(A) = \operatorname{span}\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ -4 \\ 1 \\ 1 \end{bmatrix} \right\}$$

and

$$\ker(A) = \left\{ \begin{bmatrix} \xi_1 \\ -4\xi_3 - 2\xi_5 + 2\xi_6 \\ \xi_3 \\ 2\xi_5 - 5\xi_6 \\ \xi_5 \\ \xi_6 \\ 0 \end{bmatrix} : \xi_1, \xi_3, \xi_5, \xi_6 \in \mathbb{F} \right\}.$$

Our method for finding a basis for the image of a matrix leads us to a different proof of the rank theorem. The *column rank* of a matrix is simply the dimension of the image, in other words, the maximal number of linearly independent column vectors. Similarly the *row rank* is the maximal number of linearly independent rows. In other words, the row rank is the dimension of the image of the transposed matrix.

THEOREM 11. (The Rank Theorem) *Any $n \times m$ matrix has the property that the row rank is equal to the column rank.*

PROOF. We just saw that the column rank for A and A_{rref} are the same and equal to k with the above notation. Because of the row operations we use, it is clear that the rows of A_{rref} are linear combinations of the rows of A. As the process can be reversed the rows of A are also linear combinations of the rows A_{rref}. Hence A and A_{rref} also have the same row rank. Now A_{rref} has k linearly independent rows and must therefore have row rank k. □

Using the rank theorem together with the dimension formula leads to an interesting corollary.

COROLLARY 10. *Let* $A \in \text{Mat}_{n\times n}(\mathbb{F})$. *Then*

$$\dim(\ker(A)) = \dim\left(\ker\left(A^t\right)\right),$$

where $A^t \in \text{Mat}_{n\times n}(\mathbb{F})$ *is the transpose of* A.

We are now going to clarify what type of matrices P occur when we do the row reduction to obtain $PA = A_{\text{rref}}$. If we have an $n \times n$ matrix A with trivial kernel, then it must follow that $A_{\text{rref}} = 1_{\mathbb{F}^n}$. Therefore, if we perform Gauss-Jordan elimination on the augmented matrix

$$A|1_{\mathbb{F}^n},$$

then we end up with an answer that looks like

$$1_{\mathbb{F}^n}|B.$$

The matrix B evidently satisfies $AB = 1_{\mathbb{F}^n}$. To be sure that this is the inverse we must also check that $BA = 1_{\mathbb{F}^n}$. However, we know that A has an inverse A^{-1}. If we multiply the equation $AB = 1_{\mathbb{F}^n}$ by A^{-1} on the left we obtain $B = A^{-1}$. This settles the uncertainty.

The space of all invertible $n \times n$ matrices is called the *general linear group* and is denoted by:

$$Gl_n(\mathbb{F}) = \left\{A \in \text{Mat}_{n\times n}(\mathbb{F}) : \exists\ A^{-1} \in \text{Mat}_{n\times n}(\mathbb{F}) \text{ with } AA^{-1} = A^{-1}A = 1_{\mathbb{F}^n}\right\}.$$

This space is a so called *group*. This means that we have a set G and a product operation $G \times G \to G$ denoted by $(g,h) \to gh$. This product operation must satisfy

1. Associativity: $(g_1g_2)g_3 = g_1(g_2g_3)$.
2. Existence of a unit $e \in G$ such that $eg = ge = g$.
3. Existence of inverses: For each $g \in G$ there is $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$.

If we use matrix multiplication in $Gl_n(\mathbb{F})$ and $1_{\mathbb{F}^n}$ as the unit, then it is clear that $Gl_n(\mathbb{F})$ is a group. Note that we don't assume that the product operation in a group is commutative, and indeed it isn't commutative in $Gl_n(\mathbb{F})$ unless $n = 1$.

If a possibly infinite subset $S \subset G$ of a group has the property that any element in G can be written as a product of elements in S, then we say that S *generates* G.

We can now prove

THEOREM 12. *The general linear group* $Gl_n(\mathbb{F})$ *is generated by the elementary matrices* I_{kl}, $R_{kl}(\alpha)$, *and* $M_k(\alpha)$.

PROOF. We already observed that I_{kl}, $R_{kl}(\alpha)$, and $M_k(\alpha)$ are invertible and hence form a subset in $Gl_n(\mathbb{F})$. Let $A \in Gl_n(\mathbb{F})$, then we know that also $A^{-1} \in Gl_n(\mathbb{F})$. Now observe that we can find $P \in Gl_n(\mathbb{F})$ as a product of elementary matrices such that $PA^{-1} = 1_{\mathbb{F}^n}$. This was the content of the Gauss-Jordan elimination process for finding the inverse of a matrix. This means that $P = A$ and hence A is a product of elementary matrices. □

As a corollary we have:

COROLLARY 11. *Let* $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$, *then it is possible to find* $P \in Gl_n(\mathbb{F})$ *such that* PA *is upper triangular:*

$$PA = \begin{bmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ 0 & \beta_{22} & \cdots & \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \beta_{nn} \end{bmatrix}$$

Moreover

$$\ker(A) = \ker(PA)$$

and $\ker(A) \neq \{0\}$ *if and only if the product of the diagonal elements in* PA *is zero:*

$$\beta_{11}\beta_{22}\cdots\beta_{nn} = 0.$$

We are now ready to see how the process of calculating A_{rref} using row operations can be interpreted as a change of basis in the image space.

Two matrices $A, B \in \mathrm{Mat}_{n\times m}(\mathbb{F})$ are said to be *row equivalent* if we can find $P \in Gl_n(\mathbb{F})$ such that $A = PB$. Thus row equivalent matrices are the matrices that can be obtained from each other via row operations. We can also think of row equivalent matrices as being different matrix representations of the same linear map with respect to different bases in $\mathbb{F}^n$. To see this consider a linear map $L : \mathbb{F}^m \to \mathbb{F}^n$ that has matrix representation A with respect to the standard bases. If we perform a change of basis in $\mathbb{F}^n$ from the standard basis $f_1, ..., f_n$ to a basis $y_1, ..., y_n$ such that

$$\begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} = \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} P,$$

i.e., the columns of P are regarded as a new basis for $\mathbb{F}^n$, then $B = P^{-1}A$ is simply the matrix representation for $L : \mathbb{F}^m \to \mathbb{F}^n$ when we have changed the basis in $\mathbb{F}^n$ according to P. This information can be encoded in the diagram

$$\begin{array}{ccc} \mathbb{F}^m & \xrightarrow{A} & \mathbb{F}^n \\ \downarrow 1_{\mathbb{F}^m} & & \downarrow 1_{\mathbb{F}^n} \\ \mathbb{F}^m & \xrightarrow{L} & \mathbb{F}^n \\ \uparrow 1_{\mathbb{F}^m} & & \uparrow P \\ \mathbb{F}^m & \xrightarrow{B} & \mathbb{F}^n \end{array}$$

When we consider abstract matrices rather than systems of equations we could equally well have performed column operations. This is accomplished by multiplying the elementary matrices on the right rather than the left. We can see explicitly what happens in the 2×2 case:

$$AI_{12} = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \alpha_{12} & \alpha_{11} \\ \alpha_{22} & \alpha_{21} \end{bmatrix}$$

$$AR_{12}(\alpha) = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \alpha\alpha_{11} + \alpha_{12} \\ \alpha_{21} & \alpha\alpha_{21} + \alpha_{22} \end{bmatrix}$$

$$AR_{21}(\alpha) = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix} = \begin{bmatrix} \alpha_{11} + \alpha\alpha_{12} & \alpha_{12} \\ \alpha_{21} + \alpha\alpha_{22} & \alpha_{22} \end{bmatrix}$$

$$AM_1(\alpha) = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha\alpha_{11} & \alpha_{12} \\ \alpha\alpha_{21} & \alpha_{22} \end{bmatrix}$$

$$AM_2(\alpha) = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \alpha \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \alpha\alpha_{12} \\ \alpha_{21} & \alpha\alpha_{22} \end{bmatrix}$$

The only important and slightly confusing thing to be aware of is that, while $R_{kl}(\alpha)$ as a row operation multiplies row l by α and then adds it to row k, it now multiplies column k by α and adds it to column l as a column operation. This is because AE_{kl} is the matric whose l^{th} column is the k^{th} column of A and whose other columns vanish.

Two matrices $A, B \in \text{Mat}_{n\times m}(\mathbb{F})$ are said to be *column equivalent* if $A = BQ$ for some $Q \in Gl_m(\mathbb{F})$. According to the above interpretation this corresponds to a change of basis in the domain space $\mathbb{F}^m$.

More generally we say that $A, B \in \text{Mat}_{n\times m}(\mathbb{F})$ are *equivalent* if $A = PBQ$, where $P \in Gl_n(\mathbb{F})$ and $Q \in Gl_m(\mathbb{F})$. The diagram for the change of basis then looks like

$$\begin{array}{ccc} \mathbb{F}^m & \xrightarrow{A} & \mathbb{F}^n \\ \downarrow 1_{\mathbb{F}^m} & & \downarrow 1_{\mathbb{F}^n} \\ \mathbb{F}^m & \xrightarrow{L} & \mathbb{F}^n \\ \uparrow Q^{-1} & & \uparrow P \\ \mathbb{F}^m & \xrightarrow{B} & \mathbb{F}^n \end{array}$$

In this way we see that two matrices are equivalent if and only if they are matrix representations for the same linear map. Recall from the previous section that any linear map between finite dimensional spaces always has a matrix representation of the form

$$\begin{bmatrix} 1 & \cdots & & 0 & & 0 \\ & \ddots & & & & \\ 0 & \cdots & 1 & \vdots & & \vdots \\ & & & 0 & & 0 \\ \vdots & & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}$$

where there are k ones in the diagonal if the linear map has rank k. This implies

Corollary 12. (Characterization of Equivalent Matrices) $A, B \in \text{Mat}_{n\times m}(\mathbb{F})$ *are equivalent if and only if they have the same rank. Moreover any matrix of rank k is equivalent to a matrix that has k ones on the diagonal and zeros elsewhere.*

13.1. Exercises.

(1) Find bases for kernel and image for the following matrices.

(a) $\begin{bmatrix} 1 & 3 & 5 & 1 \\ 2 & 0 & 6 & 0 \\ 0 & 1 & 7 & 2 \end{bmatrix}$

(b) $\begin{bmatrix} 1 & 2 \\ 0 & 3 \\ 1 & 4 \end{bmatrix}$

(c) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$

(d) $\begin{bmatrix} \alpha_{11} & 0 & \cdots & 0 \\ \alpha_{21} & \alpha_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{bmatrix}$ In this case it will be necessary to discuss whether or not $\alpha_{ii} = 0$ for each $i = 1, ..., n$.

(2) Find A^{-1} for each of the following matrices.

(a) $\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$

(b) $\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

(c) $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

(3) Let $A \in \mathrm{Mat}_{n\times m}(\mathbb{F})$. Show that we can find $P \in Gl_n(\mathbb{F})$ that is a product of matrices of the types I_{ij} and $R_{ij}(\alpha)$ such that PA is upper triangular.

(4) Let $A = \mathrm{Mat}_{n\times n}(\mathbb{F})$. We say that A has an LU decomposition if $A = LU$, where L is lower triangular with 1s on the diagonal and U is upper triangular. Show that A has an LU decomposition if all the *leading principal minors* are invertible. The leading principal $k \times k$ minor is the $k \times k$ submatrix gotten from A by eliminating the last $n - k$ rows and columns. Hint: Do Gauss elimination using only $R_{ij}(\alpha)$.

(5) Assume that $A = PB$,where $P \in Gl_n(\mathbb{F})$

(a) Show that $\ker(A) = \ker(B)$.

(b) Show that if the column vectors $y_{i_1}, ..., y_{i_k}$ of B form a basis for $\mathrm{im}(B)$, then the corresponding column vectors $x_{i_1}, ..., x_{i_k}$ for A form a basis for $\mathrm{im}(A)$.

(6) Let $A \in \mathrm{Mat}_{n\times m}(\mathbb{F})$.

(a) Show that the $m \times m$ elementary matrices $I_{ij}, R_{ij}(\alpha), M_i(\alpha)$ when multiplied on the right correspond to column operations.

(b) Show that we can find $Q \in Gl_m(\mathbb{F})$ such that AQ is lower triangular.

(c) Use this to conclude that $\mathrm{im}(A) = \mathrm{im}(AQ)$ and describe a basis for $\mathrm{im}(A)$.

(d) Use Q to find a basis for $\ker(A)$ given a basis for $\ker(AQ)$ and describe how you select a basis for $\ker(AQ)$.

(7) Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ be upper triangular.

(a) Show that $\dim(\ker(A)) \leq$ number of zero entries on the diagonal.

(b) Give an example where $\dim(\ker(A)) <$ number of zero entries on the diagonal.

(8) In this exercise you are asked to show some relationships between the elementary matrices.

(a) Show that $M_i(\alpha) = I_{ij} M_j(\alpha) I_{ji}$.
(b) Show that $R_{ij}(\alpha) = M_j\left(\alpha^{-1}\right) R_{ij}(1) M_j(\alpha)$.
(c) Show that $I_{ij} = R_{ij}(-1) R_{ji}(1) R_{ij}(-1) M_j(-1)$.
(d) Show that $R_{kl}(\alpha) = I_{ki} I_{lj} R_{ij}(\alpha) I_{jl} I_{ik}$, where in case $i = k$ or $j = k$ we interpret $I_{kk} = I_{ll} = 1_{\mathbb{F}^n}$.

(9) A matrix $A \in Gl_n(\mathbb{F})$ is a *permutation matrix* if $Ae_1 = e_{\sigma(i)}$ for some bijective map (permutation)

$$\sigma : \{1, ..., n\} \to \{1, ..., n\}.$$

(a) Show that

$$A = \sum_{i=1}^{n} E_{\sigma(i)i}$$

(b) Show that A is a permutation matrix if and only if A has exactly one entry in each row and column which is 1 and all other entries are zero.
(c) Show that A is a permutation matrix if and only if it is a product of the elementary matrices I_{ij}.

(10) Assume that we have two fields $\mathbb{F} \subset \mathbb{L}$, such as $\mathbb{R} \subset \mathbb{C}$, and consider $A \in \mathrm{Mat}_{n\times m}(\mathbb{F})$. Let $A_{\mathbb{L}} \in \mathrm{Mat}_{n\times m}(\mathbb{L})$ be the matrix A thought of as an element of $\mathrm{Mat}_{n\times m}(\mathbb{L})$. Show that $\dim_{\mathbb{F}}(\ker(A)) = \dim_{\mathbb{L}}(\ker(A_{\mathbb{L}}))$ and $\dim_{\mathbb{F}}(\mathrm{im}(A)) = \dim_{\mathbb{L}}(\mathrm{im}(A_{\mathbb{L}}))$. Hint: Show that A and $A_{\mathbb{L}}$ have the same reduced row echelon form.

(11) Given $\alpha_{ij} \in \mathbb{F}$ for $i < j$ and $i, j = 1, ..., n$ we wish to solve

$$\frac{\xi_i}{\xi_j} = \alpha_{ij}.$$

(a) Show that this system either has no solutions or infinitely many solutions. Hint: try $n = 2, 3$ first.
(b) Give conditions on α_{ij} that guarantee an infinite number of solutions.
(c) Rearrange this system into a linear system and explain the above results.

14. Dual Spaces*

For a vector space V over $\mathbb{F}$ we define the *dual vector space* $V' = \hom(V, \mathbb{F})$ as the set of linear functions on V. One often sees the notation V^* for V'. However, we have reserved V^* for the conjugate vector space to a complex vector space. When V is finite dimensional we know that V and V' have the same dimension. In this section we shall see how the dual vector space can be used as a substitute for an inner product on V in case V doesn't come with a natural inner product (see chapter 3 for the theory on inner product spaces).

We have a natural dual pairing $V \times V' \to \mathbb{F}$ defined by $(x, f) = f(x)$ for $x \in V$ and $f \in V'$. We are going to think of (x, f) as a sort of inner product between x and f. Using this notation will enable us to make the theory virtually the same as for inner product spaces. Observe that this pairing is linear in both variables. Linearity in the first variable is a consequence of using linear functions in the second variable. Linearity in the second variable is completely trivial:

$$\begin{aligned}(\alpha x+\beta y,f) &= f(\alpha x+\beta y)\\ &= \alpha f(x)+\beta f(y)\\ &= \alpha(x,f)+\beta(y,f),\\ (x,\alpha f+\beta g) &= (\alpha f+\beta g)(x)\\ &= \alpha f(x)+\beta g(x)\\ &= \alpha(x,f)+\beta(x,g).\end{aligned}$$

We start with our construction of a dual basis, these are similar to orthonormal bases. Let V have a basis $x_1,...,x_n$, and define linear functions f_i by $f_i(x_j)=\delta_{ij}$. Thus $(x_i,f_j)=f_j(x_i)=\delta_{ij}$.

Example 44. *Recall that we defined* $dx^i:\mathbb{R}^n\to\mathbb{R}$ *as the linear function such that* $dx^i(e_j)=\delta_{ij}$, *where* $e_1,...,e_n$ *is the canonical basis for* $\mathbb{R}^n$.*Thus* dx^i *is the dual basis to the canonical basis.*

Proposition 4. *The vectors* $f_1,...,f_n$ *for* V' *form a basis called the* dual basis *of* $x_1,...,x_n$. *Moreover for* $x\in V$ *and* $f\in V'$ *we have the expansions*

$$\begin{aligned}x &= (x,f_1)x_1+\cdots+(x,f_n)x_n,\\ f &= (x_1,f)f_1+\cdots+(x_n,f)f_n.\end{aligned}$$

Proof. Consider a linear combination $\alpha_1f_1+\cdots+\alpha_nf_n$. Then

$$\begin{aligned}(x_i,\alpha_1f_1+\cdots+\alpha_nf_n) &= \alpha_1(x_i,f_1)+\cdots+\alpha_n(x_i,f_n)\\ &= \alpha_i.\end{aligned}$$

Thus $\alpha_i=0$ if $\alpha_1f_1+\cdots+\alpha_nf_n=0$. Since V and V' have the same dimension this shows that $f_1,....f_n$ form a basis for V'. Moreover, if we have an expansion $f=\alpha_1f_1+\cdots+\alpha_nf_n$, then it follows that $\alpha_i=(x_i,f)=f(x_i)$.

Finally assume that $x=\beta_1x_1+\cdots+\beta_nx_n$. Then

$$\begin{aligned}(x,f_i) &= (\beta_1x_1+\cdots+\beta_nx_n,f_i)\\ &= \beta_1(x_1,f_i)+\cdots+\beta_n(x_n,f_i)\\ &= \beta_i,\end{aligned}$$

which is what we wanted to prove. □

Next we define annihilators, these are counter parts to orthogonal complements. Let $M\subset V$ be a subspace and define the *annihilator* to M in V as the subspace $M^0\subset V'$ given by

$$\begin{aligned}M^o &= \{f\in V':(x,f)=0\text{ for all }x\in M\}\\ &= \{f\in V':f(x)=0\text{ for all }x\in M\}\\ &= \{f\in V':f(M)=\{0\}\}\\ &= \{f\in V':f|_M=0\}.\end{aligned}$$

Using dual bases we can get a slightly better grip on these annihilators.

Proposition 5. *If* $M\subset V$ *is a subspace of a finite dimensional space and* $x_1,...,x_n$ *is a basis for* V *such that*

$$M=\operatorname{span}\{x_1,...,x_m\},$$

then

$$M^o = \text{span}\{f_{m+1}, ..., f_n\}$$

where $f_1, ..., f_n$ *is the dual basis. In particular we have*

$$\dim(M) + \dim(M^o) = \dim(V) = \dim(V').$$

PROOF. If $M = \text{span}\{x_1, ..., x_m\}$, then $f_{m+1}, ..., f_n \in M^o$ by definition of the annihilator as each of $f_{m+1}, ..., f_n$ vanish on the vectors $x_1, ..., x_m$. Conversely take $f \in M^o$ and expand it $f = \alpha_1 f_1 + \cdots + \alpha_n f_n$. If $1 \le i \le m$, then

$$0 = (x_i, f) = \alpha_i.$$

So $f = \alpha_{m+1} f_{m+1} + \cdots + \alpha_n f_n$ as desired. □

We now wish to establish the *reflexive* property. This will allow us to go from V' back to V itself rather than to $(V')' = V''$. Thus we have to find a natural identification $V \to V''$. There is, indeed a natural linear map that takes each $x \in V$ to a linear function on V' defined by $\text{ev}_x(f) = (x, f) = f(x)$. To see that it is linear observe that

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

Evidently we have defined ev_x in such a way that

$$(x, f) = (f, \text{ev}_x).$$

Next note that if V is finite dimensional, then the kernel of $x \to \text{ev}_x$ is $\{0\}$. To prove this we select a dual basis $f_1, ..., f_n$ for V' and observe that since $\text{ev}_x(f_i) = (x, f_i)$ records the coordinates of x it is not possible for x to be in the kernel unless it is zero. Finally we use that $\dim(V) = \dim(V') = \dim(V'')$ to conclude that this map is an isomorphism. Thus any element of V'' is of the form ev_x for a unique $x \in V$.

The first interesting observation we make is that if $f_1, ..., f_n$ is dual to $x_1, ..., x_n$, then $\text{ev}_{x_1}, ..., \text{ev}_{x_n}$ is dual to $f_1, ..., f_n$ as

$$\text{ev}_{x_i}(f_j) = (x_i, f_j) = \delta_{ij}.$$

If we agree to identify V'' with V, i.e., we think of x as identified with ev_x, then we can define the annihilator of a subspace $N \subset V'$ as

$$\begin{aligned}N^o &= \{x \in V : (x, f) = 0 \text{ for all } f \in N\} \\ &= \{x \in V : f(x) = 0 \text{ for all } f \in N\}.\end{aligned}$$

We then claim that for $M \subset V$ and $N \subset V'$ we have $M^{oo} = M$ and $N^{oo} = N$. Both identities follow directly from the above proposition about the construction of a basis for the annihilator.

Next we observe an interesting relationship between annihilators and the dual spaces of subspaces.

PROPOSITION 6. *Assume that the finite dimensional space* $V = M \oplus N$, *then also* $V' = M^o \oplus N^o$ *and the restriction maps* $V' \to M'$ *and* $V' \to N'$ *give isomorphisms*

$$\begin{aligned}M^o &\approx N', \\ N^o &\approx M'.\end{aligned}$$

Proof. Select a basis $x_1, ..., x_n$ for V such that

$$\begin{aligned} M &= \operatorname{span}\{x_1, ..., x_m\}, \\ N &= \operatorname{span}\{x_{m+1}, ..., x_n\}. \end{aligned}$$

Then let $f_1, ..., f_n$ be the dual basis and simply observe that

$$\begin{aligned} M^o &= \operatorname{span}\{f_{m+1}, ..., f_n\}, \\ N^o &= \operatorname{span}\{f_1, ..., f_m\}. \end{aligned}$$

This proves that $V' = M^o \oplus N^o$. Next we note that

$$\begin{aligned} \dim(M^o) &= \dim(V) - \dim(M) \\ &= \dim(N) \\ &= \dim(N'). \end{aligned}$$

So at least M^o and N' have the same dimension. What is more, if we restrict $f_{m+1}, ..., f_n$ to N, then we still have that $(x_j, f_i) = \delta_{ij}$ for $j = m+1, ..., n$. As $N = \operatorname{span}\{x_{m+1}, ..., x_n\}$, this means that $f_{m+1}|_N, ..., f_n|_N$ form a basis for N'. The proof that $N^o \approx M'$ is similar. □

The main problem with using dual spaces rather than inner products is that while we usually have a good picture of what V is we rarely get a good description of the dual space. Thus the constructions mentioned here should be thought of as being theoretical and strictly auxiliary to the developments of the theory of linear operators on a fixed vector space V.

Below we consider a few examples of constructions of dual spaces.

Example 45. *Let $V = \operatorname{Mat}_{n\times m}(\mathbb{F})$, then we can identify $V' = \operatorname{Mat}_{m\times n}(\mathbb{F})$. For each $A \in \operatorname{Mat}_{m\times n}(\mathbb{F})$, the corresponding linear function is*

$$f_A(X) = \operatorname{tr}(AX) = \operatorname{tr}(XA).$$

Example 46. *If V is a finite dimensional inner product space then $f_y(x) = (x|y)$ defines a linear function and we know that all linear functions are of that form. Thus we can identify V' with V. Note however that in the complex case $y \to f_y$ is not complex linear. It is in fact conjugate linear, i.e., $f_{\lambda y} = \bar{\lambda} f_y$. Thus V' is identified with V^* where $V = V^*$ as real vector spaces but in V^* we have the modified scalar multiplication $\lambda * x = \bar{\lambda} x$. This conforms with the idea that the inner product defines a bilinear paring on $V \times V^*$ via $(x, y) \to (x, y)$ that is linear in both variables!*

Example 47. *If we think of V as $\mathbb{R}$ with $\mathbb{Q}$ as scalar multiplication, then it is not at all clear that we have any linear functions $f : \mathbb{R} \to \mathbb{Q}$. In fact the Axiom of Choice has to be invoked in order to show that they exist.*

Example 48. *Finally we have an exceedingly intereting infinite dimensional examples wehere the dual gets quite a bit bigger. Let $V = \mathbb{F}[t]$ be the vector space of polynomials. We have a natural basis $1, t, t^2, ...$. Thus a linear map $f : \mathbb{F}[t] \to \mathbb{F}$ is determined by it values on this basis $\alpha_n = f(t^n)$. Coversely given an infinite sequence $\alpha_0, \alpha_1, \alpha_2, ... \in \mathbb{F}$ we have a linear map such that $f(t^n) = \alpha_n$. So while V consists of finite seqeunces of elements from $\mathbb{F}$, the dual consists of infinite seqeunces of elemnts from $\mathbb{F}$. We can evidently identify $V' = \mathbb{F}[[t]]$ we power series by* *recording the values on the basis as coefficients*

$$\sum_{n=0}^{\infty} \alpha_n t^n = \sum_{n=0}^{\infty} f(n)\, t^n.$$

This means that V' inherits a product structure through taking products of power series. There is a large literature on this whole set-up under the title Umbral Calculus. *For more on this see* [**Roman**].

The dual space construction leads to a *dual map* $L' : W' \to V'$ for a linear map $L : V \to W$. This dual map is a generalization of the transpose of a matrix. The definition is very simple

$$L'(g) = g \circ L.$$

Thus if $g \in W'$ we get a linear function $g \circ L : V \to \mathbb{F}$ since $L : V \to W$. The dual to L is often denoted $L' = L^t$ as with matrices. This will be justified in the exercises to this section. Note that if we use the pairing (x, f) between V and V' then the dual map satisfies

$$(L(x), g) = (x, L'(g))$$

for all $x \in V$ and $g \in W'$. Thus the the dual map really is defined in a manner analogous to the adjoint.

The following properties follow almost immediately from the definition.

Proposition 7. *Let $L, \tilde{L} : V \to W$ and $K : W \to U$, then*

(1) $\left(\alpha L + \beta \tilde{L}\right)' = \alpha L' + \beta \tilde{L}'$.
(2) $(K \circ L)' = L' \circ K'$.
(3) $L'' = (L')' = L$ *if we identify* $V'' = V$ *and* $W'' = W$.
(4) *If* $M \subset V$ *and* $N \subset W$ *are subspaces with* $L(M) \subset N$, *then* $L'(N^o) \subset M^o$.

Proof. 1. Just note that

$$\begin{aligned} \left(\alpha L + \beta \tilde{L}\right)'(g) &= g \circ \left(\alpha L + \beta \tilde{L}\right) \\ &= \alpha g \circ L + \beta g \circ \tilde{L} \\ &= \alpha L'(g) + \beta \tilde{L}'(g) \end{aligned}$$

as g is linear.

2. This comes from

$$\begin{aligned} (K \circ L)'(h) &= h \circ (K \circ L) \\ &= (h \circ K) \circ L \\ &= K'(h) \circ L \\ &= L'(K'(h)). \end{aligned}$$

3. Note that $L'' : V'' \to W''$. If we take $\mathrm{ev}_x \in V''$ and use $(x, f) = (f, \mathrm{ev}_x)$ then

$$\begin{aligned} (g, L''(\mathrm{ev}_x)) &= (L'(g), \mathrm{ev}_x) \\ &= (x, L'(g)) \\ &= (L(x), g). \end{aligned}$$

This shows that $L''(\mathrm{ev}_x)$ is identified with $L(x)$ as desired.

4. If $g \in V'$, then we have that $(x, L'(g)) = (L(x), g)$. So if $x \in M$, then we have $L(x) \in N$ and hence $g(L(x)) = 0$ for $g \in N^o$. This means that $L'(g) \in M^o$. □

Just like for adjoint maps we have a type of Fredholm alternative for dual maps.

THEOREM 13. (The Generalized Fredholm Alternative) *Let $L : V \to W$ be a linear map between finite dimensional vector spaces. Then*

$$\begin{aligned} \ker(L) &= \operatorname{im}(L')^o, \\ \ker(L') &= \operatorname{im}(L)^o, \\ \ker(L)^o &= \operatorname{im}(L'), \\ \ker(L')^o &= \operatorname{im}(L). \end{aligned}$$

PROOF. We only need to prove the first statement as $L'' = L$ and $M^{oo} = M$.

$$\begin{aligned} \ker(L) &= \{x \in V : Lx = 0\}, \\ \operatorname{im}(L')^o &= \{x \in V : (x, L'(g)) = 0 \text{ for all } g \in W\}. \end{aligned}$$

Using that $(x, L'(g)) = (L(x), g)$ we note first that if $x \in \ker(L)$, then it must also belong to $\operatorname{im}(L')^o$. Conversely if $0 = (x, L'(g)) = (L(x), g)$ for all $g \in W$ it must follow that $L(x) = 0$ and hence $x \in \ker(L)$. □

As a corollary we get.

COROLLARY 13. (The Rank Theorem) *Let $L : V \to W$ be a linear map between finite dimensional vector spaces. Then*

$$\operatorname{rank}(L) = \operatorname{rank}(L').$$

14.1. Exercises.

(1) Let $x_1, .., x_n$ be a basis for V and $f_1, ..., f_n$ a dual basis for V'. Show that the inverses to the isomorphisms

$$\begin{aligned} \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} &: \mathbb{F}^n \to V, \\ \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} &: \mathbb{F}^n \to V' \end{aligned}$$

are given by

$$\begin{aligned} \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^{-1}(x) &= \begin{bmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{bmatrix}, \\ \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix}^{-1}(f) &= \begin{bmatrix} f(x_1) \\ \vdots \\ f(x_n) \end{bmatrix}. \end{aligned}$$

(2) Let $L : V \to W$ with basis $x_1, ..., x_m$ for V, $y_1, ..., y_n$ for W and dual basis $g_1, ..., g_n$ for W'. Show that we have

$$\begin{aligned} L &= \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} [L] \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix}^{-1} \\ &= \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} [L] \begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix} \end{aligned}$$

where $[L]$ is the matrix representation for L with respect to the given bases.

(3) Given the basis $1, t, t^2$ for P_2 identify P_2 with $\mathbb{C}^3$ and $(P_2)'$ with $\mathrm{Mat}_{1\times 3}(\mathbb{C})$.
  (a) Using these identifications find a dual basis to $1, 1+t, 1+t+t^2$ in $(P_2)'$.
  (b) Using these identifications find the matrix representation for $f \in (P_2)'$ defined by
$$f(p) = p(t_0).$$
  (c) Using these identifications find the matrix representation for $f \in (P_2)'$ defined by
$$f(p) = \int_a^b p(t)\,dt.$$
  (d) Are all elements of $(P_2)'$ represented by the types described in either b or c?

(4) Let $f, g \in V'$ and assume that $g \neq 0$. Show that $f = \lambda g$ for some $\lambda \in \mathbb{F}$ if and only if $\ker(f) \supset \ker(g)$.

(5) Let $M \subset V$ be a subspace. Show that we have linear maps
$$M^o \overset{i}{\to} V' \overset{\pi}{\to} M',$$
where ι is one-to-one, π is onto, and $\mathrm{im}(i) = \ker(\pi)$. Conclude that V' is isomorphic to $M^o \times M'$.

(6) Let V and W be finite dimensional vector spaces. Exhibit an isomorphism between $V' \times W'$ and $(V \times W)'$ that does not depend on choosing bases for V and W.

(7) Let $M, N \subset V$ be subspaces of a finite dimensional vector space. Show that
$$\begin{aligned} M^o + N^o &= (M \cap N)^o, \\ (M+N)^o &= M^o \cap N^o. \end{aligned}$$

(8) Let $L : V \to W$ and assume that we have bases $x_1, ..., x_m$ for V, $y_1, ..., y_n$ for W and corresponding dual bases $f_1, ..., f_m$ for V' and $g_1, ..., g_n$ for W'. Show that if $[L]$ is the matrix representation for L with respect to the given bases, then $[L]^t = [L']$ with respect to the dual bases.

(9) Assume that $L : V \to W$ is a linear map and that $L(M) \subset N$ for subspaces $M \subset V$ and $N \subset W$. Is there a relationship between $(L|_M)' : N' \to M'$ and $L'|_{N^o} : N^o \to M^o$?

(10) *(The Rank Theorem)* This exercise is an abstract version of what happened in the proof of the rank theorem in "Linear Independence". Let $L : V \to W$ and $x_1, ..., x_k$ a basis for $\mathrm{im}(L)$.
  (a) Show that
$$L(x) = (x, f_1)\,x_1 + \cdots + (x, f_k)\,x_k$$
  for suitable $f_1, ..., f_k \in V'$.
  (b) Show that
$$L'(f) = (x_1, f)\,f_1 + \cdots + (x_k, f)\,f_k$$
  for $f \in W'$.

(c) Conclude that $\text{rank}(L') \leq \text{rank}(L)$.
(d) Show that $\text{rank}(L') = \text{rank}(L)$.

(11) Let $M \subset V$ be a finite dimensional subspace of V and $x_1, ..., x_k$ a basis for M. Let

$$L(x) = (x, f_1)x_1 + \cdots + (x, f_k)x_k$$

for $f_1, ..., f_k \in V'$

(a) If $(x_j, f_i) = \delta_{ij}$, then L is a projection onto M, i.e., $L^2 = L$ and $\text{im}(L) = M$.
(b) If E is a projection onto M, then

$$E = (x, f_1)x_1 + \cdots + (x, f_k)x_k,$$

with $(x_j, f_i) = \delta_{ij}$.

(12) Let $M, N \subset V$ be subspaces of a finite dimensional vector space and consider $L : M \times N \to V$ defined by $L(x, y) = x - y$.

(a) Show that $L'(f)(x, y) = f(x) - f(y)$.
(b) Show that $\ker(L')$ can be identified with both $M^o \cap N^o$ and $(M + N)^o$.

15. Quotient Spaces*

In "Dual Spaces" we saw that if $M \subset V$ is a subspace of a general vector space, then the annihilator subspace $M^o \subset V'$ can play the role of a canonical complement of M. One thing missing from this set-up, however, is the projection whose kernel is M. In this section we shall construct a different type of vector space that can substitute as a complement to M. It is called the *quotient space* of V over M and is denoted V/M. In this case there is an onto linear map $P : V \to V/M$ whose kernel is M. The quotient space construction is somewhat abstract, but it is also quite general and can be developed with a minimum of information as we shall see. It is in fact quite fundamental and can be used to prove several of the important results mentioned "Linear Maps and Subspaces".

Similar to addition for subspaces in "Subspaces" we can in fact define addition for any subsets of a vector space. If $S, T \subset V$ are subsets then we define

$$S + T = \{x + y : x \in S \text{ and } y \in T\}.$$

It is immediately clear that this addition on subsets is associative and commutative. In case one of the sets contains only one element we simplify the notation by writing

$$S + \{x_0\} = S + x_0 = \{x + x_0 : x \in S\}$$

and we call $S + x_0$ a *translate* of S. Geometrically all of the sets $S + x_0$ appear to be parallel pictures of S that are translated in V as we change x_0. We also say that S and T are *parallel* and denoted it $S \parallel T$ if $T = S + x_0$ for some $x_0 \in V$.

It is also possible to scale subsets

$$\alpha S = \{\alpha x : x \in S\}.$$

This scalar multiplication satisfies some of the usual properties of scalar multiplication

$$\begin{aligned} (\alpha\beta) S &= \alpha(\beta S), \\ 1S &= S, \\ \alpha(S+T) &= \alpha S + \alpha T. \end{aligned}$$

However, the other distributive law can fail

$$(\alpha+\beta) S \stackrel{?}{=} \alpha S + \beta S$$

since it may not be true that

$$2S \stackrel{?}{=} S + S.$$

Certainly $2S \subset S + S$, but elements $x + y$ do not have to belong to $2S$ if $x, y \in S$ are distinct. Take, e.g., $S = \{x, -x\}$, where $x \neq 0$. Then $2S = \{2x, -2x\}$, while $S + S = \{2x, 0, -2x\}$.

Our picture of the quotient space V/M, when $M \subset V$ is a subspace, is the set of all translates $M + x_0$ for $x_0 \in V$

$$V/M = \{M + x_0 : x_0 \in V\}$$

Several of these translates are in fact equal as

$$x_1 + M = x_2 + M$$

precisely when $x_1 - x_2 \in M$. To see why this is, note that if $z \in M$, then $z + M = M$ since M is a subspace. Thus $x_1 - x_2 \in M$ implies that

$$\begin{aligned} x_1 + M &= x_2 + (x_1 - x_2) + M \\ &= x_2 + M. \end{aligned}$$

Conversely if $x_1 + M = x_2 + M$, then $x_1 = x_2 + x$ for some $x \in M$ implying that $x_1 - x_2 \in M$.

We see that in the trivial case where $M = \{0\}$ the translates of $\{0\}$ can be identified with V itself. Thus $V/\{0\} = V$. In the other trivial case where $M = V$ all the translates are simply V itself. So V/V contains only the element V.

We now need to see how addition and scalar multiplication works on V/M. The important property that simplifies calculations and will turn V/M into a vector space is the fact that M is a subspace. Thus for all scalars $\alpha, \beta \in \mathbb{F}$ we have

$$\alpha M + \beta M = M.$$

This implies that addition and scalar multiplication is considerably simplified.

$$\begin{aligned} \alpha(M+x) + \beta(M+y) &= \alpha M + \beta M + \alpha x + \beta y \\ &= M + \alpha x + \beta y. \end{aligned}$$

With this in mind we can show that V/M is a vector space. The zero element is M since $M + (M + x_0) = M + x_0$. The negative of $M + x_0$ is the translate $M - x_0$.

Finally the important distributive law that wasn't true in general also holds because

$$\begin{aligned}(\alpha+\beta)(M+x_0) &= M+(\alpha+\beta)x_0\\ &= M+\alpha x_0+\beta x_0\\ &= (M+\alpha x_0)+(M+\beta x_0)\\ &= \alpha(M+x_0)+\beta(M+x_0).\end{aligned}$$

The 'projection' $P : V \to V/M$ is now defined by

$$P(x) = M + x.$$

Clearly P is onto and $P(x) = 0$ if and only if $x \in M$. The fact that P is linear follows from the way we add elements in V/M

$$\begin{aligned}P(\alpha x+\beta y) &= M+\alpha x+\beta y\\ &= \alpha(M+x)+\beta(M+y)\\ &= \alpha P(x)+\beta P(y).\end{aligned}$$

This projection can be generalized to the setting where $M \subset N \subset V$. Here we get $V/M \to V/N$ by mapping $x + M$ to $x + N$.

If $L : V \to W$ and $M \subset V$, $L(M) \subset N \subset W$, then we get an induced map $L : V/M \to W/N$ by sending $x+M$ to $L(x)+N$. We need to check that this indeed gives a well-defined map. Assuming that $x_1 + M = x_2 + M$, we have to show that $L(x_1) + N = L(x_2) + N$. The first condition is equivalent to $x_1 - x_2 \in M$, thus

$$\begin{aligned}L(x_1)-L(x_2) &= L(x_1-x_2)\\ &\in L(M)\subset N,\end{aligned}$$

implying that $L(x_1) + N = L(x_2) + N$.

We are now going to investigate how the quotient space can be used to understand some of the developments from "Linear Maps and Subspaces". For any linear map we have that $L(\ker(L)) = \{0\}$. Thus L induces a linear map

$$V/(\ker(L)) \to W/\{0\} \approx W.$$

Since the image of $\ker(L) + x$ is $\{0\} + L(x) \approx x$, we see that the induced map has trivial kernel. This implies that we have an isomorphism

$$V/(\ker(L)) \to \operatorname{im}(L).$$

We can put all of this into a commutative diagram

$$\begin{array}{ccc} V & \xrightarrow{L} & W\\ P\downarrow & & \uparrow\\ V/(\ker(L)) & \xrightarrow{\approx} & \operatorname{im}(L)\end{array}$$

Note that, as yet, we have not used any of the facts we know about finite dimensional spaces. The two facts we shall assume are that the dimension of a vector space is well-defined and that any subspace in a finite dimensional vector space has a finite dimensional complement (see "Subspaces"). We start by considering subspaces.

Theorem 14. (The Subspace Theorem) *Let V be a finite dimensional vector space. If $M \subset V$ is a subspace, then both M and V/M are finite dimensional and*

$$\dim V = \dim M + \dim(V/M).$$

Proof. We start by selecting a subspace $N \subset V$ that is complementary to M. If we restrict the projection $P : V \to V/M$ to $P|_N : N \to V/M$, then it has no kernel as $M \cap N = \{0\}$. On the other hand since any $z \in V$ can be written as $z = x + y$ where $x \in M$ and $y \in N$, we see that

$$\begin{aligned} M + z &= M + x + y \\ &= M + y \\ &= P(y). \end{aligned}$$

Thus $P|_N : N \to V/M$ is an isomorphism. This shows that V/M is finite dimensional if we picked N to be finite dimensional. In the same way we see that the projection $Q : V \to V/N$ restricts to an isomorphism $Q|_M : M \to V/N$. By selecting a finite dimensional complement for $N \subset V$ we also get that V/N is finite dimensional. This shows that M is finite dimensional.

We can now use that $V = M \oplus N$ to show that

$$\begin{aligned} \dim V &= \dim M + \dim N \\ &= \dim M + \dim(V/M). \end{aligned}$$

□

The dimension formula now follows from our observations above.

Corollary 14. (The Dimension Formula) *Let V be a finite dimensional vector space. If $L : V \to W$ is a linear map, then*

$$\dim V = \dim(\ker(L)) + \dim(\operatorname{im}(L)).$$

Proof. We just saw that

$$\dim V = \dim(\ker(L)) + \dim(V/(\ker(L))).$$

In addition we have an isomorphism

$$V/(\ker(L)) \longrightarrow \operatorname{im}(L).$$

This proves the claim. □

15.1. Exercises.

(1) An affine subspace $A \subset V$ is a subset such that if $x_1, ..., x_k \in A$, $\alpha_1, ..., \alpha_k \in \mathbb{F}$, and $\alpha_1 + \cdots + \alpha_k = 1$, then $\alpha_1 x_1 + \cdots + \alpha_k x_k \in A$. Show that V/M consists of all of the affine subspaces parallel to M.

(2) Find an example of a nonzero linear operator $L : V \to V$ and a subspace $M \subset V$ such that $L|_M = 0$ and the induced map $L : V/M \to V/M$ is also zero.

(3) This exercise requires knowledge of the characteristic polynomial. Let $L : V \to V$ be a linear operator with an invariant subspace $M \subset V$. Show that $\chi_L(t)$ is the product of the characteristic polynomials of $L|_M$ and the induced map $L : V/M \to V/M$.

(4) Let $M \subset V$ be a subspace and assume that we have $x_1, ..., x_n \in V$ such that $x_1, ..., x_k$ form a basis for M and $x_{k+1} + M, ..., x_n + M$ form a basis for V/M. Show that $x_1, ..., x_n$ is a basis for V.

(5) Let $L : V \to W$ be a linear map and assume that $L(M) \subset N$. How does the induced map $L : V/M \to W/N$ compare to the dual maps constructed in exercise 2 in "Dual Maps".

(6) Let $M \subset V$ be a subspace. Show that there is a natural isomorphism $M^o \to (V/M)'$, i.e., an isomorphism that doesn't depend on a choice of basis for the spaces.

CHAPTER 2

Linear Operators

In this chapter we are going to present all of the results that relate to linear operators on abstract finite dimensional vector spaces. Aside from a section on polynomials we start with a section on linear differential equations in order to motivate both some material from chapter 1 and also give a reason for why it is desirable to study matrix representations. Eigenvectors and eigenvalues are first introduced in the context of differential equations where they are used to solve such equations. It is, however, possible to start with the section "Eigenvalues" and ignore the discussion on differential equations. The material developed in chapter 1 on Gauss elimination is used to calculate eigenvalues and vectors and to give a weak definition of the characteristic polynomial. We also introduce the minimal polynomial and use it to characterize diagonalizable maps. We then move on to cyclic subspaces leading us to fairly simple proofs of the Cayley-Hamilton Theorem and the cyclic subspace decomposition. This in turn gives us a nice proof of the Frobenius canonical from. We finish with a discussion of the Jordan Canonical form.

Various properties of polynomials are used quite a bit in this chapter. Most of these properties are probably already known to the student and in any case are ceratinly well-known from arithmetic of integers, nevertheless we have chosen to collect some them in an optional section at the beginning of this chapter.

It is possible to simply cover the sections "Eigenvalues" and "Diagonalizability" and then move on to the chapters on inner product spaces. In fact it is possible to skip this chapter entirely as it isn't really used in the theory of inner product spaces.

1. Polynomials*

The space of polynomials with coefficients in the field $\mathbb{F}$ is denoted $\mathbb{F}[t]$. This space consists of expressions of the form

$$\alpha_0 + \alpha_1 t + \cdots + \alpha_k t^k$$

where $\alpha_0, ..., \alpha_k \in \mathbb{F}$ and k is a nonnegative integer. One can think of these expressions as functions on $\mathbb{F}$, but in this section we shall only use the formal algebraic structure that comes from writing polynomials in the above fashion. Recall that integers are written in a similar way if we use the standard positional base 10 system (or any other base for that matter)

$$a_k \cdots a_0 = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0.$$

Indeed there are many basic number theoretic similarities between integers and polynomials as we shall see below.

Addition is defined by adding term by term

$$\begin{aligned} & \left(\alpha_0+\alpha_1 t+\alpha_2 t^2+\cdots\right)+\left(\beta_0+\beta_1 t+\beta_2 t^2+\cdots\right) \\ = \quad & \left(\alpha_0+\beta_0\right)+\left(\alpha_1+\beta_1\right) t+\left(\alpha_2+\beta_2\right) t^2+\cdots \end{aligned}$$

Multiplication is a bit more complicated but still completely naturally defined by multiplying all the different terms and then collecting according to the powers of t

$$\begin{aligned} & \left(\alpha_0+\alpha_1 t+\alpha_2 t^2+\cdots\right) \cdot\left(\beta_0+\beta_1 t+\beta_2 t^2+\cdots\right) \\ = \quad & \alpha_0 \cdot \beta_0+\left(\alpha_0 \beta_1+\alpha_1 \beta_0\right) t+\left(\alpha_0 \beta_2+\alpha_1 \beta_1+\alpha_2 \beta_0\right) t^2+\cdots \end{aligned}$$

Note that in "addition" the indices match the power of t, while in "multiplication" each term has the property that the sum of the indices matches the power of t.

The *degree* of a polynomial $\alpha_0+\alpha_1 t+\cdots+\alpha_n t^n$ is the largest k such that $\alpha_k \neq 0$. In particular

$$\alpha_0+\alpha_1 t+\cdots+\alpha_k t^k+\cdots+\alpha_n t^n=\alpha_0+\alpha_1 t+\cdots+\alpha_k t^k,$$

where k is the degree of the polynomial. We also write $\deg(p)=k$. The degree satisfies the following elementary properties

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

Note that if $\deg(p)=0$ then $p(t)=\alpha_0$ is simply a scalar.

We are now ready to discuss the "number theoretic" properties of polynomials. It is often convenient to work with *monic* polynomials. These are the polynomials of the form

$$\alpha_0+\alpha_1 t+\cdots+1 \cdot t^k.$$

Note that any polynomial can be made into a monic polynomial by diving by the scalar that appears in front of the term of highest degree. Working with monic polynomials is similar to working with positive integers rather than all integers.

If $p, q \in \mathbb{F}[t]$, then we say that p *divides* q if $q=pd$ for some $d \in \mathbb{F}[t]$. Note that if p divides q, then it must follow that $\deg(p) \leq \deg(q)$. The converse is of course not true, but polynomial long division gives us a very useful partial answer to what might happen.

THEOREM 15. (The Euclidean Algorithm) *If* $p, q \in \mathbb{F}[t]$ *and* $\deg(p) \leq \deg(q)$, *then* $q=pd+r$, *where* $\deg(r)<\deg(p)$.

PROOF. The proof is along the same lines as how we do long division with remainder. The idea of the Euclidean algorithm is that whenever $\deg(p) \leq \deg(q)$ it is possible to find d_1 and r_1 such that

$$\begin{aligned} q & = pd_1+r_1, \\ \deg(r_1) & < \deg(q). \end{aligned}$$

To establish this assume

$$\begin{aligned} q & = \alpha_n t^n+\alpha_{n-1} t^{n-1}+\cdots+\alpha_0, \\ p & = \beta_m t^m+\beta_{m-1} t^{m-1}+\cdots+\beta_0 \end{aligned}$$

where $\alpha_n, \beta_m \neq 0$. Then define $d_1 = \frac{\alpha_n}{\beta_m} t^{n-m}$ and

$$\begin{aligned} r_1 &= q - pd_1 \\ &= \left(\alpha_n t^n + \alpha_{n-1} t^{n-1} + \cdots + \alpha_0\right) \\ &\quad - \left(\beta_m t^m + \beta_{m-1} t^{m-1} + \cdots + \beta_0\right) \frac{\alpha_n}{\beta_m} t^{n-m} \\ &= \left(\alpha_n t^n + \alpha_{n-1} t^{n-1} + \cdots + \alpha_0\right) \\ &\quad - \left(\alpha_n t^n + \beta_{m-1} \frac{\alpha_n}{\beta_m} t^{n-1} + \cdots + \beta_0 \frac{\alpha_n}{\beta_m} t^{n-m}\right) \\ &= 0 \cdot t^n + \left(\alpha_{n-1} - \beta_{m-1} \frac{\alpha_n}{\beta_m}\right) t^{n-1} + \cdots \end{aligned}$$

Thus $\deg(r_1) < n = \deg(q)$.

If $\deg(r_1) < \deg(p)$ we are finished, otherwise we use the same construction to get

$$\begin{aligned} r_1 &= pd_2 + r_2, \\ \deg(r_2) &< \deg(r_1). \end{aligned}$$

We then continue this process and construct

$$\begin{aligned} r_k &= pd_{k+1} + r_{k+1}, \\ \deg(r_{k+1}) &< \deg(r_k). \end{aligned}$$

Eventually we must arrive at a situation where $\deg(r_k) \geq \deg(p)$ but $\deg(r_{k+1}) < \deg(p)$.

Collecting each step in this process we see that

$$\begin{aligned} q &= pd_1 + r_1 \\ &= pd_1 + pd_2 + r_2 \\ &= p(d_1 + d_2) + r_2 \\ &\vdots \\ &= p(d_1 + d_2 + \cdots + d_{k+1}) + r_{k+1}. \end{aligned}$$

This proves the theorem. □

The Euclidean algorithm is the central construction that makes all of the following results work.

Proposition 8. *Let $p \in \mathbb{F}[t]$ and $\lambda \in \mathbb{F}$. $(t-\lambda)$ divides p if and only if λ is a root of p, i.e., $p(\lambda) = 0$.*

Proof. If $(t-\lambda)$ divides p, then $p = (t-\lambda) q$. Hence $p(\lambda) = 0 \cdot q(\lambda) = 0$.

Conversely use the Euclidean algorithm to write

$$\begin{aligned} p &= (t-\lambda) q + r, \\ \deg(r) &< \deg(t-\lambda) = 1. \end{aligned}$$

This means that $r = \beta \in \mathbb{F}$. Now evaluate this at λ

$$\begin{aligned} 0 &= p(\lambda) \\ &= (\lambda - \lambda) q(\lambda) + r \\ &= r \\ &= \beta. \end{aligned}$$

Thus $r = 0$ and $p = (t - \lambda) q$. □

This gives us an important corollary.

COROLLARY 15. *Let $p \in \mathbb{F}[t]$. If $\deg(p) = k$, then p has no more than k roots.*

PROOF. We prove this by induction. When $k = 0$ or 1 there is nothing to prove. If p has a root $\lambda \in \mathbb{F}$, then $p = (t - \lambda) q$, where $\deg(q) < \deg(p)$. Thus q has no more than $\deg(q)$ roots. In addition we have that $\mu \neq \lambda$ is a root of p if and only if it is a root of q. Thus p cannot have more than $1 + \deg(q) \leq \deg(p)$ roots. □

In the next proposition we show that two polynomials always have a *greatest common divisor*.

PROPOSITION 9. *Let $p, q \in \mathbb{F}[t]$, then there is a unique monic polynomial $d = \gcd\{p, q\}$ with the property that if d_1 divides both p and q then d_1 divides d. Moreover, there are $r, s \in \mathbb{F}[t]$ such that $d = pr + qs$.*

PROOF. Let d be a monic polynomial of smallest degree such that $d = ps_1 + qs_2$. It is clear that any polynomial d_1 that divides p and q must also divide d. So we must show that d divides p and q. We show more generally that d divides all polynomials of the form $d' = ps_1' + qs_2'$. For such a polynomial we have $d' = du + r$ where $\deg(r) < \deg(d)$. This implies

$$\begin{aligned} r &= d' - du \\ &= p(s_1' - us_1) + q(s_2' - us_2). \end{aligned}$$

It must follow that $r = 0$ as we could otherwise find a monic polynomial of the form $ps_1'' + qs_2''$ of degree $< \deg(d)$. Thus d divides d'. In particular d must divide $p = p \cdot 1 + q \cdot 0$ and $q = p \cdot 0 + q \cdot 1$.

To check uniqueness assume d_1 is a monic polynomial with the property that any polynomial that divides p and q also divides d_1. This means that d divides d_1 and also that d_1 divides d. Since both polynomials are monic this shows that $d = d_1$. □

We can more generally show that for any finite collection $p_1, ..., p_n$ of polynomials there is a *greatest common divisor*

$$d = \gcd\{p_1, ..., p_n\}.$$

As in the above proposition the polynomial d is a monic polynomial of smallest degree such that

$$d = p_1 s_1 + \cdots + p_n s_n.$$

Moreover it has the property that any polynomial that divides $p_1, ..., p_n$ also divides d. The polynomials $p_1, ..., p_n \in \mathbb{F}[t]$ are said to be *relatively prime* or have *no common factors* if the only monic polynomial that divides $p_1, ..., p_n$ is 1. In other words $\gcd\{p_1, ..., p_n\} = 1$.

We can also show that two polynomials have a *least common multiple.*

PROPOSITION 10. *Let $p, q \in \mathbb{F}[t]$, then there is a unique monic polynomial $m = \operatorname{lcm}\{p, q\}$ with the property that if p and q divide m_1 then m divides m_1.*

PROOF. Let m be the monic polynomial of smallest degree that is divisible by both p and q. Note that such polynomials exists as pq is divisible by both p and q. Next suppose that p and q divide m_1. Since $\deg(m_1) \geq \deg(m)$ we have that $m_1 = sm + r$ with $\deg(r) < \deg(m)$. Since p and q divide m_1 and m, they must also divide $m_1 - sm = r$. As m has the smallest degree with this property it must follow that $r = 0$. Hence m divides m_1. □

A monic polynomial $p \in \mathbb{F}[t]$ of degree ≥ 1 is said to be *prime* or *irreducible* if the only monic polynomials from $\mathbb{F}[t]$ that divide p are 1 and p. The simplest irreducible polynomials are the linear ones $t - \alpha$. If the field $\mathbb{F} = \mathbb{C}$, then all irreducible polynomials are linear. While if the field $\mathbb{F} = \mathbb{R}$, then the only other irreducible polynomials are the quadratic ones $t^2 + \alpha t + \beta$ with negative discriminant $D = \alpha^2 - 4\beta < 0$. These two facts are not easy to prove and depend on the "Fundamental Theorem of Algebra" which we discuss below.

In analogy with the prime factorization of integers we also have a prime factorization of polynomials. Before establishing this decomposition we need to prove a very useful property for irreducible polynomials.

LEMMA 12. *Let $p \in \mathbb{F}[t]$ be irreducible. If p divides $q_1 \cdot q_2$, then p divides either q_1 or q_2.*

PROOF. Let $d_1 = \gcd(p, q_1)$. Since d_1 divides p it follows that $d_1 = 1$ or $d_1 = p$. In the latter case $d_1 = p$ divides q_1 so we are finished. If $d_1 = 1$, then we can write $1 = pr + q_1 s$. In particular

$$q_2 = q_2 pr + q_2 q_1 s.$$

Here we have that p divides $q_2 q_1$ and p. Thus it also divides

$$q_2 = q_2 pr + q_2 q_1 s.$$

□

THEOREM 16. (Unique Factorization of Polynomials) *Let $p \in \mathbb{F}[t]$ be a monic polynomial, then $p = p_1 \cdots p_k$ is a product of irreducible polynomials. Moreover, except for rearranging these polynomials this factorization is unique.*

PROOF. We can prove this result by induction on $\deg(p)$. If p is only divisible by 1 and p, then p is irreducible and we are finished. Otherwise $p = q_1 \cdot q_2$, where q_1 and q_2 are monic polynomials with $\deg(q_1), \deg(q_2) < \deg(p)$. By assumption each of these two factors can be decomposed into irreducible polynomials, hence we also get such a decomposition for p.

For uniqueness assume that $p = p_1 \cdots p_k = q_1 \cdots q_l$ are two decompositions of p into irreducible factors. Using induction again we see that it suffices to show that $p_1 = q_i$ for some i. The previous lemma now shows that p_1 must divide q_1 or $q_2 \cdots q_l$. In the former case it follows that $p_1 = q_1$ as q_1 is irreducible. In the latter case we get again that p_1 must divide q_2 or $q_3 \cdots q_l$. Continuing in this fashion it must follow that $p_1 = q_i$ for some i. □

If all the irreducible factors of a monic polynomial $p \in \mathbb{F}[t]$ are linear, then we say that that p *splits*. Thus p splits if and only if

$$p(t) = (t - \alpha_1) \cdots (t - \alpha_k)$$

for $\alpha_1, ..., \alpha_k \in \mathbb{F}$.

Finally we show that all complex polynomials have a root. It is curious that while this theorem is algebraic in nature the proof is analytic. There are many completely different proofs of this theorem including ones that are far more algebraic. The one presented here, however, seems to be the most elementary.

THEOREM 17. (The Fundamental Theorem of Algebra) *Any complex polynomial of degree ≥ 1 has a root.*

PROOF. Let $p(z) \in \mathbb{C}[z]$ have degree $n \geq 1$. Our first claim is that we can find $z_0 \in \mathbb{C}$ such that $|p(z)| \geq |p(z_0)|$ for all $z \in \mathbb{C}$. To see why $|p(z)|$ has to have a minimum we first observe that

$$\begin{aligned} \frac{p(z)}{z^n} &= \frac{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0}{z^n} \\ &= a_n + a_{n-1} \frac{1}{z} + \cdots + a_1 \frac{1}{z^{n-1}} + a_0 \frac{1}{z^n} \\ &\to a_n \text{ as } z \to \infty. \end{aligned}$$

Since $a_n \neq 0$, we can therefore choose $R > 0$ so that

$$|p(z)| \geq \frac{|a_n|}{2} |z|^n \text{ for } |z| \geq R.$$

By possibly increasing R further we can also assume that

$$\frac{|a_n|}{2} |R|^n \geq |p(0)|.$$

On the compact set $\bar{B}(0, R) = \{z \in \mathbb{C} : |z| \leq R\}$ we can now find z_0 such that $|p(z)| \geq |p(z_0)|$ for all $z \in \bar{B}(0, R)$. By our assumptions this also holds when $|z| \geq R$ since in that case

$$\begin{aligned} |p(z)| &\geq \frac{|a_n|}{2} |z|^n \\ &\geq \frac{|a_n|}{2} |R|^n \\ &\geq |p(0)| \\ &\geq |p(z_0)|. \end{aligned}$$

Thus we have found our global minimum for $|p(z)|$.

We now define a new polynomial of degree $n \geq 1$

$$q(z) = \frac{p(z + z_0)}{p(z_0)}.$$

This polynomial satisfies

$$\begin{aligned} q(0) &= \frac{p(z_0)}{p(z_0)} = 1, \\ |q(z)| &= \left|\frac{p(z+z_0)}{p(z_0)}\right| \\ &\geq \left|\frac{p(z_0)}{p(z_0)}\right| \\ &= 1 \end{aligned}$$

Thus

$$q(z) = 1 + b_k z^k + \cdots + b_n z^n$$

where $b_k \neq 0$. We can now investigate what happens to $q(z)$ for small z. We first note that

$$\begin{aligned} q(z) &= 1 + b_k z^k + b_{k+1} z^{k+1} + \cdots + b_n z^n \\ &= 1 + b_k z^k + \left(b_{k+1} z + \cdots + b_n z^{n-k}\right) z^k \end{aligned}$$

where

$$\left(b_{k+1} z \cdots + b_n z^{n-k}\right) \to 0 \text{ as } z \to 0.$$

If we write $z = re^{i\theta}$ and choose θ so that

$$b_k e^{ik\theta} = -|b_k|$$

then

$$\begin{aligned} |q(z)| &= \left|1 + b_k z^k + \left(b_{k+1} z \cdots + b_n z^{n-k}\right) z^k\right| \\ &= \left|1 - |b_k| r^k + \left(b_{k+1} z \cdots + b_n z^{n-k}\right) r^k e^{ik\theta}\right| \\ &\leq 1 - |b_k| r^k + \left|\left(b_{k+1} z \cdots + b_n z^{n-k}\right) r^k e^{ik\theta}\right| \\ &= 1 - |b_k| r^k + \left|b_{k+1} z \cdots + b_n z^{n-k}\right| r^k \\ &\leq 1 - \frac{|b_k|}{2} r^k \end{aligned}$$

as long as r is chosen so small that $1 - |b_k| r^k > 0$ and $\left|b_{k+1} z \cdots + b_n z^{n-k}\right| \leq \frac{|b_k|}{2}$. This, however, implies that $\left|q\left(re^{i\theta}\right)\right| < 1$ for small r. We have therefore arrived at a contradiction. □

2. Linear Differential Equations*

In this section we shall study linear differential equations. Everything we have learned about linear independence, bases, special matrix representations etc. will be extremely useful when trying to solve such equations. In fact we shall in several section of this text see that virtually every development in linear algebra can be used to understand the structure of solutions to linear differential equations. It is possible to skip this section if one doesn't want to be bothered by differential equations while learning linear algebra.

We start with systems of differential equations:

$$\begin{aligned} \dot{x}_1 &= a_{11} x_1 + \cdots + a_{1m} x_m + b_1 \\ \vdots \quad & \vdots \qquad\qquad \vdots \\ \dot{x}_m &= a_{n1} x_1 + \cdots + a_{nm} x_m + b_n \end{aligned}$$

where $a_{ij}, b_i \in C^\infty([a,b], \mathbb{C})$ (or just $C^\infty([a,b], \mathbb{R})$) and the functions $x_j : [a,b] \to \mathbb{C}$ are to be determined. We can write the system in matrix form and also rearrange it a bit to make it look like we are solving $L(x) = b$. To do this we use

$$x = \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix},\ b = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix},\ A = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix}$$

and define

$$\begin{aligned} L &: C^\infty([a,b], \mathbb{C}^m) \to C^\infty([a,b], \mathbb{C}^n) \\ L(x) &= \dot{x} - Ax. \end{aligned}$$

The equation $L(x) = 0$ is called the *homogeneous system.* We note that the following three properties can be used as a general outline for what to do.

(1) $L(x) = b$ can be solved if and only if $b \in \operatorname{im}(L)$.
(2) If $L(x_0) = b$ and $x \in \ker(L)$, then $L(x + x_0) = b$.
(3) If $L(x_0) = b$ and $L(x_1) = b$, then $x_0 - x_1 \in \ker(L)$.

The specific implementation of actually solving the equations, however, is quite different from what we did with systems of (algebraic) equations.

First of all we only consider the case where $n = m$. This implies that for given $t_0 \in [a,b]$ and $x_0 \in \mathbb{C}^n$ the *initial value problem*

$$\begin{aligned} L(x) &= b, \\ x(t_0) &= x_0 \end{aligned}$$

has a unique solution $x \in C^\infty([a,b], \mathbb{C}^n)$. We shall not prove this result in this generality, but we shall eventually see why this is true when the matrix A has entries that are constants rather than functions. As we learn more about linear algebra we shall revisit this problem and slowly try to gain a better understanding of it. For now let us just note an important consequence.

THEOREM 18. *The complete collection of solutions to*

$$\begin{aligned} \dot{x}_1 &= a_{11}x_1 + \cdots + a_{1n}x_n + b_1 \\ \vdots \quad & \vdots \qquad\qquad \vdots \\ \dot{x}_n &= a_{n1}x_1 + \cdots + a_{nn}x_n + b_n \end{aligned}$$

can be found by finding one solution x_0 and then adding it to the solutions of the homogeneous equation $L(z) = 0$, i.e.,

$$\begin{aligned} x &= z + x_0, \\ L(z) &= 0, \end{aligned}$$

moreover $\dim(\ker(L)) = n$.

Some particularly interesting and important linear equations are the n^{th} order equations

$$D^n x + a_{n-1}D^{n-1}x + \cdots + a_1 Dx + a_0 x = b,$$

where $D^k x$ is the k^{th} order derivative of x. If we assume that $a_{n-1}, ..., a_0, b \in C^\infty([a,b], \mathbb{C})$ and define

$$\begin{aligned} L &: C^\infty([a,b], \mathbb{C}) \to C^\infty([a,b], \mathbb{C}) \\ L(x) &= \left(D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0\right)(x), \end{aligned}$$

then we have a nice linear problem just as in the previous cases of linear systems of differential or algebraic equations. The problem of solving $L(x) = b$ can also be reinterpreted as a linear system of differential equations by defining

$$x_1 = x, x_2 = Dx, ..., x_n = D^{n-1}x$$

and then considering the system

$$\begin{array}{ccc}\dot{x}_1 & = & x_2 \\ \dot{x}_2 & = & x_3 \\ \vdots & \vdots & \vdots \\ \dot{x}_n & = & -a_{n-1}x_n - \cdots - a_1 x_2 - a_0 x_1 + b_n\end{array}$$

This won't help us in solving the desired equation, but it does tells us that the initial value problem

$$\begin{array}{rcl}L(x) & = & b, \\ x(t_0) & = & c_0, Dx(t_0) = c_1, ..., D^{n-1}x(t_0) = c_{n-1},\end{array}$$

has a unique solution and hence the above theorem can be paraphrased.

THEOREM 19. *The complete collection of solutions to*

$$D^n x + a_{n-1}D^{n-1}x + \cdots + a_1 Dx + a_0 x = b$$

can be found by finding one solution x_0 *and then adding it to the solutions of the homogeneous equation* $L(z) = 0$*, i.e.,*

$$\begin{array}{rcl}x & = & z + x_0, \\ L(z) & = & 0,\end{array}$$

moreover $\dim(\ker(L)) = n$.

It is not hard to give a complete account of how to solve the homogeneous problem $L(x) = 0$ when $a_0, ..., a_{n-1} \in \mathbb{C}$ are constants. Let us start with $n = 1$. Then we are trying to solve

$$Dx + a_0 x = \dot{x} + a_0 x = 0.$$

Clearly $x = \exp(-a_0 t)$ is a solution and the complete set of solutions is

$$x = c\exp(-a_0 t), c \in \mathbb{C}.$$

The initial value problem

$$\begin{array}{rcl}\dot{x} + a_0 x & = & 0, \\ x(t_0) & = & c_0\end{array}$$

has the solution

$$x = c_0 \exp(-a_0(t - t_0)).$$

The trick to solving the higher order case is to note that we can rewrite L as

$$\begin{array}{rcl}L & = & D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0 \\ & = & p(D).\end{array}$$

This makes L look like a polynomial where D is the variable. The corresponding polynomial

$$p(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$

is called the *characteristic polynomial*. The idea behind solving these equations comes from

PROPOSITION 11. (The Reduction Principle) *If* $q(t) = t^m + b_{m-1}t^{m-1} + \cdots + b_0$ *is a polynomial that divides* $p(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$*, then any solution to* $q(D)(x) = 0$ *is also a solution to* $p(D)(x) = 0$.

PROOF. This simply hinges of observing that $p(t) = r(t)q(t)$, then $p(D) = r(D)q(D)$. So by evalutaing the latter on x we get $p(D)(x) = r(D)(q(D)(x)) = 0$. □

The simplest factors are, of course, the linear factors $t - \lambda$ and we know that the solutions to

$$(D - \lambda)(x) = Dx - \lambda x = 0$$

are given by $x(t) = C\exp(\lambda t)$. This means that we should be looking for roots to $p(t)$. These roots are called *eigenvalues* or *characteristic values*. The Fundamental Theorem of Algebra asserts that any polynomial $p \in \mathbb{C}[t]$ can be factored over the complex numbers

$$\begin{aligned} p(t) &= t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \\ &= (t - \lambda_1)^{k_1} \cdots (t - \lambda_m)^{k_m}. \end{aligned}$$

Here the roots $\lambda_1, ..., \lambda_m$ are assumed to be distinct, each occurs with multiplicity $k_1, ..., k_m$, and $k_1 + \cdots + k_m = n$.

The original equation

$$L = D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0$$

then factors

$$\begin{aligned} L &= D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0 \\ &= (D - \lambda_1)^{k_1} \cdots (D - \lambda_m)^{k_m} \end{aligned}$$

and we reduce the original problem to solving the equations

$$\begin{aligned} (D - \lambda_1)^{k_1}(x) &= 0, \\ &\vdots \\ (D - \lambda_m)^{k_m}(x) &= 0. \end{aligned}$$

Note that if we had not insisted on using the more abstract and less natural complex numbers we would not have been able to make the reduction so easily. If we are in a case where the differential equation is real and there is a good physical reason for keeping solutions real as well, then we can still solve it as if it were complex and then take real and imaginary parts of the complex solutions to get real ones. It would seem that the n complex solutions would then lead to $2n$ real ones. This is not really the case. First observe that each real eigenvalue λ only gives rise to a one parameter family of real solutions $c\exp(\lambda(t - t_0))$. As for complex eigenvalues we know that real polynomials have the property that complex roots come in conjugate pairs. Then we note that $\exp(\lambda(t - t_0))$ and $\exp(\bar{\lambda}(t - t_0))$ up to sign have the same real and imaginary parts and so these pairs of eigenvalues only lead to a two parameter family of real solutions which if $\lambda = \lambda_1 + i\lambda_2$ looks like

$$c\exp(\lambda_1(t - t_0))\cos(\lambda_2(t - t_0)) + d\exp(\lambda_1(t - t_0))\sin(\lambda_2(t - t_0))$$

Let us return to the complex case again. If $m = n$ and $k_1 = \cdots = k_m = 1$, we simply get n first order equations and we see that the complete set of solutions to $L(x) = 0$ is given by

$$x = \alpha_1 \exp(\lambda_1 t) + \cdots + \alpha_n \exp(\lambda_n t).$$

It should be noted that we need to show that $\exp(\lambda_1 t), ..., \exp(\lambda_n t)$ are linearly independent in order to show that we have found all solutions. This was discussed in “Linear Independence" in chapter 1 and will also be established below in “Diagonalizability”.

With a view towards solving the initial value problem we rewrite the solution as

$$x = d_1 \exp(\lambda_1 (t - t_0)) + \cdots + d_n \exp(\lambda_n (t - t_0)).$$

To solve the initial value problem requires differentiating this expression several times and then solving

$$\begin{aligned} x(t_0) &= d_1 + \cdots + d_n, \\ Dx(t_0) &= \lambda_1 d_1 + \cdots + \lambda_n d_n, \\ &\vdots \\ D^{n-1} x(t_0) &= \lambda_1^{n-1} d_1 + \cdots + \lambda_n^{n-1} d_n \end{aligned}$$

for $d_1, ..., d_n$. In matrix form this becomes

$$\begin{bmatrix} 1 & \cdots & 1 \\ \lambda_1 & \cdots & \lambda_n \\ \vdots & \ddots & \vdots \\ \lambda_1^{n-1} & \cdots & \lambda_n^{n-1} \end{bmatrix} \begin{bmatrix} d_1 \\ \vdots \\ d_n \end{bmatrix} = \begin{bmatrix} x(t_0) \\ \dot{x}(t_0) \\ \vdots \\ x^{(n-1)}(t_0) \end{bmatrix}$$

In “Linear Independence” we saw that this matrix has rank n if $\lambda_1, ..., \lambda_n$ are distinct. Thus we can solve for the ds in this case.

When roots have multiplicity things get a little more complicated. We first need to solve the equation

$$(D - \lambda)^k (x) = 0.$$

One can check that the k functions $\exp(\lambda t)$, $t \exp(\lambda t)$, ..., $t^{k-1} \exp(\lambda t)$ are solutions to this equation. One can also prove that they are linearly independent using that 1, t, ..., t^{k-1} are linearly independent. This will lead us to a complete set of solutions to $L(x) = 0$ even when we have multiple roots. The problem of solving the initial value is somewhat more involved due to the problem of taking derivatives of $t^l \exp(\lambda t)$. This can be simplified a little by considering the solutions $\exp(\lambda(t - t_0))$, $(t - t_0) \exp(\lambda(t - t_0))$, ..., $(t - t_0)^{k-1} \exp(\lambda(t - t_0))$.

For the sake of illustration let us consider the simplest case of trying to solve $(D - \lambda)^2 (x) = 0$. The complete set of solutions can be parametrized as

$$x = d_1 \exp(\lambda(t - t_0)) + d_2 (t - t_0) \exp(\lambda(t - t_0))$$

Then

$$Dx = \lambda d_1 \exp(\lambda(t - t_0)) + (1 + \lambda(t - t_0)) d_2 \exp(\lambda(t - t_0))$$

Thus we have to solve

$$\begin{aligned} x(t_0) &= d_1 \\ Dx(t_0) &= \lambda d_1 + d_2. \end{aligned}$$

This leads us to the system

$$\begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \end{bmatrix} = \begin{bmatrix} x(t_0) \\ Dx(t_0) \end{bmatrix}$$

If $\lambda = 0$ we are finished. Otherwise we can multiply the first equation by λ and subtract it from the second to obtain

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \end{bmatrix} = \begin{bmatrix} x(t_0) \\ Dx(t_0) - \lambda x(t_0) \end{bmatrix}$$

Thus the solution to the initial value problem is

$$x = x(t_0) \exp(\lambda(t - t_0)) + (Dx(t_0) - \lambda x(t_0))(t - t_0) \exp(\lambda(t - t_0)).$$

A similar method of finding a characteristic polynomial and its roots can also be employed in solving linear systems of equations as well as homogeneous systems of linear differential with constant coefficients. The problem lies in deciding what the characteristic polynomial should be and what its roots mean for the system. This will be studied in subsequent sections and chapters. In the last three sections of this chapter we shall also see that systems of first order differential equations can solved using our knowledge of higher order equations.

For now let us see how one can approach systems of linear differential equations from the point of view of first trying to define the eigenvalues. We are considering the homogeneous problem

$$L(x) = \dot{x} - Ax = 0,$$

where A is an $n \times n$ matrix with real or complex numbers as entries. If the system is *decoupled*, i.e., $\dot{x}_i$ depends only on x_i then we have n first order equations that can be solved as above. In this case the entries that are not on the diagonal of A are zero. A particularly simple case occurs when $A = \lambda 1_{\mathbb{C}^n}$ for some λ. In this case the general solution is given by

$$x = x_0 \exp(\lambda(t - t_0)).$$

We now observe that for fixed x_0 this is still a solution to the general equation $\dot{x} = Ax$ provided only that $Ax_0 = \lambda x_0$. Thus we are lead to seek pairs of scalars λ and vectors x_0 such that $Ax_0 = \lambda x_0$. If we can find such pairs where $x_0 \neq 0$, then we call λ an *eigenvalue* for A and x_0 and *eigenvector* for λ. Therefore, if we can find a basis $v_1, ..., v_n$ for $\mathbb{R}^n$ or $\mathbb{C}^n$ of eigenvectors with $Av_1 = \lambda_1 v_1$, ..., $Av_n = \lambda_n v_x$, then we have that the complete solution must be

$$x = v_1 \exp(\lambda_1(t - t_0)) c_1 + \cdots + v_n \exp(\lambda_n(t - t_0)) c_n.$$

The initial value problem $L(x) = 0$, $x(t_0) = x_0$ is then handled by solving

$$v_1 c_1 + \cdots + v_n c_n = \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = x_0.$$

Since $v_1, ..., v_n$ was assumed to be a basis we know that this system can be solved. Gauss elimination can then be used to find $c_1, ..., c_n$.

What we accomplished by this change of basis was to decouple the system in a different coordinate system. One of the goals in the study of linear operators is to find a basis that makes the matrix representation of the operator as simple as possible. As we have just seen this can then be used to great effect in solving what might appear to be a rather complicated problem. Even so it might not be possible to find the desired basis of eigenvectors. This happens if we consider the second order equation $(D-\lambda)^2=0$ and convert it to a system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -\lambda^2 & 2\lambda \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

Here the general solution to $(D-\lambda)^2=0$ is of the form

$$x = x_1 = c_1 \exp(\lambda t) + c_2 t \exp(\lambda t)$$

so

$$x_2 = \dot{x}_1 = c_1 \lambda \exp(\lambda t) + c_2 (\lambda t + 1) \exp(\lambda t).$$

This means that

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = c_1 \begin{bmatrix} 1 \\ \lambda \end{bmatrix} \exp(\lambda t) + c_2 \begin{bmatrix} t \\ \lambda t + 1 \end{bmatrix} \exp(\lambda t).$$

Since we cannot write this in the form

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = c_1 v_1 \exp(\lambda_1 t) + c_2 v_2 \exp(\lambda_2 t)$$

there cannot be any reason to expect that a basis of eigenvectors can be found even for the simple matrix

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

Below we shall see that any square matrix and indeed any linear operator on a finite dimensional vector space has a characteristic polynomial whose roots are the eigenvalues of the map. Having done that we shall spend considerable time on trying to determine exactly what properties of the linear map further guarantees that it admits a basis of eigenvectors. In "Cyclic Subspaces", "The Frobenius Canonical Form" and "The Jordan Canonical Form" below we shall show that any system of equations can be transformed into a new system that looks like several uncoupled higher order equations.

There is another rather intriguing way of solving linear differential equations by reducing them to *recurrences*. We will emphasize higher order equations, it works equally well with systems. The goal is to transform the differential equation:

$$D^n x + a_{n-1} D^{n-1} x + \cdots + a_1 D x + a_0 x = p(D)(x) = 0$$

into something that can be solved using combinatorial methods.

Assume that x is given by its MacLaurin expansion

$$\begin{aligned} x(t) &= \sum_{k=0}^{\infty} \left(D^k x\right)(0) \frac{t^k}{k!} \\ &= \sum_{k=0}^{\infty} c_k \frac{t^k}{k!} \end{aligned}$$

The derivative is then given by

$$\begin{aligned} Dx &= \sum_{k=1}^{\infty} c_k \frac{t^{k-1}}{(k-1)!} \\ &= \sum_{k=0}^{\infty} c_{k+1} \frac{t^k}{k!} \end{aligned}$$

and more generally

$$D^l x = \sum_{k=0}^{\infty} c_{k+l} \frac{t^k}{k!}.$$

Thus the derivative of x is simply a shift in the index for the sequence (c_k). The differential equation gets to look like

$$\begin{aligned} & D^n x + a_{n-1} D^{n-1} x + \cdots + a_1 D x + a_0 x \\ = & \sum_{k=0}^{\infty} (c_{k+n} + a_{n-1} c_{k+n-1} + \cdots + a_1 c_{k+1} + a_0 c_k) \frac{t^k}{k!}. \end{aligned}$$

From this we can conclude that x is a solution if and only if the sequence c_k solves the *linear* n^{th} *order recurrence*

$$c_{k+n} + a_{n-1} c_{k+n-1} + \cdots + a_1 c_{k+1} + a_0 c_k = 0,$$

or

$$c_{k+n} = -(a_{n-1} c_{k+n-1} + \cdots + a_1 c_{k+1} + a_0 c_k).$$

For such a sequence it is clear that we need to know the initial values $c_0, ..., c_{n-1}$ in order to find the whole sequence. This corresponds to the initial value problem for the corresponding differential equation as $c_k = (D^k x)(0)$.

The correspondence between systems $\dot{x} = Ax$ and recurrences of vectors $c_{n+1} = Ac_n$ comes about by assuming that the solution to the differential equation looks like

$$\begin{aligned} x(t) &= \sum_{n=0}^{\infty} c_n \frac{t^n}{n!}, \\ c_n &\in \mathbb{C}^n \end{aligned}$$

2.1. Exercises.

(1) Find the solution to the differential equations with the general initial values: $x(t_0) = x_0$, $\dot{x}(t_0) = \dot{x}_0$, and $\ddot{x}(t_0) = \ddot{x}_0$.
 (a) $\dddot{x} - 3\ddot{x} + 3\dot{x} - x = 0$.
 (b) $\dddot{x} - 5\ddot{x} + 8\dot{x} - 4x = 0$.
 (c) $\dddot{x} + 6\ddot{x} + 11\dot{x} + 6x = 0$.

(2) Find the complete solution to the initial value problems.
 (a) $\begin{bmatrix} \dot{x} \\ \dot{y} \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$, where $\begin{bmatrix} x(t_0) \\ y(t_0) \end{bmatrix} = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix}$.
 (b) $\begin{bmatrix} \dot{x} \\ \dot{y} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$, where $\begin{bmatrix} x(t_0) \\ y(t_0) \end{bmatrix} = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix}$.

(3) Find the real solution to the differential equations with the general initial values: $x(t_0) = x_0$, $\dot{x}(t_0) = \dot{x}_0$, and $\ddot{x}(t_0) = \ddot{x}_0$ in the third order cases.
 (a) $\ddot{x} + x = 0$.
 (b) $\dddot{x} + \dot{x} = 0$.
 (c) $\ddot{x} - 6\dot{x} + 25x = 0$.
 (d) $\dddot{x} - 5\ddot{x} + 19\dot{x} + 25 = 0$.

(4) Consider the vector space $C^{\infty}([a,b], \mathbb{C}^n)$ of infinitely differentiable curves in $\mathbb{C}^n$ and let $z_1, ..., z_n \in C^{\infty}([a,b], \mathbb{C}^n)$.
 (a) If we can find $t_0 \in [a,b]$ so that the vectors $z_1(t_0), ..., z_n(t_0) \in \mathbb{C}^n$ are linearly independent, then the functions $z_1, ..., z_n \in C^{\infty}([a,b], \mathbb{C}^n)$ are also linearly independent.

(b) Find a linearly independent pair $z_1, z_2 \in C^\infty\left([a,b], \mathbb{C}^2\right)$ so that $z_1(t), z_2(t) \in \mathbb{C}^2$ are linearly dependent for all $t \in [a,b]$.

(c) Assume now that each $z_1, ..., z_n$ solves the linear differential equation $\dot{x} = Ax$. Show that if $z_1(t_0), ..., z_n(t_0) \in \mathbb{C}^n$ are linearly dependent for some t_0, then $z_1, ..., z_n \in C^\infty([a,b], \mathbb{C}^n)$ are linearly dependent as well.

(5) Let $p(t) = (t - \lambda_1) \cdots (t - \lambda_n)$, where we allow multiplicities among the roots.

(a) Show that $(D - \lambda)(x) = f(t)$ has

$$x = \exp(\lambda t) \int_0^t \exp(-\lambda s) f(s)\, ds$$

as a solution.

(b) Show that a solution x to $p(D)(x) = f$ can be found by successively solving

$$\begin{aligned} (D - \lambda_1)(z_1) &= f, \\ (D - \lambda_2)(z_2) &= z_1, \\ &\vdots \\ (D - \lambda_n)(z_n) &= z_{n-1}. \end{aligned}$$

(6) Show that the initial value problem

$$\begin{aligned} \dot{x} &= Ax, \\ x(t_0) &= x_0 \end{aligned}$$

can be solved "explicitly" if A is upper (or lower) triangular. This holds even in the case where the entries of A and b are functions of t.

(7) Assume that $x(t)$ is a solution to $\dot{x} = Ax$, where $A \in \mathrm{Mat}_{n \times n}(\mathbb{C})$.

(a) Show that the phase shifts $x_\omega(t) = x(t + \omega)$ are also solutions.

(b) If the vectors $x(\omega_1), ..., x(\omega_n)$ form a basis for $\mathbb{C}^n$, then all solutions to $\dot{x} = Ax$ are linear combinations of the phase shifted solutions $x_{\omega_1}, ..., x_{\omega_n}$.

(8) Assume that x is a solution to $p(D)(x) = 0$, where $p(D) = D^n + \cdots + a_1 D + a_0$.

(a) Show that the phase shifts $x_\omega(t) = x(t + \omega)$ are also solutions.

(b) If the vectors

$$\begin{bmatrix} x(\omega_1) \\ Dx(\omega_1) \\ \vdots \\ D^{n-1}x(\omega_1) \end{bmatrix}, ..., \begin{bmatrix} x(\omega_n) \\ Dx(\omega_n) \\ \vdots \\ D^{n-1}x(\omega_n) \end{bmatrix}$$

form a basis for $\mathbb{C}^n$, then all solutions to $p(D)(x) = 0$ are linear combinations of the phase shifted solutions $x_{\omega_1}, ..., x_{\omega_n}$.

(9) Let $p(t) = (t - \lambda_1) \cdots (t - \lambda_n)$. Show that the higher order equation $L(y) = p(D)(y) = 0$ can be made into a system of equations $\dot{x} - Ax = 0$,

where

$$A=\begin{bmatrix}\lambda_1 & 1 & & 0\\ 0 & \lambda_2 & \ddots & \\ & & \ddots & 1\\ 0 & & & \lambda_n\end{bmatrix}$$

by choosing

$$x=\begin{bmatrix} y\\ (D-\lambda_1)\,y\\ \vdots\\ (D-\lambda_1)\cdots(D-\lambda_{n-1})\,y\end{bmatrix}.$$

(10) Show that $p(t)\exp(\lambda t)$ solves $(D-\lambda)^k x=0$ if $p(t)\in\mathbb{C}[t]$ and $\deg(p)\leq k-1$. Conclude that $\ker\left((D-\lambda)^k\right)$ contains a k-dimensional subspace.

(11) Let $V=\operatorname{span}\{\exp(\lambda_1 t),...,\exp(\lambda_n t)\}$, where $\lambda_1,...,\lambda_n\in\mathbb{C}$ are distinct.
 (a) Show that $\exp(\lambda_1 t),...,\exp(\lambda_n t)$ form a basis for V. Hint: One way of doing this is to construct a linear isomorphism

$$\begin{aligned} L &: V\to\mathbb{C}^n\\ L(f) &= (f(t_1),...,f(t_n)) \end{aligned}$$

 by selecting suitable points $t_1,...,t_n\in\mathbb{R}$ depending on $\lambda_1,...,\lambda_n\in\mathbb{C}$ such that $L(\exp(\lambda_i t))$, $i=1,...,n$ form a basis.
 (b) Show that if $x\in V$, then $Dx\in V$.
 (c) Compute the matrix representation for the linear operator $D:V\to V$ with respect to $\exp(\lambda_1 t),...,\exp(\lambda_n t)$.
 (d) More generally, show that $p(D):V\to V$, where $p(D)=a_kD^k+\cdots+a_1D+a_0 1_V$.
 (e) Show that $p(D)=0$ if and only if $\lambda_1,...,\lambda_n$ are all roots of $p(t)$.

(12) Let $p\in\mathbb{C}[t]$ and consider $\ker(p(D))=\{x:p(D)(x)=0\}$, i.e., it is the space of solutions to $p(D)=0$.
 (a) Assuming unique solutions to initial values problems show that

$$\dim_{\mathbb{C}}\ker(p(D))=\deg p=n.$$

 (b) Show that $D:\ker(p(D))\to\ker(p(D))$.
 (c) Show that $q(D):\ker(p(D))\to\ker(p(D))$ for any polynomial $q(t)\in\mathbb{C}[t]$.
 (d) Show that $\ker(p(D))$ has a basis for the form $x,Dx,...,D^{n-1}x$. Hint: Let x be the solution to $p(D)(x)=0$ with the initial values $x(0)=Dx(0)=\cdots=D^{n-2}x(0)=0$, and $D^{n-1}x(0)=1$.

(13) Let $p\in\mathbb{R}[t]$ and consider

$$\begin{aligned} \ker_{\mathbb{R}}(p(D)) &= \{x:\mathbb{R}\to\mathbb{R}:p(D)(x)=0\},\\ \ker_{\mathbb{C}}(p(D)) &= \{z:\mathbb{R}\to\mathbb{C}:p(D)(z)=0\} \end{aligned}$$

 i.e., the real valued, respectively, complex valued solutions.
 (a) Show that $x\in\ker_{\mathbb{R}}(p(D))$ if and only if $x=\operatorname{Re}(z)$ where $z\in\ker_{\mathbb{C}}(p(D))$.
 (b) Show that $\dim_{\mathbb{C}}\ker(p(D))=\deg p=\dim_{\mathbb{R}}\ker(p(D))$.

3. Eigenvalues

We are now ready to give the abstract definitions for eigenvalues and eigenvectors. Consider a linear operator $L : V \to V$ on a vector space over $\mathbb{F}$. If we have a scalar $\lambda \in \mathbb{F}$ and a vector $x \in V - \{0\}$ so that $L(x) = \lambda x$, then we say that λ is an *eigenvalue* of L and x is an *eigenvector* for λ. If we add zero to the space of eigenvectors for λ, then it can be identified with the subspace

$$\ker(L - \lambda 1_V) = \{x \in V : L(x) - \lambda x = 0\} \subset V.$$

This is also called the *eigenspace* for λ. In many texts this space is often denoted

$$E_\lambda = \ker(L - \lambda 1_V).$$

At this point we can give a procedure for computing the eigenvalues/vectors using Gauss elimination. The more standard method using determinants can be found in virtually every other book on linear algebra. We start by considering a matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$. If we wish to find an eigenvalue λ for A, then we need to determine when there is a nontrivial solution to $(A - \lambda 1_{\mathbb{F}^n})(x) = 0$. In other words, the augmented system

$$\begin{bmatrix} \alpha_{11} - \lambda & \cdots & \alpha_{1n} & 0 \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} - \lambda & 0 \end{bmatrix}$$

should have a nontrivial solution. This is something we know how to deal with using Gauss elimination. The only complication is that if λ is simply an abstract number, then it can be a bit tricky to decide when we are allowed to divide by expression that involve λ.

Before discussing this further let us consider some examples.

Example 49. *Let*

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Row reduction tells us:

$$\begin{aligned} A - \lambda 1_{\mathbb{F}^4} &= \begin{bmatrix} -\lambda & 1 & 0 & 0 & 0 \\ -1 & -\lambda & 0 & 0 & 0 \\ 0 & 0 & -\lambda & 1 & 0 \\ 0 & 0 & 1 & -\lambda & 0 \end{bmatrix} \begin{matrix} \textit{interchange rows 1 and 2,} \\ \\ \textit{interchange rows 3 and 4,} \end{matrix} \\ &\begin{bmatrix} -1 & -\lambda & 0 & 0 & 0 \\ -\lambda & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -\lambda & 0 \\ 0 & 0 & \lambda & 1 & 0 \end{bmatrix} \begin{matrix} \textit{Use row 1 to eliminate } -\lambda \textit{ in row 2} \\ \\ \textit{Use row 3 to eliminate } \lambda \textit{ in row 4} \end{matrix} \\ &\begin{bmatrix} -1 & -\lambda & 0 & 0 & 0 \\ 0 & 1+\lambda^2 & 0 & 0 & 0 \\ 0 & 0 & 1 & -\lambda & 0 \\ 0 & 0 & 0 & 1-\lambda^2 & 0 \end{bmatrix} \end{aligned}$$

We see that this system has nontrivial solutions precisely when $1+\lambda^2 = 0$ *or* $1-\lambda^2 = 0$. *Thus the eigenvalues are* $\lambda = \pm i$ *and* $\lambda = \pm 1$. *Note that the two conditions can be multiplied into one* characteristic equation *of degree 4:* $(1+\lambda^2)(1-\lambda^2) = 0$.

Having found the eigenvalues we then need to insert them into the system and find the eigenvectors. Since the system has already been reduced this is quite simple. First let $\lambda = \pm i$ *so that we have*

$$\begin{bmatrix} 1 & \pm i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & \mp i & 0 \\ 0 & 0 & 0 & 2 & 0 \end{bmatrix}$$

Thus we get

$$\begin{bmatrix} 1 \\ i \\ 0 \\ 0 \end{bmatrix} \longleftrightarrow \lambda = i \text{ and } \begin{bmatrix} i \\ 1 \\ 0 \\ 0 \end{bmatrix} \longleftrightarrow \lambda = -i$$

Then we let $\lambda = \pm 1$ *and consider*

$$\begin{bmatrix} 1 & \pm 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & \mp 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

to get

$$\begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \leftrightarrow 1 \text{ and } \begin{bmatrix} 0 \\ 0 \\ -1 \\ 1 \end{bmatrix} \leftrightarrow -1$$

EXAMPLE 50. *Let*

$$A = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \alpha_{nn} \end{bmatrix}$$

be upper triangular, i.e., all entries below the diagonal are zero: $\alpha_{ij} = 0$ *if* $i > j$. *Then we are looking at*

$$\begin{bmatrix} \alpha_{11} - \lambda & \cdots & \alpha_{1n} & 0 \\ \vdots & \ddots & \vdots & 0 \\ 0 & \cdots & \alpha_{nn} - \lambda & 0 \end{bmatrix}.$$

Note again that we don't perform any divisions so as to make the diagonal entries 1. This is because if they are zero we evidently have a nontrivial solution and that is what we are looking for. Therefore, the eigenvalues are $\lambda = \alpha_{11}, ..., \alpha_{nn}$. *Note that the eigenvalues are precisely the roots of the polynomial that we get by multiplying the diagonal entries. This polynomial is going to be the* characteristic polynomial *of* A.

In order to help us finding roots we have a few useful facts.

PROPOSITION 12. *Let* $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ *and*

$$\chi_A(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 = (t - \lambda_1)\cdots(t - \lambda_n).$$

(1) $\operatorname{tr} A = \lambda_1 + \cdots + \lambda_n = -a_{n-1}$.
(2) $\lambda_1 \cdots \lambda_n = (-1)^n a_0$.

(3) *If* $\chi_A(t) \in \mathbb{R}[t]$ *and* $\lambda \in \mathbb{C}$ *is a root, then* $\bar{\lambda}$ *is also a root. In particular the number of real roots is even, respectively odd, if* n *is even, respectively odd.*
(4) *If* $\chi_A(t) \in \mathbb{R}[t]$, n *is even, and* $a_0 < 0$, *then there are at least two real roots, one negative and one positive.*
(5) *If* $\chi_A(t) \in \mathbb{R}[t]$ *and* n *is odd then there is at least one real root, whose sign is the opposite of* a_0.
(6) *If* $\chi_A(t) \in \mathbb{Z}[t]$, *then all rational roots are in fact integers that divide* a_0.

PROOF. The proofs of 3 and 6 are basic algebraic properties for polynomials. Property 6 was already covered in the previous section. The proofs of 4 and 5 follow from the intermediate value theorem. Simply note that $\chi_A(0) = a_0$ and that $\chi_A(t) \to \infty$ as $t \to \infty$ while $(-1)^n \chi_A(t) \to \infty$ as $t \to -\infty$.

The facts that

$$\begin{aligned} \lambda_1 + \cdots + \lambda_n &= -a_{n-1}, \\ \lambda_1 \cdots \lambda_n &= (-1)^n a_0 \end{aligned}$$

follow directly from the equation

$$t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 = (t - \lambda_1) \cdots (t - \lambda_n).$$

Finally the relation $\operatorname{tr} A = \lambda_1 + \cdots + \lambda_n$ will be established when we can prove that complex matrices are similar to upper triangular matrice. In other words we will show that one can find $B \in Gl_n(\mathbb{C})$ such that $B^{-1}AB$ is upper triangular. We then observe that A and $B^{-1}AB$ have the same eigenvalues as $Ax = \lambda x$ if and only if $B^{-1}AB\left(B^{-1}x\right) = \lambda\left(B^{-1}x\right)$. However as the eigenvalues for the upper triangular matrix $B^{-1}AB$ are precisely the diagonal entries we see that

$$\begin{aligned} \lambda_1 + \cdots + \lambda_n &= \operatorname{tr}\left(B^{-1}AB\right) \\ &= \operatorname{tr}\left(ABB^{-1}\right) \\ &= \operatorname{tr}(A). \end{aligned}$$

Another proof of $\operatorname{tr} A = -a_{n-1}$ that works for all fields is presented below in the exercises to “The Frobenius Canonical Form”.

For 6 let p/q be a rational root in reduced form, then

$$\left(\frac{p}{q}\right)^n + \cdots + a_1\left(\frac{p}{q}\right) + a_0 = 0,$$

and

$$\begin{aligned} 0 &= p^n + \cdots + a_1 p q^{n-1} + a_0 q^n \\ &= p^n + q\left(a_{n-1}p^{n-1} + \cdots + a_1 p q^{n-2} + a_0 q^{n-1}\right) \\ &= p\left(p^{n-1} + \cdots + a_1 q^{n-1}\right) + a_0 q^n. \end{aligned}$$

Thus q divides p^n and p divides $a_0 q^n$. Since p and q have no divisors in common the result follows. □

EXAMPLE 51. *Let*

$$A = \begin{bmatrix} 1 & 2 & 4 \\ -1 & 0 & 2 \\ 3 & -1 & 5 \end{bmatrix},$$

and perform row operations on

$$\begin{bmatrix} 1-\lambda & 2 & 4 & 0 \\ -1 & -\lambda & 2 & 0 \\ 3 & -1 & 5-\lambda & 0 \end{bmatrix} \quad \begin{array}{l} \textit{Change sign in row 2} \\ \textit{Interchange rows 1 and 2} \end{array}$$

$$\begin{bmatrix} 1 & \lambda & -2 & 0 \\ 1-\lambda & 2 & 4 & 0 \\ 3 & -1 & 5-\lambda & 0 \end{bmatrix} \quad \textit{Use row 1 to cancel } 1-\lambda \textit{ in row 2}$$

$$\begin{bmatrix} 1 & \lambda & -2 & 0 \\ 0 & 2-\lambda+\lambda^2 & 6-2\lambda & 0 \\ 0 & -1-3\lambda & 11-\lambda & 0 \end{bmatrix} \quad \textit{Interchange rows 2 and 3}$$

$$\begin{bmatrix} 1 & \lambda & -2 & 0 \\ 0 & -1-3\lambda & 11-\lambda & 0 \\ 0 & 2-\lambda+\lambda^2 & 6-2\lambda & 0 \end{bmatrix} \quad \begin{array}{l} \textit{Change sign in row 2,} \\ \textit{use row 2 to cancel } 2-\lambda+\lambda^2 \textit{ in row 3} \\ \textit{this requires that we have } 1+3\lambda \neq 0! \end{array}$$

$$\begin{bmatrix} 1 & \lambda & -2 & 0 \\ 0 & 1+3\lambda & -11+\lambda & 0 \\ 0 & 0 & 6-2\lambda-\frac{2-\lambda+\lambda^2}{1+3\lambda}(-11+\lambda) & 0 \end{bmatrix} \quad \textit{Common denominator for row 3}$$

$$\begin{bmatrix} 1 & \lambda & -2 & 0 \\ 0 & 1+3\lambda & -11+\lambda & 0 \\ 0 & 0 & \frac{-28-3\lambda-6\lambda^2+\lambda^3}{1+3\lambda} & 0 \end{bmatrix}$$

Note that we are not allowed to have $1+3\lambda=0$ *in this formula. If* $1+3\lambda=0$, *then we note that* $2-\lambda+\lambda^2 \neq 0$ *and* $11-\lambda \neq 0$ *so that the third display*

$$\begin{bmatrix} 1 & \lambda & -2 & 0 \\ 0 & 2-\lambda+\lambda^2 & 6-2\lambda & 0 \\ 0 & -1-3\lambda & 11-\lambda & 0 \end{bmatrix}$$

guarantees that there are no nontrivial solutions in that case. This means that our analysis is valid and that multiplying the diagonal entries will get us the characteristic polynomial $-28-3\lambda-6\lambda^2+\lambda^3$. *We note first that* 7 *is a root of this polynomial. We can then find the other two roots by dividing*

$$\frac{-28-3\lambda-6\lambda^2+\lambda^3}{\lambda-7} = \lambda^2+\lambda+4$$

and using the quadratic formula: $-\frac{1}{2}+\frac{1}{2}i\sqrt{15}, -\frac{1}{2}-\frac{1}{2}i\sqrt{15}$.

The *characteristic polynomial* of a matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ is a polynomial $\chi_A(\lambda) \in \mathbb{F}[\lambda]$ of degree n such that all eigenvalues of A are roots of χ_A. In addition we scale the polynomial so that the leading term is λ^n, i.e., the polynomial is monic. To get a better understanding of the process that leads us to the characteristic polynomial we study the 2×2 and 3×3 cases as well as a few specialized $n\times n$ situations.

Starting with $A \in \mathrm{Mat}_{2\times 2}(\mathbb{F})$ we investigate

$$A - \lambda 1_{\mathbb{F}^2} = \begin{bmatrix} \alpha_{11}-\lambda & \alpha_{12} \\ \alpha_{21} & \alpha_{22}-\lambda \end{bmatrix}.$$

If $\alpha_{21} = 0$, the matrix is in uppertriangular form and the characteristic polynomial is

$$\begin{aligned} \chi_A &= (\alpha_{11} - \lambda)(\alpha_{22} - \lambda) \\ &= \lambda^2 - (\alpha_{11} + \alpha_{22})\lambda + \alpha_{11}\alpha_{22}. \end{aligned}$$

If $\alpha_{21} \neq 0$, then we switch the first and second row and then eliminate the bottom entry in the first column:

$$\begin{bmatrix} \alpha_{11} - \lambda & \alpha_{12} \\ \alpha_{21} & \alpha_{22} - \lambda \end{bmatrix}$$
$$\begin{bmatrix} \alpha_{21} & \alpha_{22} - \lambda \\ \alpha_{11} - \lambda & \alpha_{12} \end{bmatrix}$$
$$\begin{bmatrix} \alpha_{21} & \alpha_{22} - \lambda \\ 0 & \alpha_{12} - \frac{1}{\alpha_{21}}(\alpha_{11} - \lambda)(\alpha_{22} - \lambda) \end{bmatrix}$$

Multiplying the diagonal entries gives

$$\begin{aligned} & \alpha_{21}\alpha_{12} - (\alpha_{11} - \lambda)(\alpha_{22} - \lambda) \\ = & -\lambda^2 + (\alpha_{11} + \alpha_{22})\lambda - \alpha_{11}\alpha_{22} + \alpha_{21}\alpha_{12}. \end{aligned}$$

In both cases the characteristic polynomial is given by

$$\begin{aligned} \chi_A &= \lambda^2 - (\alpha_{11} + \alpha_{22})\lambda + (\alpha_{11}\alpha_{22} - \alpha_{21}\alpha_{12}) \\ &= \lambda^2 - \operatorname{tr}(A)\lambda + \det(A). \end{aligned}$$

We now make an attempt at the case where $A \in \mathrm{Mat}_{3\times 3}(\mathbb{F})$. Thus we consider

$$A - \lambda 1_{\mathbb{F}^3} = \begin{bmatrix} \alpha_{11} - \lambda & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} - \lambda & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} - \lambda \end{bmatrix}$$

When $\alpha_{21} = \alpha_{31} = 0$ there is nothing to do in the first column and we are left with the bottom right 2×2 matrix to consider. This is done as above.

If $\alpha_{21} = 0$ and $\alpha_{31} \neq 0$, then we switch the first and third rows and eliminate the last entry in the first row. This will look like

$$\begin{bmatrix} \alpha_{11} - \lambda & \alpha_{12} & \alpha_{13} \\ 0 & \alpha_{22} - \lambda & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} - \lambda \end{bmatrix}$$
$$\begin{bmatrix} \alpha_{31} & \alpha_{32} & \alpha_{33} - \lambda \\ 0 & \alpha_{22} - \lambda & \alpha_{23} \\ \alpha_{11} - \lambda & \alpha_{12} & \alpha_{13} \end{bmatrix}$$
$$\begin{bmatrix} \alpha_{31} & \alpha_{32} & \alpha_{33} - \lambda \\ 0 & \alpha_{22} - \lambda & \alpha_{23} \\ 0 & \alpha\lambda + \beta & p(\lambda) \end{bmatrix}$$

where p has degree 2. If $\alpha\lambda + \beta$ is proportional to $\alpha_{22} - \lambda$, then we can eliminate it to get an upper triangular matrix. Otherwise we can still eliminate $\alpha\lambda$ by multiplying the second row by α and adding it to the third row. This leads us to a matrix of the form

$$\begin{bmatrix} \alpha_{31} & \alpha_{32} & \alpha_{33} - \lambda \\ 0 & \alpha_{22} - \lambda & \alpha_{23} \\ 0 & \beta' & p'(\lambda) \end{bmatrix}$$

where β' is a scalar and p' a polynomial of degree 2. If $\beta' = 0$ we are finished. Otherwise we switch the second and third rows and elimate.

If $\alpha_{21} \neq 0$, then we switch the first two rows and cancel below the diagonal in the first column. This gives us something like

$$\begin{bmatrix} \alpha_{11}-\lambda & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22}-\lambda & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33}-\lambda \end{bmatrix}$$
$$\begin{bmatrix} \alpha_{21} & \alpha_{22}-\lambda & \alpha_{23} \\ \alpha_{11}-\lambda & \alpha_{12} & \alpha_{13} \\ \alpha_{31} & \alpha_{32} & \alpha_{33}-\lambda \end{bmatrix}$$
$$\begin{bmatrix} \alpha_{21} & \alpha_{22}-\lambda & \alpha_{23} \\ 0 & p(\lambda) & \alpha'_{13} \\ 0 & q'(\lambda) & q(\lambda) \end{bmatrix}$$

where p has degree 2 and q, q' have degree 1. If $q' = 0$, we are finished. Otherwise, we switch the last two rows. If q' divides p we can eliminate p to get an upper triangular matrix. If q' does not divide p, then we can still eliminate the degree 2 term in p to reduce it to a polynomial of degree 1. This lands us in a situation similar to what we ended up with when $\alpha_{21} = 0$. So we can finish using the same procedure.

Note that we avoided making any illegal moves in the above procedure. It is possible to formalize this proceedure for $n \times n$ matrices, but it still doesn't lead us to a complete understanding of the characteristic polynomial. The idea is simply to treat λ as a variable and the entries as polynomials. To eleiminate entries we then use polynomial devision to reduce the degrees of entries until they can be eliminated. Since we wish to treat λ as a variable we shall rename it t when doing the Gauss elinimation and only use λ for the eigenvalues and roots of the characteristic polynomial.

The *characteristic polynomial* of a matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ is the polynomial $\chi_A(t) \in \mathbb{F}[t]$ we get by applying Gauss elimination to $A - t1_{\mathbb{F}^n}$ until it is in upper triangular form, then multiplying the diagonal entries and if necessary making the highest degree term t^n. Below in "The Frobenius Canonical Form" we shall give an alternate and completely rigorous definition of the characteristic polynomial. This will show that it really is well defined and has degree n, it will also be obvious that we above procedure really leads us to the rigorously defined characteristic polynomial.

Let us try to carry out this slightly more careful procedure on an example.

Example 52. *Let*

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 4 \\ 2 & 1 & -1 \end{bmatrix}$$

Then the calculations go as follows

$$
\begin{aligned}
A - t1_{\mathbb{F}^3} &= \begin{bmatrix} 1-t & 2 & 3 \\ 0 & 2-t & 4 \\ 2 & 1 & -1-t \end{bmatrix} \\
& \begin{bmatrix} 2 & 1 & -1-t \\ 0 & 2-t & 4 \\ 1-t & 2 & 3 \end{bmatrix} \\
& \begin{bmatrix} 2 & 1 & -1-t \\ 0 & 2-t & 4 \\ 0 & 2-\frac{1-t}{2} & 3+\frac{(1-t)(1+t)}{2} \end{bmatrix} \\
& \begin{bmatrix} 2 & 1 & -1-t \\ 0 & 2-t & 4 \\ 0 & \frac{3}{2}+\frac{t}{2} & 3+\frac{(1-t)(1+t)}{2} \end{bmatrix} \\
& \begin{bmatrix} 2 & 1 & -1-t \\ 0 & 2-t & 4 \\ 0 & \frac{3}{2}+1 & 5+\frac{(1-t)(1+t)}{2} \end{bmatrix} \\
& \begin{bmatrix} 2 & 1 & -1-t \\ 0 & \frac{5}{2} & 5+\frac{(1-t)(1+t)}{2} \\ 0 & 2-t & 4 \end{bmatrix} \\
& \begin{bmatrix} 2 & 1 & -1-\lambda \\ 0 & \frac{5}{2} & 5+\frac{(1-\lambda)(1+\lambda)}{2} \\ 0 & 0 & 4-2\frac{2-\lambda}{5}\left(5+\frac{(1-\lambda)(1+\lambda)}{2}\right) \end{bmatrix}
\end{aligned}
$$

Multiplying the diagonal entries gives us

$$
\begin{aligned}
& 5\left(4-2\frac{2-t}{5}\left(5+\frac{(1-t)(1+t)}{2}\right)\right) \\
= & -t^3+2t^2+11t-2
\end{aligned}
$$

and the characteristic polynomial is

$$
\chi_A(t) = t^3 - 2t^2 - 11t + 2
$$

When the matrix A can be written in block triangular form it becomes somewhat easier to calculate the characteristic polynomial.

LEMMA 13. *Assume that* $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ *has the form*

$$
A = \begin{bmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{bmatrix},
$$

where $A_{11} \in \mathrm{Mat}_{k\times k}(\mathbb{F})$, $A_{22} \in \mathrm{Mat}_{(n-k)\times(n-k)}(\mathbb{F})$, *and* $A_{12} \in \mathrm{Mat}_{k\times(n-k)}(\mathbb{F})$, *then*

$$
\chi_A(t) = \chi_{A_{11}}(t)\,\chi_{A_{22}}(t).
$$

PROOF. To compute $\chi_A(t)$ we do row operations on

$$
t1_{\mathbb{F}^n} - A = \begin{bmatrix} t1_{\mathbb{F}^k} - A_{11} & A_{12} \\ 0 & t1_{\mathbb{F}^{n-k}} - A_{22} \end{bmatrix}.
$$

This can be done by first doing row operations on the first k rows leading to a situation that looks like

$$\begin{bmatrix} q_1(t) & & * & & \\ & \ddots & & & * \\ 0 & & q_k(t) & & \\ & 0 & & & t1_{\mathbb{F}^{n-k}} - A_{22} \end{bmatrix}$$

Having accomplished this we then do row operations on the last $n-k$ rows. to get

$$\begin{bmatrix} p_1(t) & & * & & & \\ & \ddots & & & * & \\ 0 & & p_k(t) & & & \\ & & & r_1(t) & & * \\ & 0 & & & \ddots & \\ & & & 0 & & r_{n-k}(t) \end{bmatrix}$$

As these two sets of operations do not depend on each other we see that

$$\begin{aligned} \chi_A(t) &= q_1(t)\cdots q_k(t)\, r_1(t)\cdots r_{n-k}(t) \\ &= \chi_{A_{11}}(t)\,\chi_{A_{22}}(t). \end{aligned}$$

□

Finally we need to figure out how this matrix procedure generates eigenvalues for general linear maps $L : V \to V$. In case V is finite dimensional we can simply pick a basis and then study the matrix representation $[L]$. The diagram

$$\begin{array}{ccc} V & \xrightarrow{L} & V \\ \uparrow & & \uparrow \\ \mathbb{F}^n & \xrightarrow{[L]} & \mathbb{F}^n \end{array}$$

then quickly convinces us that eigenvectors in $\mathbb{F}^n$ for $[L]$ are mapped to eigenvectors in V for L without changing the eigenvalue, i.e.,

$$[L]\,\xi = \lambda\xi$$

implies

$$Lx = \lambda x$$

and vice versa if $\xi \in \mathbb{F}^n$ is the coordinate vector for $x \in V$. Thus we define the characteristic polynomial of L as $\chi_L(t) = \chi_{[L]}(t)$. While we don't have a problem with finding eigenvalues for L by finding them for $[L]$ it is less clear that $\chi_L(t)$ is well-defined with this definition. To see that it is well-defined we would have to show that $\chi_{[L]}(t) = \chi_{B^{-1}[L]B}(t)$ where B the the matrix transforming one basis into the other. For now we are going to take this on faith. The proof will be given when we introduce a cleaner definition of $\chi_L(t)$ in "The Frobenius canonical form". Note, however, that computing $\chi_{[L]}(t)$ does give us a rigorous method for finding the eigenvalues as L. In particular, all of the matrix representations for L must have the same eigenvalues. Thus there is nothing wrong with searching for eigenvalues using a fixed matrix representation.

In the case where $\mathbb{F} = \mathbb{Q}$ or $\mathbb{R}$ we can still think of $[L]$ as a complex matrix. As such we might get complex eigenvalues that do not lie in the field $\mathbb{F}$. These roots of χ_L cannot be eigenvalues for L as we are not allowed to multiply elements in V by complex numbers.

We now need to prove that our method for computing the characteristic polynomial of a matrix gives us the expected answer for the differential equation defined using the operator

$$L = D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0.$$

The corresponding system is

$$\begin{aligned} L(x) &= \dot{x} - Ax \\ &= \dot{x} - \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-1} \end{bmatrix} x \\ &= 0 \end{aligned}$$

So we consider the matrix

$$A = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-1} \end{bmatrix}$$

and with it

$$A - t1_{\mathbb{F}^n} = \begin{bmatrix} -t & 1 & \cdots & 0 \\ 0 & -t & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ -a_0 & -a_1 & \cdots & -t - a_{n-1} \end{bmatrix}$$

We immediately run into a problem as we don't know if some or all of a_0, ..., a_{n-1} are zero. Thus we proceed without interchanging rows.

$$\begin{bmatrix} -t & 1 & \cdots & 0 \\ 0 & -t & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ -a_0 & -a_1 & \cdots & -t - a_{n-1} \end{bmatrix}$$

$$\begin{bmatrix} -t & 1 & \cdots & 0 \\ 0 & -t & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ 0 & -a_1 - \frac{a_0}{t} & \cdots & -a_{n-1} - t \end{bmatrix}$$

$$\begin{bmatrix} -t & 1 & & \cdots & 0 \\ 0 & -t & 1 & \ddots & \vdots \\ \vdots & \vdots & & \ddots & 1 \\ 0 & 0 & -a_2 - \frac{a_1}{t} - \frac{a_0}{t^2} & \cdots & a_{n-1} - t \end{bmatrix}$$

$$\vdots$$

$$\begin{bmatrix} -t & 1 & & \cdots & 0 \\ 0 & -t & 1 & \ddots & \vdots \\ \vdots & \vdots & & \ddots & 1 \\ 0 & 0 & 0 & \cdots & -t - a_{n-1} - \frac{a_{n-2}}{t} - \cdots - \frac{a_1}{t^{n-2}} - \frac{a_0}{t^{n-1}} \end{bmatrix}$$

We see that $t = 0$ is the only value that might give us trouble. In case $t = 0$ we note that there cannot be a nontrivial kernel unless $a_0 = 0$. Thus $\lambda = 0$ is an eigenvalue if and only if $a_0 = 0$. Fortunately this gets build into our characteristic polynomial. After multiplying the diagonal entries together we have

$$\begin{aligned} p(t) &= (-1)^n (t)^{n-1} \left(t + a_{n-1} + \frac{a_{n-2}}{t} + \cdots + \frac{a_1}{t^{n-2}} + \frac{a_0}{t^{n-1}} \right) \\ &= (-1)^n \left(t^n + a_{n-1} t^{n-1} + a_{n-2} t^{n-2} + \cdots + at + a_0 \right) \end{aligned}$$

where $\lambda = 0$ is a root precisely when $a_0 = 0$ as hoped for. Finally we see that $p(t) = 0$ is up to sign our old characteristic equation for $p(D) = 0$.

3.1. Exercises.

(1) Find the characteristic polynomial and if possible the eigenvalues and eigenvectors for each of the following matrices.

(a) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$

(b) $\begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 3 \\ 2 & 3 & 0 \end{bmatrix}$

(c) $\begin{bmatrix} 0 & 1 & 2 \\ -1 & 0 & 3 \\ -2 & -3 & 0 \end{bmatrix}$

(2) Find the characteristic polynomial and if possible eigenvalues and eigenvectors for each of the following matrices.
 (a) $\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$
 (b) $\begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$
 (c) $\begin{bmatrix} 1 & i & 0 \\ i & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix}$
(3) Find the eigenvalues for the following matrices with a minimum of calculations (try not to compute the characteristic polynomial).
 (a) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$
 (b) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$
 (c) $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$
(4) Find the characteristic polynomial, eigenvalues and eigenvectors for each of the following linear operators $L : P_3 \to P_3$.
 (a) $L = D$.
 (b) $L = tD = T \circ D$.
 (c) $L = D^2 + 2D + 1$.
 (d) $L = t^2 D^3 + D$.
(5) Let $p \in \mathbb{C}[t]$ be a monic polynomial. Show that the characteristic polynomial for $D : \ker(p(D)) \to \ker(p(D))$ is $p(t)$.
(6) Assume that $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ is upper or lower triangular and let $p \in \mathbb{F}[t]$. Show that μ is an eigenvalue for $p(A)$ if and only if $\mu = p(\lambda)$ where λ is an eigenvalue for A.
(7) Let $L : V \to V$ be a linear operator on a complex vector space. Assume that we have a polynomial $p \in \mathbb{C}[t]$ such that $p(L) = 0$. Show that all eigenvalues of L are roots of p.
(8) Let $L : V \to V$ be a linear operator and $K : W \to V$ an isomorphism. Show that L and $K^{-1} \circ L \circ K$ have the same eigenvalues.
(9) Let $K : V \to W$ and $L : W \to V$ be two linear maps.
 (a) Show that $K \circ L$ and $L \circ K$ have the same nonzero eigenvalues. Hint: If $x \in V$ is an eigenvector for $L \circ K$, then $K(v) \in W$ is an eigenvector for $K \circ L$.
 (b) Give an example where 0 is an eigenvalue for $L \circ K$ but not for $K \circ L$. Hint: Try to have different dimensions for V and W.
 (c) If $\dim V = \dim W$, then a. also holds for the zero eigenvalue. Hint: Use that

$$\begin{aligned} \dim(\ker(K \circ L)) &\geq \max\{\dim(\ker(L)), \dim(\ker(K))\}, \\ \dim(\ker(L \circ K)) &\geq \max\{\dim(\ker(L)), \dim(\ker(K))\} \end{aligned}$$

and conclude that if the right hand side is zero then all the linear maps are isomorphisms.

(10) Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$.
   (a) Show that A and A^t have the same eigenvalues and that for each eigenvalue λ we have
$$\dim\left(\ker\left(A-\lambda 1_{\mathbb{F}^n}\right)\right)=\dim\left(\ker\left(A^t-\lambda 1_{\mathbb{F}^n}\right)\right).$$
   (b) Show by example that A and A^t need not have the same eigenvectors.

(11) Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$. Consider the following two linear operators on $\mathrm{Mat}_{n\times n}(\mathbb{F}) : L_A(X) = AX$ and $R_A(X) = XA$.
   (a) Show that λ is an eigenvalue for A if and only if λ is an eigenvalue for L_A.
   (b) Show that $\chi_{L_A}(t) = (\chi_A(t))^n$.
   (c) Show that λ is an eigenvalue for A^t if and only if λ is an eigenvalue for R_A.
   (d) Relate $\chi_{A^t}(t)$ and $\chi_{R_A}(t)$.

(12) Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ and $B \in \mathrm{Mat}_{m\times m}(\mathbb{F})$ and consider
$$\begin{aligned} L &: \mathrm{Mat}_{n\times m}(\mathbb{F}) \to \mathrm{Mat}_{n\times m}(\mathbb{F}), \\ L(X) &= AX - XB. \end{aligned}$$
   (a) Show that if A and B have a common eigenvalue then, L has nontrivial kernel. Hint: Use that B and B^t have the same eigenvalues.
   (b) Show more generally that if λ is an eigenvalue of A and μ and eigenvalue for B, then $\lambda - \mu$ is an eigenvalue for L.

(13) Find the characteristic polynomial, eigenvalues and eigenvectors for
$$A=\begin{bmatrix}\alpha & -\beta\\ \beta & \alpha\end{bmatrix},\alpha,\beta\in\mathbb{R}$$
as a map $A : \mathbb{C}^2 \to \mathbb{C}^2$.

(14) Show directly, using the methods developed in this section, that the characteristic polynomial for a 3×3 matrix has degree 3.

(15) Let
$$A=\begin{bmatrix}a & b\\ c & d\end{bmatrix},a,b,c,d\in\mathbb{R}$$
Show that the roots are either both real or are conjugates of each other.

(16) Show that the eigenvalues of $\begin{bmatrix}a & b\\ \bar{b} & d\end{bmatrix}$, where $a, d \in \mathbb{R}$ and $b \in \mathbb{C}$, are real.

(17) Show that the eigenvalues of $\begin{bmatrix}ia & -b\\ \bar{b} & id\end{bmatrix}$, where $a, d \in \mathbb{R}$ and $b \in \mathbb{C}$, are purely imaginary.

(18) Show that the eigenvalues of $\begin{bmatrix}a & -\bar{b}\\ b & \bar{a}\end{bmatrix}$, where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$, are complex numbers of unit length.

(19) Let

$$A=\begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-1} \end{bmatrix}.$$

(a) Show that all eigenspaces are 1 dimensional.
(b) Show that $\ker(A) \neq \{0\}$ if and only if $a_0 = 0$.

(20) Let

$$\begin{aligned} p(t) &= (t-\lambda_1)\cdots(t-\lambda_n) \\ &= t^n + \alpha_{n-1}t^{n-1} + \cdots + \alpha_1 t + \alpha_0, \end{aligned}$$

where $\lambda_1, ..., \lambda_n \in \mathbb{F}$. Show that there is a change of basis such that

$$\begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ -\alpha_0 & -\alpha_1 & \cdots & -\alpha_{n-1} \end{bmatrix} = B \begin{bmatrix} \lambda_1 & 1 & & 0 \\ 0 & \lambda_2 & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_n \end{bmatrix} B^{-1}.$$

Hint: Try $n = 2, 3$, assume that B is lower triangular with 1s on the diagonal, and look at the exercises to "Linear Differential Equations".

(21) Show that
(a) The multiplication operator $T : C^\infty(\mathbb{R},\mathbb{R}) \to C^\infty(\mathbb{R},\mathbb{R})$ does not have any eigenvalues. Recall that $T(f)(t) = t \cdot f(t)$.
(b) Show that the differential operator $D : \mathbb{C}[t] \to \mathbb{C}[t]$ only has 0 as an eigenvalue.
(c) Show that $D : C^\infty(\mathbb{R},\mathbb{R}) \to C^\infty(\mathbb{R},\mathbb{R})$ has all real numbers as eigenvalues.
(d) Show that $D : C^\infty(\mathbb{R},\mathbb{C}) \to C^\infty(\mathbb{R},\mathbb{C})$ has all complex numbers as eigenvalues.

4. The Minimal Polynomial

The minimal polynomial of a linear operator is, unlike the characteristic polynomial, fairly easy to define rigorously. It is, however, not quite as easy to calculate. The amazing properties contained in the minimal polynomial on the other hand seem to make it sufficiently desirable that it would be a shame to ignore it.

Recall that projections are characterized by a very simple polynomial relationship $L^2 - L = 0$. The purpose of this section is to find a polynomial $p(t)$ for a linear operator $L : V \to V$ such that $p(L) = 0$. This polynomial will, like the characteristic polynomial, also tell us the eigenvalues of L. In subsequent sections we shall then study the properties of L from what we know about such p. Before passing on to the abstract constructions let us consider two examples.

EXAMPLE 53. *An* involution *is a linear operator $L : V \to V$ such that $L^2 = 1_V$. This means that $p(L) = 0$ if $p(t) = t^2 - 1$. Our first observation is that this relationship implies that L is invertible and that $L^{-1} = L$. Next we note that any eigenvalue must satisfy $\lambda^2 = 1$ and hence be a root of p. We can actually glean* *even more information out of this polynomial relationship. We claim that L is diagonalizable, in fact*

$$V = \ker(L - 1_V) \oplus \ker(L + 1_V).$$

First we observe that these spaces have trivial intersection as they are eigenspaces for different eigenvalues. If $x \in \ker(L - 1_V) \cap \ker(L + 1_V)$, then

$$-x = L(x) = x$$

so $x = 0$. To show that

$$V = \ker(L - 1_V) + \ker(L + 1_V)$$

we observe that any $x \in V$ can be written as

$$x = \frac{1}{2}(x - L(x)) + \frac{1}{2}(x + L(x)).$$

Next we see that

$$\begin{aligned} L(x \pm L(x)) &= L(x) \pm L^2(x) \\ &= L(x) \pm x \\ &= \mp (x \pm L(x)). \end{aligned}$$

Thus $x + L(x) \in \ker(L - 1_V)$ and $x - L(x) \in \ker(L + 1_V)$. This proves the desired claim.

Example 54. *Consider a linear operator $L : V \to V$ such that $(L - 1_V)^2 = 0$. This relationship implies that 1 is the only possible eigenvalue. Therefore, if L is diagonalizable, then $L = 1_V$ and hence also satisfies the simpler relationship $L - 1_V = 0$. Thus L is not diagonalizable unless it is the identity map. By multiplying out the polynomial relationship we obtain*

$$L^2 - 2L + 1_V = 0.$$

This implies that

$$(2 \cdot 1_V - L) L = 1_V.$$

Hence L is invertible with $L^{-1} = 2 \cdot 1_V - L$.

These two examples, together with our knowledge of projections, tell us that one can get a tremendous amount of information from knowing that an operator satisfies a polynomial relationship. To commence our more abstract developments we start with a very simple observation.

Proposition 13. *Let $L : V \to V$ be a linear operator and*

$$p(t) = t^k + \alpha_{n-1} t^{k-1} + \cdots + \alpha_1 t + \alpha_0 \in \mathbb{F}[t]$$

a polynomial such that

$$p(L) = L^k + \alpha_{n-1} L^{k-1} + \cdots + \alpha_1 L + \alpha_0 1_V = 0.$$

(1) *All eigenvalues for L are roots of $p(t)$.*
(2) *If $p(0) = \alpha_0 \neq 0$, then L is invertible and*

$$L^{-1} = \frac{-1}{\alpha_0}\left(L^{k-1} + \alpha_{n-1} L^{k-2} + \cdots + \alpha_1 1_V\right).$$

To begin with it would be nice to find a polynomial $p(t) \in \mathbb{F}[t]$ such that both of the above properties become bi-implications. In other words $\lambda \in \mathbb{F}$ is an eigenvalues for L if and only $p(\lambda) = 0$, and L is invertible if and only if $p(0) \neq 0$. It turns out that the characteristic polynomial does have this property, but there is a polynomial that has even more information as well as being much easier to define.

One defect of the characteristic polynomial can be seen by considering the two matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

They clearly have the same characteristic polynomial $p(t) = (t-1)^2$, but only the first matrix is diagonalizable.

We define the *minimal polynomial* $\mu_L(t)$ for L in the following way. Consider 1_V, L, L^2, ..., $L^k, .. \in \hom(V, V)$. Since V and hence $\hom(V, V)$ are finite dimensional we can find a smallest $k \geq 1$ such that L^k is a linear combination of 1_V, L, L^2, ..., L^{k-1}:

$$\begin{aligned} L^k &= -\left(\alpha_0 1_V + \alpha_1 L + \alpha_2 L^2 + \cdots + \alpha_{k-1} L^{k-1}\right), \text{ or} \\ 0 &= L^k + \alpha_{k-1} L^{k-1} + \cdots + \alpha_1 L + \alpha_0 1_V. \end{aligned}$$

The minimal polynomial of L is defined as

$$\mu_L(t) = t^k + \alpha_{k-1} t^{k-1} + \cdots + \alpha_1 t + \alpha_0.$$

The first interesting thing to note is that the minimal polynomial for $L = 1_V$ is given by $\mu_{1_V}(t) = t - 1$. Hence it is not the characteristic polynomial. The name "minimal" is justified by the next proposition.

Proposition 14. *Let $L : V \to V$ be a linear operator on a finite dimensional space.*

(1) *If $p(t) \in \mathbb{F}[t]$ satisfies $p(L) = 0$, then $\deg(p) \geq \deg(\mu_L)$.*
(2) *If $p(t) \in \mathbb{F}[t]$ satisfies $p(L) = 0$ and $\deg(p) = \deg(\mu_L)$, then $p(t) = \alpha \cdot \mu_L(t)$ for some $\alpha \in \mathbb{F}$.*

Proof. 1. Assume that $p \neq 0$ and $p(L) = 0$, then

$$\begin{aligned} p(L) &= \alpha_m L^m + \alpha_{m-1} L^{m-1} + \cdots + \alpha_1 L + \alpha_0 1_V \\ &= 0 \end{aligned}$$

If $\alpha_m \neq 0$, then L^m is a linear combination of lower order terms and hence $m \geq \deg(\mu_L)$.

2. In case $m = \deg(\mu_L) = k$ we have that 1_V, L, ..., L^{k-1} are linearly independent. Thus there is only one way in which to make L^k into a linear combination of 1_V, L, ..., L^{k-1}. This implies the claim. □

Before discussing further properties of the minimal polynomial let us try to compute it for some simple matrices.

EXAMPLE 55. *Let*

$$A = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$$
$$B = \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}$$
$$C = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & i \end{bmatrix}$$

We note that A is not proportional to 1_V, while

$$\begin{aligned} A^2 &= \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}^2 \\ &= \begin{bmatrix} \lambda^2 & 2\lambda \\ 0 & \lambda^2 \end{bmatrix} \\ &= 2\lambda \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} - \lambda^2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

Thus

$$\mu_A(t) = t^2 - 2\lambda t + \lambda^2 = (t-\lambda)^2$$

The calculation for B is similar and evidently yields the same minimal polynomial

$$\mu_B(t) = t^2 - 2\lambda t + \lambda^2 = (t-\lambda)^2.$$

Finally for C we note that

$$C^2 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

Thus

$$\mu_C(t) = t^2 + 1.$$

The next proposition shows that the minimal polynomial contains much of the information that we usually glean from the characteristic polynomial. In subsequent sections we shall delve much deeper into the properties of the minimal polynomial and what it tells us about possible matrix representations of L.

PROPOSITION 15. *Let $L : V \to V$ be a linear operator on an n-dimensional space. Then*

(1) *If $p(L) = 0$ for some $p \in \mathbb{F}[t]$, then m_L divides p, i.e., $p(t) = \mu_L(t)\,q(t)$ for some $q(t) \in \mathbb{F}[t]$.*
(2) *Let $\lambda \in \mathbb{F}$, then λ is an eigenvalue for L if and only if $\mu_L(\lambda) = 0$.*
(3) *L is invertible if and only if $\mu_L(0) \neq 0$.*

PROOF. 1. Assume that $p(L) = 0$. We know that $\deg(p) \geq \deg(\mu_L)$ so if we perform polynomial division (The Euclidean Algorithm), then $p(t) = q(t)\,\mu_L(t) + r(t)$, where $\deg(r) < \deg(\mu_L)$. Sustituting L for t gives $p(L) = q(L)\,\mu_L(L) + r(L)$. Since both $p(L) = 0$ and $\mu_L(L) = 0$ we also have $r(L) = 0$. This will give us a contradiction with the definition of the minimal polynomial unless $r = 0$. Thus μ_L divides p.

2. We already know that eigenvalues are roots. Conversely, if $\mu_L(\lambda) = 0$, then we can write $\mu_L(t) = (t - \lambda) p(t)$. Thus

$$0 = \mu_L(L) = (L - \lambda 1_V) p(L)$$

Since $\deg(p) < \deg(\mu_L)$ we know that $p(L) \neq 0$, but then the relationship $(L - \lambda 1_V) p(L) = 0$ shows that $L - \lambda 1_V$ is not invertible.

3. If $\mu_L(0) \neq 0$, then we already know that L is invertible. Conversely suppose that $\mu_L(0) = 0$. Then 0 is an eigenvalue by 2. and hence L cannot be invertible. □

EXAMPLE 56. *The derivative map $D : P_n \to P_n$ has $\mu_D = t^{n+1}$. Certainly D^{n+1} vanishes on P_n as all the polynomials in P_n have degree $\leq n$. This means that $\mu_D(t) = t^k$ for some $k \leq n+1$. On the other hand $D^n(t^n) = n! \neq 0$ forcing $k = n+1$.*

EXAMPLE 57. *Let $V = \operatorname{span}\{\exp(\lambda_1 t), ..., \exp(\lambda_n t)\}$, with $\lambda_1, ..., \lambda_n$ being distinct, and consider again the derivative map $D : V \to V$. Then we have $D(\exp(\lambda_i t)) = \lambda_i \exp(\lambda_i t)$. In "Linear Independence" and "Row Reduction"in Chapter 1 it was shown that $\exp(\lambda_1 t)$, ..., $\exp(\lambda_n t)$ form a basis for V. Now observe that*

$$(D - \lambda_1 1_V) \cdots (D - \lambda_n 1_V)(\exp(\lambda_n) t) = 0.$$

By rearranging terms it follows that

$$(D - \lambda_1 1_V) \cdots (D - \lambda_n 1_V) = 0 \text{ on } V.$$

On the other hand

$$(D - \lambda_1 1_V) \cdots (D - \lambda_{n-1} 1_V)(\exp(\lambda_n) t) \neq 0.$$

This measn that μ_D divides $(t - \lambda_1) \cdots (t - \lambda_n)$ but can't be $(t - \lambda_1) \cdots (t - \lambda_{n-1})$. Since the order of the λs is irrelevant this shows that $\mu_D(t) = (t - \lambda_1) \cdots (t - \lambda_n)$.

Finally let us compute the minimal polynomials in two interesting and somewhat tricky situations.

PROPOSITION 16. *The minimal polynimial for*

$$A = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ -\alpha_0 & -\alpha_1 & \cdots & -\alpha_{n-1} \end{bmatrix}$$

is given by

$$\mu_A(t) = t^n + \alpha_{n-1} t^{n-1} + \cdots + \alpha_1 t + \alpha_0.$$

PROOF. It turns out to be easier to calculate the minimal polynomial for the transpose

$$B = A^t = \begin{bmatrix} 0 & 0 & \cdots & 0 & -\alpha_0 \\ 1 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & \cdots & 0 & -\alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -\alpha_{n-1} \end{bmatrix}$$

and it is not hard to see that a matrix and its transpose have the same minimal polynomials.

We claim that $\mu_B(t) = p(t) = \chi_A(t)$. To see this, first note that $e_k = B(e_{k-1})$, for $k = 2, ..., n$ showing that $e_k = B^{k-1}(e_1)$, for $k = 2, ..., n$. Thus the vectors e_1, $B(e_1)$, ..., $B^{n-1}(e_1)$ are linearly independent. This shows that $1_{\mathbb{F}^n}$, B, ..., B^{n-1} must also be linearly independent. Next we can also show that $p(B) = 0$. This is because

$$\begin{aligned} p(B)(e_k) &= p(B) \circ B^{k-1}(e_1) \\ &= B^{k-1} \circ p(B)(e_1) \end{aligned}$$

and $p(B)(e_1) = 0$ since

$$\begin{aligned} p(B)(e_1) &= \left((B)^n + \alpha_{n-1}(B)^{n-1} + \cdots + \alpha_1 B + \alpha_0 1_{\mathbb{F}^n}\right) e_1 \\ &= (B)^n(e_1) + \alpha_{n-1}(B)^{n-1}(e_1) + \cdots + \alpha_1 B(e_1) + \alpha_0 1_{\mathbb{F}^n}(e_1) \\ &= Be_n + \alpha_{n-1}e_n + \cdots + \alpha_1 e_2 + \alpha_0 e_1 \\ &= -\alpha_0 e_1 - \alpha_1 e_2 - \cdots - \alpha_{n-1}e_n \\ &\quad +\alpha_{n-1}e_n + \cdots + \alpha_1 e_2 + \alpha_0 e_1 \\ &= 0. \end{aligned}$$

□

Next we show

Proposition 17. *The minimal polynomial for*

$$C = \begin{bmatrix} \lambda_1 & 1 & & 0 \\ 0 & \lambda_2 & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_n \end{bmatrix}$$

is given by

$$\mu_C(t) = (t - \lambda_1) \cdots (t - \lambda_n).$$

Proof. In fact in the exercises to "Eigenvalues" it was shown that C is similar to A if we define the αs by

$$p(t) = t^n + \alpha_{n-1}t^{n-1} + \cdots + \alpha_1 t + \alpha_0 = (t - \lambda_1) \cdots (t - \lambda_n).$$

The claim can also be established directly by first showing that $p(C) = 0$. This means that μ_C divides p. We then just need to show that $q_i(C) \neq 0$, where

$$q_i(t) = \frac{p(t)}{t - \lambda_i}.$$

The key observation for these facts follow from knowing how to multiply certain upper triangular matrices:

$$\begin{bmatrix} 0 & 1 & 0 & \\ 0 & \gamma_2 & 1 & \\ 0 & 0 & \gamma_3 & \ddots \\ & & & \ddots \end{bmatrix} \begin{bmatrix} \delta_1 & 1 & 0 & \\ 0 & 0 & 1 & \\ 0 & 0 & \delta_3 & \ddots \\ & & & \ddots \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & * & \\ 0 & 0 & \gamma_3\delta_3 & \\ \vdots & \vdots & & \ddots \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & * & \\ 0 & 0 & \gamma_3\delta_3 & \\ & & & \end{bmatrix} \begin{bmatrix} \varepsilon_1 & 1 & 0 & \\ 0 & \varepsilon_2 & 1 & \\ 0 & 0 & 0 & 1 \\ & & & \ddots \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & * \\ 0 & 0 & 0 & * \\ \vdots & \vdots & \vdots & \gamma_4\delta_4\varepsilon_4 \end{bmatrix}$$

Therefore, when we do the multiplication

$$(C - \lambda_1 1_{\mathbb{F}^n})(C - \lambda_2 1_{\mathbb{F}^n}) \cdots (C - \lambda_n 1_{\mathbb{F}^n})$$

by starting at the right, we get that the first k columns are zero in

$$(C - \lambda_1 1_{\mathbb{F}^n})(C - \lambda_2 1_{\mathbb{F}^n}) \cdots (C - \lambda_k 1_{\mathbb{F}^n})$$

but that the $(k+1)^{\text{th}}$ column has 1 as the first entry. Clearly this shows that $p(C) = 0$ as well as $q_n(C) \neq 0$. Since we didn't specify the last λ_n this will also show that $q_i(C) \neq 0$ for all $i = 1, ..., n$. □

4.1. Exercises.

(1) Find the minimal and characteristic polynomials for

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

(2) Assume that $L : V \to V$ has an invariant subspace $M \subset V$. Show that $\mu_{L|_M}$ divides μ_L.

(3) Show that $\mu_L(t) = \mu_{L'}(t)$, where L' is the dual of L. Alternatively show that a matrix and its transpose have the same minimal polynomials.

(4) Let $L : V \to V$ be a linear operator such that $L^2 + 1 = 0$.
   (a) If V is real vector space show that 1_V and L are linearly independent and that $\mu_L(t) = t^2 + 1$.
   (b) If V and L are complex show that 1_V and L need not be linearly independent.
   (c) Find the possibilities for the minimal polynomial of $L^3 + 2L^2 + L + 3$.

(5) Let $L : V \to V$ be a linear operator and $p \in \mathbb{F}[t]$ a polynomial. Show

$$\deg \mu_{p(L)}(t) \leq \deg \mu_L(t).$$

(6) Assume that $L : V \to V$ has minimal polynomial $\mu_L(t) = t^2 + 1$. Find a polynomial $p(t)$ such that $L^{-1} = p(L)$.

(7) Assume that $L : V \to V$ has minimal polynomial $\mu_L(t) = t^3 + 2t + 1$. Find a polynomial $q(t)$ of degree ≤ 2 such that $L^4 = q(L)$.

(8) Assume that $L : V \to V$ has minimal polynomial $\mu_L(t) = t$. Find a matrix representation for L.

(9) If $l \geq \deg(\mu_L) = k$, then show that L^l is a linear combination of $1_V, L, ..., L^{k-1}$. If L is invertible show the same for all $l < 0$.

(10) Show that the minimal polynomial for $D : \ker(p(D)) \to \ker(p(D))$ is $\mu_D = p$.

(11) Let $A \in \text{Mat}_{n\times n}(\mathbb{F})$ and consider the two linear operators $L_A, R_A : \text{Mat}_{n\times n}(\mathbb{F}) \to \text{Mat}_{n\times n}(\mathbb{F})$ defined by $L_A(X) = AX$ and $R_A(X) = XA$. Find the minimal polynomial of L_A, R_A given $\mu_A(t)$.

(12) Consider two matrices A and B, show that the minimal polynomial for the block diagonal matrix

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

is $\mathrm{lcm}\left\{\mu_A, \mu_B\right\}$. Generalize this to block diagonal matrices

$$\begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_k \end{bmatrix}$$

5. Diagonalizability

In this section we shall investigate how and when one can find a basis that puts a linear operator $L : V \to V$ into the simplest possible form. This problem will reappear in Chapter 4 for symmetric and self-adjoint operators, but what we do here is more general. From the section on differential equations we have seen that decoupling the system by finding a basis of eigenvectors for a matrix considerably simplifies the problem of solving the equation. It is from that set-up that we shall take our cue to the simplest form of a linear operator.

A linear operator $L : V \to V$ on a finite dimensional vector space is said to be *diagonalizable* if we can find a basis for V that consists of eigenvectors for L, i.e., a basis e_1, ..., e_n for V such that $L(e_i) = \lambda_i e_i$ for all $i = 1, ..., n$. This is the same as saying that

$$\begin{bmatrix} L(e_1) & \cdots & L(e_n) \end{bmatrix} = \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{bmatrix}.$$

In other words, the matrix representation for L is a diagonal matrix.

One advantage of having a basis that diagonalizes a linear operator L is that it becomes much simpler to calculate the powers L^k since $L^k(e_i) = \lambda_i^k e_i$. More generally if $p(t) \in \mathbb{F}[t]$, then we have $p(L)(e_i) = p(\lambda_i) e_i$. Thus $p(L)$ is diagonalized with respect to the same basis and with eigenvalues $p(\lambda_i)$.

We are now ready for a few examples and then the promised application of diagonalizability.

Example 58. *The derivative map $D : P_n \to P_n$ is not diagonalizable. We already know that is has a matrix representation that is upper triangular and with zeros on the diagonal. Thus the characteristic polynomial is t^{n+1}. So the only eigenvalue is 0. Therefore, had D been diagonalizable it would have had to be the zero transformation 0_{P_n}. Since this is not true we conclude that $D : P_n \to P_n$ is not diagonalizable.*

Example 59. *Let $V = \mathrm{span}\left\{\exp(\lambda_1 t), ..., \exp(\lambda_n t)\right\}$ and consider again the derivative map $D : V \to V$. Then we have $D(\exp(\lambda_i t)) = \lambda_i \exp(\lambda_i t)$. So if we extract a basis for V among the functions $\exp(\lambda_1 t)$, ..., $\exp(\lambda_n t)$, then we have found a basis of eigenvectors for D.*

These two examples show that diagonalizability is not just a property of the operator. It really matters what space the operator is restricted to live on. We can exemplify this with matrices as well.

EXAMPLE 60. *Consider*

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

As a map $A : \mathbb{R}^2 \to \mathbb{R}^2$, *this operator cannot be diagonalizable as it rotates vectors. However, as a map* $A : \mathbb{C}^2 \to \mathbb{C}^2$ *it has two eigenvalues* $\pm i$ *with eigenvectors*

$$\begin{bmatrix} 1 \\ \mp i \end{bmatrix}.$$

As these eigenvectors form a basis for $\mathbb{C}^2$ *we conclude that* $A : \mathbb{C}^2 \to \mathbb{C}^2$ *is diagonalizable.*

We have already seen how decoupling systems of differential equations is related to being able to diagonalize a matrix. Below we give a different type of example of how diagonalizability can be used to investigate a mathematical problem.

Consider the Fibonacci sequence $1, 1, 2, 3, 5, 8, \ldots$ where each element is the sum of the previous two elements. Therefore, if ϕ_n is the n^{th} term in the sequence, then $\phi_{n+2} = \phi_{n+1} + \phi_n$, with initial values $\phi_0 = 1, \phi_1 = 1$. If we record the elements in pairs

$$\Phi_n = \begin{bmatrix} \phi_n \\ \phi_{n+1} \end{bmatrix} \in \mathbb{R}^2,$$

then the relationship takes the form

$$\begin{aligned} \begin{bmatrix} \phi_{n+1} \\ \phi_{n+2} \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \phi_n \\ \phi_{n+1} \end{bmatrix}, \\ \Phi_{n+1} &= A\Phi_n. \end{aligned}$$

The goal is to find a general formula for ϕ_n and to discover what happens as $n \to \infty$. The matrix relationship tells us that

$$\begin{aligned} \Phi_n &= A^n \Phi_0, \\ \begin{bmatrix} \phi_n \\ \phi_{n+1} \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^n \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \end{aligned}$$

Thus we must find a formula for

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^n.$$

This is where diagonalization comes in handy. The matrix A has characteristic polynomial

$$t^2 - t - 1 = \left(t - \frac{1+\sqrt{5}}{2} \right) \left(t - \frac{1-\sqrt{5}}{2} \right).$$

The corresponding eigenvectors for $\frac{1\pm\sqrt{5}}{2}$ are $\begin{bmatrix} 1 \\ \frac{1\pm\sqrt{5}}{2} \end{bmatrix}$. So

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{bmatrix},$$

or

$$\begin{aligned}
\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} &= \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix}^{-1} \\
&= \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} \frac{1}{2} - \frac{1}{2\sqrt{5}} & \frac{1}{\sqrt{5}} \\ \frac{1}{2} + \frac{1}{2\sqrt{5}} & -\frac{1}{\sqrt{5}} \end{bmatrix}.
\end{aligned}$$

This means that

$$\begin{aligned}
&\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^n \\
&= \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{bmatrix}^n \begin{bmatrix} \frac{1}{2} - \frac{1}{2\sqrt{5}} & \frac{1}{\sqrt{5}} \\ \frac{1}{2} + \frac{1}{2\sqrt{5}} & -\frac{1}{\sqrt{5}} \end{bmatrix} \\
&= \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} \left(\frac{1+\sqrt{5}}{2}\right)^n & 0 \\ 0 & \left(\frac{1-\sqrt{5}}{2}\right)^n \end{bmatrix} \begin{bmatrix} \frac{1}{2} - \frac{1}{2\sqrt{5}} & \frac{1}{\sqrt{5}} \\ \frac{1}{2} + \frac{1}{2\sqrt{5}} & -\frac{1}{\sqrt{5}} \end{bmatrix} \\
&= \left[\begin{matrix} \left(\frac{1+\sqrt{5}}{2}\right)^n \left(\frac{1}{2} - \frac{1}{2\sqrt{5}}\right) + \left(\frac{1-\sqrt{5}}{2}\right)^n \left(\frac{1}{2} + \frac{1}{2\sqrt{5}}\right) \\ \left(\frac{1+\sqrt{5}}{2}\right)^{n+1} \left(\frac{1}{2} - \frac{1}{2\sqrt{5}}\right) + \left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \left(\frac{1}{2} + \frac{1}{2\sqrt{5}}\right) \end{matrix} \right. \\
&\qquad \left. \begin{matrix} \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n \\ \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \end{matrix} \right]
\end{aligned}$$

Hence

$$\begin{aligned}
\phi_n &= \left(\frac{1+\sqrt{5}}{2}\right)^n \left(\frac{1}{2} - \frac{1}{2\sqrt{5}}\right) + \left(\frac{1-\sqrt{5}}{2}\right)^n \left(\frac{1}{2} + \frac{1}{2\sqrt{5}}\right) \\
&\quad + \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n \\
&= \left(\frac{1}{2} + \frac{1}{2\sqrt{5}}\right) \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n \left(\frac{1}{2} - \frac{1}{2\sqrt{5}}\right) \\
&= \left(\frac{1+\sqrt{5}}{2\sqrt{5}}\right) \left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \left(\frac{1-\sqrt{5}}{2\sqrt{5}}\right) \\
&= \left(\frac{1}{\sqrt{5}}\right) \left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1}{\sqrt{5}}\right) \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}
\end{aligned}$$

The ratio of successive Fibonacci numbers satisfies

$$\begin{aligned}\frac{\phi_{n+1}}{\phi_n} &= \frac{\left(\frac{1}{\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^{n+2}-\left(\frac{1}{\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^{n+2}}{\left(\frac{1}{\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}-\left(\frac{1}{\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n+2}-\left(\frac{1-\sqrt{5}}{2}\right)^{n+2}}{\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}-\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)-\left(\frac{1-\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{1+\sqrt{5}}\right)^{n+1}}{1-\left(\frac{1-\sqrt{5}}{1+\sqrt{5}}\right)^{n+1}}\end{aligned}$$

where $\left(\frac{1-\sqrt{5}}{1+\sqrt{5}}\right)^{n+1} \to 0$ as $n \to \infty$. Thus

$$\lim_{n\to\infty}\frac{\phi_{n+1}}{\phi_n} = \frac{1+\sqrt{5}}{2},$$

which is the Golden Ratio. This ratio is often denoted by ϕ. The Fibonacci sequence is often observed in growth phenomena in nature and is also of fundamental importance in combinatorics.

It is not easy to come up with a criterion that guarantees that a matrix is diagonalizable and which is also easy to use. We shall see that symmetric matrices with real entries are diagonalizable in Chapter 4. It turns out that the minimal polynomial holds the key to diagonalizability of an operator.

In general what one has to do for an operator $L : V \to V$ is compute the eigenvalues, then list them without multiplicities $\lambda_1, ..., \lambda_k$, then calculate all the eigenspaces $\ker(L - \lambda_i 1_V)$, and finally, check if one can find a basis of eigenvectors. To help us with this process there are some useful abstract results about the relationship between the eigenspaces.

LEMMA 14. (Eigenspaces form Direct Sums) *If $\lambda_1, ..., \lambda_k$ are distinct eigenvalues for a linear operator $L : V \to V$, then*

$$\ker(L-\lambda_1 1_V)+\cdots+\ker(L-\lambda_k 1_V) = \ker(L-\lambda_1 1_V)\oplus\cdots\oplus\ker(L-\lambda_k 1_V).$$

In particular we have

$$k \leq \dim(V).$$

PROOF. The proof uses induction on k. When $k = 1$ there is nothing to prove. Assume that the result is true for any collection of k distinct eigenvalues for L and suppose that we have $k+1$ distinct eigenvalues $\lambda_1, ..., \lambda_{k+1}$ for L. Since we already know that

$$\ker(L-\lambda_1 1_V)+\cdots+\ker(L-\lambda_k 1_V) = \ker(L-\lambda_1 1_V)\oplus\cdots\oplus\ker(L-\lambda_k 1_V)$$

it will be enough to prove that

$$(\ker(L-\lambda_1 1_V)+\cdots+\ker(L-\lambda_k 1_V))\cap\ker(L-\lambda_{k+1}1_V) = \{0\}.$$

In other words we claim that that if $L(x) = \lambda_{k+1}x$ and $x = x_1 + \cdots + x_k$ where $x_i \in \ker(L - \lambda_i 1_V)$, then $x = 0$. We can prove this in two ways.

First note that if $k=1$, then $x=x_1$ implies that x is the eigenvector for two different eigenvalues. This is clearly not possible unless $x=0$. Thus we can assume that $k>1$. In that case

$$\begin{aligned}\lambda_{k+1}x &= L(x)\\ &= L(x_1+\cdots+x_k)\\ &= \lambda_1x_1+\cdots+\lambda_kx_k.\end{aligned}$$

Subtracting yields

$$0=(\lambda_1-\lambda_{k+1})x_1+\cdots+(\lambda_k-\lambda_{k+1})x_k$$

Since we assumed that

$$\ker(L-\lambda_1 1_V)+\cdots+\ker(L-\lambda_k 1_V)=\ker(L-\lambda_1 1_V)\oplus\cdots\oplus\ker(L-\lambda_k 1_V)$$

it follows that $(\lambda_1-\lambda_{k+1})x_1=0$, ..., $(\lambda_k-\lambda_{k+1})x_k=0$. As $(\lambda_1-\lambda_{k+1})\neq 0$, ..., $(\lambda_k-\lambda_{k+1})\neq 0$ we conclude that $x_1=0$, ..., $x_k=0$, implying that $x=x_1+\cdots+x_k=0$.

The second way of doing the induction is slightly trickier, but also more elegant. This proof will in addition give us an interesting criterion for when an operator is diagonalizable. Since $\lambda_1,...,\lambda_{k+1}$ are different the polynomials $t-\lambda_1$, ..., $t-\lambda_{k+1}$ have 1 as their greatest common divisor. Thus also $(t-\lambda_1)\cdots(t-\lambda_k)$ and $(t-\lambda_{k+1})$ have 1 as their greatest common divisor. This means that we can find polynomials $p(t),q(t)\in\mathbb{F}[t]$ such that

$$1=p(t)(t-\lambda_1)\cdots(t-\lambda_k)+q(t)(t-\lambda_{k+1}).$$

If we put the operator L into this formula in place of t we get:

$$1_V=p(L)(L-\lambda_1 1_V)\cdots(L-\lambda_k 1_V)+q(L)(L-\lambda_{k+1}1_V).$$

Applying this to x gives us

$$x=p(L)(L-\lambda_1 1_V)\cdots(L-\lambda_k 1_V)(x)+q(L)(L-\lambda_{k+1}1_V)(x).$$

If

$$x\in(\ker(L-\lambda_1 1_V)+\cdots+\ker(L-\lambda_k 1_V))\cap\ker(L-\lambda_{k+1}1_V)$$

then

$$\begin{aligned}(L-\lambda_1 1_V)\cdots(L-\lambda_k 1_V)(x) &= 0,\\ (L-\lambda_{k+1}1_V)(x) &= 0\end{aligned}$$

so also $x=0$. □

This gives us three criteria for diagonalizability.

Theorem 20. (First Characterization of Diagonalizability) *Let $L:V\to V$ be a linear operator on an n-dimensional vector space over $\mathbb{F}$. If $\lambda_1,...,\lambda_k\in\mathbb{F}$ are distinct eigenvalues for L such that*

$$n=\dim(\ker(L-\lambda_1 1_V))+\cdots+\dim(\ker(L-\lambda_k 1_V)),$$

Then L is diagonalizable. In particular, if L has n distinct eigenvalues in $\mathbb{F}$, then L is diagonalizable.

Proof. Our assumption together with the above lemma shows that

$$\begin{aligned} n &= \dim\left(\ker\left(L-\lambda_1 1_V\right)\right)+\cdots+\dim\left(\ker\left(L-\lambda_k 1_V\right)\right) \\ &= \dim\left(\ker\left(L-\lambda_1 1_V\right)+\cdots+\ker\left(L-\lambda_k 1_V\right)\right). \end{aligned}$$

Thus

$$\ker\left(L-\lambda_1 1_V\right)\oplus\cdots\oplus\ker\left(L-\lambda_k 1_V\right)=V$$

and we can find a basis of eigenvectors, by selecting a basis for each of the eigenspaces.

For the last statement we only need to observe that $\dim\left(\ker\left(L-\lambda 1_V\right)\right)\geq 1$ for any eigenvalue $\lambda\in\mathbb{F}$. □

The next characterization offers a particularly nice condition for diagonalizability which will give us the minimal polynomial characterization of diagonalizability.

Theorem 21. (Second Characterization of Diagonalizability) *Let $L:V\to V$ be a linear operator on an n-dimensional vector space over $\mathbb{F}$. L is diagonalizable if and only if we can find $p\in\mathbb{F}[t]$ such that $p(L)=0$ and*

$$p(t)=(t-\lambda_1)\cdots(t-\lambda_k),$$

where $\lambda_1,...,\lambda_k\in\mathbb{F}$ are distinct.

Proof. Assuming that L is diagonalizable we have

$$V=\ker\left(L-\lambda_1 1_V\right)\oplus\cdots\oplus\ker\left(L-\lambda_k 1_V\right).$$

So if we use

$$p(t)=(t-\lambda_1)\cdots(t-\lambda_k)$$

we see that $p(L)=0$ as $p(L)$ vanishes on each of the eigenspaces.

Conversely assume that $p(L)=0$ and

$$p(t)=(t-\lambda_1)\cdots(t-\lambda_k),$$

where $\lambda_1,...,\lambda_k\in\mathbb{F}$ are distinct. If some of these λs are not eigenvalues for L we can eliminate them. We then still have that L is a root of the new polynomial as $L-\lambda 1_V$ is an isomorphism unless λ is an eigenvalue. The proof now goes by induction on the number of roots in p. If there is one root the result is obvious. If $k\geq 2$ we can write

$$\begin{aligned} 1 &= r(t)(t-\lambda_1)\cdots(t-\lambda_{k-1})+s(t)(t-\lambda_k) \\ &= r(t)q(t)+s(t)(t-\lambda_k). \end{aligned}$$

We then claim that

$$V=\ker(q(L))\oplus\ker\left(L-\lambda_k 1_V\right)$$

and that

$$L(\ker(q(L)))\subset\ker(q(L)).$$

This will finish the induction step as $L|_{\ker(q(L))}$ then becomes a linear operator which is a root of q.

To establish the decomposition observe that

$$\begin{aligned} x &= q(L)(r(L)(x))+\left(L-\lambda_k 1_V\right)(s(L)(x)) \\ &= y+z. \end{aligned}$$

Here $y \in \ker(L - \lambda_k 1_V)$ since

$$\begin{aligned}(L - \lambda_k 1_V)(y) &= (L - \lambda_k 1_V)(q(L)(r(L)(x))) \\ &= p(L)(r(L)(x)) \\ &= 0,\end{aligned}$$

and $z \in \ker(q(L))$ since

$$q(L)((L - \lambda_k 1_V)(s(L)(x))) = p(L)(s(L)(x)) = 0.$$

Thus

$$V = \ker(q(L)) + \ker(L - \lambda_k 1_V).$$

If

$$x \in \ker(q(L)) \cap \ker(L - \lambda_k 1_V),$$

then we have

$$x = r(L)(q(L)(x)) + s(L)((L - \lambda_k 1_V)(x)) = 0.$$

This gives the direct sum decomposition.

Finally if $x \in \ker(q(L))$, then we see that

$$\begin{aligned}q(L)(L(x)) &= (q(L) \circ L)(x) \\ &= (L \circ q(L))(x) \\ &= L(q(L)(x)) \\ &= 0.\end{aligned}$$

Thus showing that $L(x) \in \ker(q(L))$. □

COROLLARY 16. (The Minimal Polynomial Characterization of Diagonalizability) *Let $L : V \to V$ be a linear operator on an n-dimensional vector space over $\mathbb{F}$. L is diagonalizable if and only if the minimal polynomial factors*

$$\mu_L(t) = (t - \lambda_1) \cdots (t - \lambda_k),$$

and has no multiple roots, i.e., $\lambda_1, ..., \lambda_k \in \mathbb{F}$ are distinct.

Finally we can estimate how large $\dim(\ker(L - \lambda 1_V))$ can be if we have factored the characteristic polynomial.

LEMMA 15. *Let $L : V \to V$ be a linear operator on an n-dimensional vector space over $\mathbb{F}$. If $\lambda \in \mathbb{F}$ is an eigenvalue and $\chi_L(t) = (t - \lambda)^m q(t)$, where $q(\lambda) \neq 0$, then*

$$\dim(\ker(L - \lambda 1_V)) \leq m.$$

We call $\dim(\ker(L - \lambda 1_V))$ the *geometric multiplicity* of λ and m the *algebraic multiplicity* of λ.

PROOF. Select a complement N to $\ker(L - \lambda 1_V)$ in V. Then choose a basis where $x_1, ..., x_k \in \ker(L - \lambda 1_V)$ and $x_{k+1}, ..., x_n \in N$. Since $L(x_i) = \lambda x_i$ for $i = 1, ..., k$ we see that the matrix representation has a block form that looks like

$$[L] = \begin{bmatrix} \lambda 1_{\mathbb{F}^k} & B \\ 0 & C \end{bmatrix}.$$

This implies that

$$\begin{aligned} \chi_L(t) &= \chi_{[L]}(t) \\ &= \chi_{\lambda 1_{\mathbb{F}^k}}(t)\,\chi_C(t) \\ &= (t-\lambda)^k\,\chi_C(t) \end{aligned}$$

and hence that λ has algebraic multiplicity $m \geq k$. □

Clearly the appearance of multiple roots in the characteristic polynomial is something that might prevent linear operators from becoming diagonalizable. The following criterion is often useful for deciding whether or not a polynomial has multiple roots.

PROPOSITION 18. *A polynomial $p(t) \in \mathbb{F}[t]$ has $\lambda \in \mathbb{F}$ as a multiple root if and only if λ is a root of both p and Dp.*

PROOF. If λ is a multiple root, then $p(t) = (t-\lambda)^m q(t)$, where $m \geq 2$. Thus

$$Dp(t) = m(t-\lambda)^{m-1} q(t) + (t-\lambda)^m Dq(t)$$

also has λ as a root.

Conversely if λ is a root of Dp and p, then we can write $p(t) = (t-\lambda)q(t)$ and

$$\begin{aligned} 0 &= Dp(\lambda) \\ &= q(\lambda) + (\lambda-\lambda)Dq(\lambda) \\ &= q(\lambda). \end{aligned}$$

Thus also $q(t)$ has λ as a root and hence λ is a multiple root of $p(t)$. □

EXAMPLE 61. *If $p(t) = t^2 + \alpha t + \beta$, then $Dp(t) = 2t + \alpha$. Thus we have a double root only if the root $t = -\frac{\alpha}{2}$ of Dp is a root of p. If we evaluate*

$$\begin{aligned} p\left(-\frac{\alpha}{2}\right) &= \frac{\alpha^2}{4} - \frac{\alpha^2}{2} + \beta \\ &= -\frac{\alpha^2}{4} + \beta \\ &= -\frac{\alpha^2 - 4\beta}{4} \end{aligned}$$

we see that this occurs precisely when the discriminant vanishes. This conforms nicely with the quadratic formula for the roots.

EXAMPLE 62. *If $p(t) = t^3 + 12t^2 - 14$, then the roots are pretty nasty. We can, however, check for multiple roots by finding the roots of*

$$Dp(t) = 3t^2 + 24t = 3t(t+8)$$

and cheking whether they are roots of p

$$\begin{aligned} p(0) &= -14 \neq 0, \\ p(8) &= 8^3 + 12 \cdot 8^2 - 14 \\ &= 8^2(8+12) - 14 > 0. \end{aligned}$$

As an application of the above characterizations of diagonalizability we can now complete some of our discussions about solving n^{th} order differential equations where there are no multiple roots in the characteristic polynomial.

First we wish to give a new proof that $\exp(\lambda_1 t)$, ..., $\exp(\lambda_n t)$ are linearly independent if $\lambda_1, ..., \lambda_n$ are distinct. For that we consider $V = \text{span}\{\exp(\lambda_1 t), ..., \exp(\lambda_n t)\}$ and $D : V \to V$. The result is now obvious as each of the functions $\exp(\lambda_i t)$ is an eigenvector with eigenvalue λ_i for $D : V \to V$. As $\lambda_1, ..., \lambda_n$ are distinct we can conclude that the corresponding eigenfunctions are linearly independent. Thus $\exp(\lambda_1 t)$, ..., $\exp(\lambda_n t)$ form a basis for V which diagonalizes D.

In order to solve the initial value problem for higher order differential equations it was necessary to show that the *Vandermonde matrix*

$$\begin{bmatrix} 1 & \cdots & 1 \\ \lambda_1 & \cdots & \lambda_n \\ \vdots & \ddots & \vdots \\ \lambda_1^{n-1} & \cdots & \lambda_n^{n-1} \end{bmatrix}$$

is invertible, when $\lambda_1, ..., \lambda_n \in \mathbb{F}$ are distinct. This was done is "Linear Independence" and will now be established using eigenvectors. Given the origins of this problem (in this book) it is not unnatural to consider a matrix

$$A = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ -\alpha_0 & -\alpha_1 & \cdots & -\alpha_{n-1} \end{bmatrix},$$

where

$$\begin{aligned} p(t) &= t^n + \alpha_{n-1}t^{n-1} + \cdots + \alpha_1 t + \alpha_0 \\ &= (t - \lambda_1) \cdots (t - \lambda_n). \end{aligned}$$

The characteristic polynomial for A is then $p(t)$ and hence $\lambda_1, ..., \lambda_n \in \mathbb{F}$ are the eigenvalues. When these eigenvalues are distinct we therefore know that the corresponding eigenvectors are linearly independent. To find these eigenvectors note that

$$
\begin{aligned}
A\begin{bmatrix} 1 \\ \lambda_k \\ \vdots \\ \lambda_k^{n-1} \end{bmatrix} &= \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ -\alpha_0 & -\alpha_1 & \cdots & -\alpha_{n-1} \end{bmatrix} \begin{bmatrix} 1 \\ \lambda_k \\ \vdots \\ \lambda_k^{n-1} \end{bmatrix} \\
&= \begin{bmatrix} \lambda_k \\ \lambda_k^2 \\ \vdots \\ -\alpha_0 - \alpha_1 \lambda_k - \cdots - \alpha_{n-1}\lambda_k^{n-1} \end{bmatrix} \\
&= \begin{bmatrix} \lambda_k \\ \lambda_k^2 \\ \vdots \\ \lambda_k^n \end{bmatrix}, \text{ since } p(\lambda_k) = 0 \\
&= \lambda_k \begin{bmatrix} 1 \\ \lambda_k \\ \vdots \\ \lambda_k^{n-1} \end{bmatrix}.
\end{aligned}
$$

This implies that the columns in the Vandermonde matrix are the eigenvectors for a diagonalizable operator. Hence it must be invertible. Note that A is diagonalizable if and only if $\lambda_1, ..., \lambda_n$ are distinct as all eigenspaces for A are 1 dimensional (we shall also prove and use this in the next section "Cyclic Subspaces").

An interesting special case occurs when $p(t) = t^n - 1$ and we assume that $\mathbb{F} = \mathbb{C}$. Then the roots are the n^{th} roots of unity and the operator that has these numbers as eigenvalues looks like

$$
C = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ 1 & 0 & \cdots & 0 \end{bmatrix}.
$$

The powers of this matrix have the following interesting patterns:

$$
\begin{aligned}
C^2 &= \begin{bmatrix} 0 & 0 & 1 & 0 & & 0 \\ & 0 & 0 & \ddots & & \\ & & & & 1 & 0 \\ 0 & & & & 0 & 1 \\ 1 & 0 & & & 0 & 0 \\ 0 & 1 & 0 & & & 0 \end{bmatrix}, \\
&\vdots \\
C^{n-1} &= \begin{bmatrix} 0 & \cdots & \cdots & 1 \\ 1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 1 & 0 \end{bmatrix}, \\
C^n &= \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} = 1_{\mathbb{F}^n}.
\end{aligned}
$$

A linear combination of these powers looks like:

$$
\begin{aligned}
C_{\alpha_0,\dots,\alpha_{n-1}} &= \alpha_0 1_{\mathbb{F}^n} + \alpha_1 C + \cdots + \alpha_{n-1} C^{n-1} \\
&= \begin{bmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{n-1} \\ \alpha_{n-1} & \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-2} \\ \vdots & \alpha_{n-1} & \alpha_0 & \ddots & & \vdots \\ \alpha_3 & \vdots & \alpha_{n-1} & \ddots & & \\ \alpha_2 & \alpha_3 & \vdots & \ddots & \alpha_0 & \alpha_1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{n-1} & \alpha_0 \end{bmatrix}
\end{aligned}
$$

Since we have a basis that diagonalizes C and hence also all of its powers, we have also found a basis that diagonalizes $C_{\alpha_0,\dots,\alpha_{n-1}}$. This would probably not have been so easy to see if we had just been handed the matrix $C_{\alpha_0,\dots,\alpha_{n-1}}$.

5.1. Exercises.

(1) Decide whether or not the following matrices are diagonalizable.

(a) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$

(b) $\begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 3 \\ 2 & 3 & 0 \end{bmatrix}$

(c) $\begin{bmatrix} 0 & 1 & 2 \\ -1 & 0 & 3 \\ -2 & -3 & 0 \end{bmatrix}$

(2) Decide whether or not the following matrices are diagonalizable.

(a) $\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$

(b) $\begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$

(c) $\begin{bmatrix} 1 & i & 0 \\ i & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix}$

(3) Decide whether or not the following matrices are diagonalizable.

(a) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$

(b) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$

(c) $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

(4) Find the characteristic polynomial, eigenvalues and eigenvectors for each of the following linear operators $L : P_3 \to P_3$. Then decide whether they are diagonalizable by checking whether there is a basis for eigenvectors.

(a) $L = D$.

(b) $L = tD = T \circ D$.

(c) $L = D^2 + 2D + 1$.

(d) $L = t^2D^3 + D$.

(5) Consider the linear operator on $\mathrm{Mat}_{n\times n}(\mathbb{F})$ defined by $L(X) = X^t$. Show that L is diagonalizable. Compute the eigenvalues and eigenspaces.

(6) For which s, t is the matrix diagonalizable

$$\begin{bmatrix} 1 & 1 \\ s & t \end{bmatrix}?$$

(7) For which α, β, γ is the matrix diagonalizable

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha & \beta & \gamma \end{bmatrix}?$$

(8) Assume $L : V \to V$ is diagonalizable. Show that $V = \ker(L) \oplus \mathrm{im}(L)$.

(9) Assume that $L : V \to V$ is a diagonalizable real linear map. Show that $\mathrm{tr}\left(L^2\right) \geq 0$.

(10) Assume that $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ is diagonalizable.

(a) Show that A^t is diagonalizable.

(b) Show that $L_A(X) = AX$ defines a diagonalizable operator on $\mathrm{Mat}_{n\times n}(\mathbb{F})$.

(c) Show that $R_A(X) = XA$ defines a diagonalizable operator on $\mathrm{Mat}_{n\times n}(\mathbb{F})$.

(11) If $E : V \to V$ is a projection on a finite dimensional space, then $\mathrm{tr}(E) = \dim(\mathrm{im}(E))$.

(12) Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ and $B \in \mathrm{Mat}_{m\times m}(\mathbb{F})$ and consider

$$\begin{aligned} L &: \mathrm{Mat}_{n\times m}(\mathbb{F}) \to \mathrm{Mat}_{n\times m}(\mathbb{F}), \\ L(X) &= AX - XB. \end{aligned}$$

Show that if B is diagonalizable, then all eigenvalues of L are of the form $\lambda - \mu$, where λ is an eigenvalue of A and μ an eigenvalue of B.

(13) *(Restrictions of Diagonalizable Operators)* Let $L : V \to V$ be a diagonalizable operator and $M \subset V$ a subspace such that $L(M) \subset M$.
   (a) If $x + y \in M$, where $L(x) = \lambda x$, $L(y) = \mu y$, and $\lambda \neq \mu$, then $x, y \in M$.
   (b) If $x_1 + \cdots + x_k \in M$ and $L(x_i) = \lambda_i x_i$, where $\lambda_1, ..., \lambda_k$ are distinct, then $x_1, ..., x_k \in M$. Hint: Use induction on k.
   (c) Show that $L : M \to M$ is diagonalizable.
   (d) Now use the Second Characterization of Diagonalizability to show directly that $L : M \to M$ is diagonalizable.

(14) Let $L : V \to V$ be a linear operator on a finite dimensional vector space. Show that λ is a multiple root for $\mu_L(t)$ if and only if

$$\{0\} \subsetneqq \ker(L - \lambda 1_V) \subsetneqq \ker\left((L - \lambda 1_V)^2\right).$$

(15) Assume that $L, K : V \to V$ are both diagonalizable and that $KL = LK$. Show that we can find a basis for V that diagonalizes both L and K. Hint: you can use the previous exercise with M as an eigenspace for one of the operators.

(16) Let $L : V \to V$ be an operator on a vector space and $\lambda_1, ..., \lambda_k$ distinct eigenvalues. If $x = x_1 + \cdots + x_k$, where $x_i \in \ker(L - \lambda_i 1_V)$, then

$$(L - \lambda_1 1_V) \cdots (L - \lambda_k 1_V)(x) = 0.$$

(17) Let $L : V \to V$ be an operator on a vector space and $\lambda \neq \mu$. Use the equation

$$\frac{1}{\mu - \lambda}(L - \lambda 1_V) - \frac{1}{\mu - \lambda}(L - \mu 1_V) = 1_V$$

to show that two eigenspaces for L have trivial intersection.

(18) Consider an *involution* $L : V \to V$, i.e., $L^2 = 1_V$.
   (a) Show that $x \pm L(x)$ is an eigenvector for L with eigenvalue ± 1.
   (b) Show that $V = \ker(L + 1_V) \oplus \ker(L - 1_V)$.
   (c) Conclude that L is diagonalizable.

(19) Assume $L : V \to V$ satisfies $L^2 + \alpha L + \beta 1_V = 0$ and that the roots λ_1, λ_2 of $\lambda^2 + \alpha\lambda + \beta$ are distinct and lie in $\mathbb{F}$.
   (a) Determine γ, δ so that

$$x = \gamma(L(x) - \lambda_1 x) + \delta(L(x) - \lambda_2 x).$$

   (b) Show that $L(x) - \lambda_1 x$ is an eigenvector for L with eigenvalue λ_2 and $L(x) - \lambda_2 x$ is an eigenvector for L with eigenvalue λ_1.
   (c) Conclude that $V = \ker(L - \lambda_1 1_V) \oplus \ker(L - \lambda_2 1_V)$.
   (d) Conclude that L is diagonalizable.

(20) Let $L : V \to V$ be a linear operator with minimal polynomial $m_L(t) = p(t)q(t)$, where $\gcd\{p, q\} = 1$. Show that $V = \ker(p(L)) \oplus \ker(q(L))$ and that $m_{L|_{\ker(p(L))}} = p$ and $m_{L|_{\ker(q(L))}} = q$. Hint: Look at the second proof of why eigenspaces form direct sums.

6. Cyclic Subspaces

Let $L : V \to V$ be a linear operator on a finite dimensional vector space. A subspace $M \subset V$ is said to be L *invariant* or simply invariant if $L(M) \subset M$. Thus the restriction of L to M defines a new linear operator $L|_M : M \to M$. We see that eigenvectors generate one dimensional invariant subspaces and more generally that eigenspaces $\ker(L - \lambda 1_V)$ are L-invariant.

The goal of this section is to find a relatively simple matrix representation for operators L that aren't necessarily diagonalizable. The way in which this is going to be achieved is by finding a decomposition $V = M_1 \oplus \cdots \oplus M_k$ into L-invariant subspaces M_i with the property that $L|_{M_i}$ has matrix representation that can be found by only knowing the characteristic or minimal polynomial for $L|_{M_i}$.

The invariant subspaces we are going to use are in fact a very natural generalization of eigenvectors. First we observe that $x \in V$ is an eigenvector if $L(x) \in \operatorname{span}\{x\}$ or in other words $L(x)$ is a linear combination of x. In case $L(x)$ is not a multiple of x we consider the *cyclic subspace* generated by all of the vectors $x,\ L(x),\ ....,\ L^k(x),\ ....$

$$C_x = \operatorname{span}\left\{x, L(x), L^2(x), ..., L^k(x), ...\right\}.$$

Assuming $x \neq 0$, we can find a smallest $k \geq 1$ such that

$$L^k(x) \in \operatorname{span}\left\{x, L(x), L^2(x), ..., L^{k-1}(x)\right\}.$$

With this definition and construction behind us we can now prove.

Lemma 16. *Let $L : V \to V$ be a linear operator on an n-dimensional vector space. Then C_x is L-invariant and we can find $k \leq \dim(V)$ so that $x,\ L(x),\ L^2(x),\ ...,\ L^{k-1}(x)$ form a basis for C_x. The matrix representation for $L|_{C_x}$ with respect to this basis is*

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & \alpha_0 \\ 1 & 0 & \cdots & 0 & \alpha_1 \\ 0 & 1 & \cdots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \alpha_{k-1} \end{bmatrix}$$

where

$$L^k(x) = \alpha_0 x + \alpha_1 L(x) + \cdots + \alpha_{k-1} L^{k-1}(x).$$

Proof. The vectors $x, L(x), L^2(x), ..., L^{k-1}(x)$ must be linearly independent if we pick k as the smallest k such that

$$L^k(x) = \alpha_0 x + \alpha_1 L(x) + \cdots + \alpha_{k-1} L^{k-1}(x).$$

To see that they span C_x we need to show that

$$L^m(x) \in \operatorname{span}\left\{x, L(x), L^2(x), ..., L^{k-1}(x)\right\}$$

for all $m \geq k$. We are going to use induction on m to prove this. If $m = 0, ...k-1$, there is nothing to prove. Assuming that

$$L^{m-1}(x) = \beta_0 x + \beta_1 L(x) + \cdots + \beta_{k-1} L^{k-1}(x)$$

we get

$$L^m(x) = \beta_0 L(x) + \beta_1 L^2(x) + \cdots + \beta_{k-1} L^k(x).$$

Since we already have that

$$L^k(x) \in \operatorname{span}\left\{x, L(x), L^2(x), ..., L^{k-1}(x)\right\}$$

it follows that

$$L^m(x) \in \operatorname{span}\left\{x, L(x), L^2(x), ..., L^{k-1}(x)\right\}.$$

This completes the induction step. This also explains why C_x is L invariant. Namely, if $z \in C_x$, then we have

$$z = \gamma_0 x + \gamma_1 L(x) + \cdots + \gamma_{k-1} L^{k-1}(x),$$

and

$$L(z) = \gamma_0 L(x) + \gamma_1 L^2(x) + \cdots + \gamma_{k-1} L^k(x).$$

As $L^k(x) \in C_x$ we see that $L(z) \in C_x$ as well.

To find the matrix representation we note that

$$\begin{aligned}
& \begin{bmatrix} L(x) & L(L(x)) & \cdots & L\left(L^{k-2}(x)\right) & L\left(L^{k-1}(x)\right) \end{bmatrix} \\
= & \begin{bmatrix} L(x) & L^2(x) & \cdots & L^{k-1}(x) & L^k(x) \end{bmatrix} \\
= & \begin{bmatrix} x & L(x) & \cdots & L^{k-2}(x) & L^{k-1}(x) \end{bmatrix} \begin{bmatrix} 0 & 0 & \cdots & 0 & \alpha_0 \\ 1 & 0 & \cdots & 0 & \alpha_1 \\ 0 & 1 & \cdots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \alpha_{k-1} \end{bmatrix}.
\end{aligned}$$

This proves the lemma. □

The matrix representation for $L|_{C_x}$ is apparently the transpose of the type of matrix coming from higher order differential equations that we studied in the previous sections. Therefore, we can expect our knowledge of those matrices to carry over without much effort. To be a little more precise we define the *companion matrix* of a monic polynomial $p(t) \in \mathbb{F}[t]$ as the matrix

$$\begin{aligned}
C_p & = \begin{bmatrix} 0 & 0 & \cdots & 0 & -\alpha_0 \\ 1 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & \cdots & 0 & -\alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -\alpha_{n-1} \end{bmatrix}, \\
p(t) & = t^n + \alpha_{n-1} t^{n-1} + \cdots + \alpha_1 t + \alpha_0.
\end{aligned}$$

It is worth mentioning that the companion matrix for $p = t + \alpha$ is simply the 1×1 matrix $[-\alpha]$.

PROPOSITION 19. *The characteristic and minimal polynomials of C_p are both $p(t)$ and all eigenspaces are one dimensional. In particular, C_p is diagonalizable if and only all the roots of $p(t)$ are distinct and lie in $\mathbb{F}$.*

PROOF. Even though we can prove these properties from our knowledge of the transpose of C_p it is still worthwhile to give a complete proof. Also recall that we computed the minimal polynomial in "The Minimal Polynomial" section above.

To compute the characteristic polynomial we consider:

$$t1_{\mathbb{F}^n} - C_p = \begin{bmatrix} t & 0 & \cdots & 0 & \alpha_0 \\ -1 & t & \cdots & 0 & \alpha_1 \\ 0 & -1 & \cdots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & t+\alpha_{n-1} \end{bmatrix}$$

By switching rows 1 and 2 we see that this is row equivalent to

$$\begin{bmatrix} -1 & t & \cdots & 0 & \alpha_1 \\ t & 0 & \cdots & 0 & \alpha_0 \\ 0 & -1 & \cdots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & t+\alpha_{n-1} \end{bmatrix}$$

eliminating t then gives us

$$\begin{bmatrix} -1 & t & \cdots & 0 & \alpha_1 \\ 0 & t^2 & \cdots & 0 & \alpha_0+\alpha_1 t \\ 0 & -1 & \cdots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & t+\alpha_{n-1} \end{bmatrix}.$$

Now switch rows 2 and 3 to get

$$\begin{bmatrix} -1 & t & \cdots & 0 & \alpha_1 \\ 0 & -1 & \cdots & 0 & \alpha_2 \\ 0 & t^2 & \cdots & 0 & \alpha_0+\alpha_1 t \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & t+\alpha_{n-1} \end{bmatrix}$$

and eliminate t^2

$$\begin{bmatrix} -1 & t & \cdots & 0 & \alpha_1 \\ 0 & -1 & \cdots & 0 & \alpha_2 \\ 0 & 0 & \cdots & 0 & \alpha_0+\alpha_1 t+\alpha_2 t^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & t+\alpha_{n-1} \end{bmatrix}.$$

Repeating this argument shows that $t1_{\mathbb{F}^n} - C_p$ is row equivalent to

$$\begin{bmatrix} -1 & t & \cdots & 0 & \alpha_1 \\ 0 & -1 & \cdots & 0 & \alpha_2 \\ 0 & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & & -1 & \alpha_{n-1} \\ 0 & 0 & \cdots & 0 & t^n+\alpha_{n-1}t^{n-1}+\cdots+\alpha_1 t+\alpha_0 \end{bmatrix}.$$

This implies that the characteristic polynomial is $p(t)$.

To see that all eigenspaces are one dimensional we note that, if λ is a root of $p(t)$, then we have just shown that $\lambda 1_{\mathbb{F}^n} - C_p$ is row equivalent to the matrix

$$\begin{bmatrix} -1 & \lambda & \cdots & 0 & \alpha_1 \\ 0 & -1 & \cdots & 0 & \alpha_2 \\ 0 & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & & -1 & \alpha_{n-1} \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Since all but the last diagonal entry is nonzero we see that the kernel must be one dimensional. □

Cyclic subspaces lead us to a very elegant proof of the Cayley-Hamilton theorem.

THEOREM 22. (The Cayley-Hamilton Theorem) *Let $L : V \to V$ be a linear operator on a finite dimensional vector space. Then L is a root of its own characteristic polynomial*

$$\chi_L(L) = 0.$$

In particular, the minimal polynomial divides the characteristic polynomial.

PROOF. Select any $x \neq 0$ in V and a complement M to the cyclic subspace C_x generated by x. This gives us a nontrivial decomposition $V = C_x \oplus M$, where L maps C_x to it self and M into V. If we select a basis for V that starts with the cyclic basis for C_x, then L will have a matrix representaion that looks like

$$[L] = \begin{bmatrix} C_p & B \\ 0 & D \end{bmatrix},$$

where C_p is the companion matrix representaion for L restricted to C_x. This shows that

$$\begin{aligned} \chi_L(t) &= \chi_{C_p}(t)\,\chi_D(t) \\ &= p(t)\,\chi_D(t). \end{aligned}$$

We know that $p(C_p) = 0$ from the previous result. This shows that $p(L|_{C_x}) = 0$ and in particular that $p(L)(x) = 0$. Thus

$$\begin{aligned} \chi_L(L)(x) &= \chi_D(L) \circ p(L)(x) \\ &= 0. \end{aligned}$$

Since x was arbitrary this shows that $\chi_L(L) = 0$. □

We now have quite a good understanding of the basic building blocks in the decomposition we are seeking.

THEOREM 23. (The Cyclic Subspace Decomposition) *Let $L : V \to V$ be a linear operator on a finite dimensional vector space. Then V has a cyclic subspace decomposition*

$$V = C_{x_1} \oplus \cdots \oplus C_{x_k}$$

where each C_x is a cyclic subspace. In particular, L has a block diagonal matrix representation where each block is a companion matrix

$$[L] = \begin{bmatrix} C_{p_1} & 0 & & 0 \\ 0 & C_{p_2} & & \\ & & \ddots & \\ 0 & & & C_{p_k} \end{bmatrix}$$

and $\chi_L(t) = p_1(t) \cdots p_k(t)$. Moreover the geometric multiplicity satisfies

$$\dim(\ker(L - \lambda 1_V)) = \text{ number of } p_i s \text{ such that } p_i(\lambda) = 0.$$

In particular, we see that L is diagonalizable if and only if all of the companion matrices C_p have distinct eigenvalues.

Proof. The proof uses induction on the dimension of the vector space. Thus the goal is to show that either $V = C_x$ for some $x \in V$ or that $V = C_x \oplus M$ for some L invariant subspace M. We assume that $\dim(V) = n$.

Let $m \leq n$ be the largest dimension of a cyclic subspace, i.e., $\dim C_x \leq m$ for all $x \in V$ and there is an $x_1 \in V$ such that $\dim C_{x_1} = m$. In other words $L^m(x) \in \operatorname{span}\{x, L(x), ..., L^{m-1}(x)\}$ for all $x \in V$ and we can find $x_1 \in V$ such that $x_1, L(x_1), ..., L^{m-1}(x_1)$ are linearly independent.

In case $m = n$, it follows that $C_{x_1} = V$ and we are finished. Otherwise we must show that there is an L invariant complement to $C_{x_1} = \operatorname{span}\{x_1, L(x_1), ..., L^{m-1}(x_1)\}$ in V. To construct this complement we consider the linear map $K : V \to \mathbb{F}^m$ defined by

$$K(x) = \begin{bmatrix} f(x) \\ f(L(x)) \\ \vdots \\ f(L^{m-1}(x)) \end{bmatrix},$$

where $f : V \to \mathbb{F}$ is a linear functional chosen so that

$$\begin{aligned} f(x_1) &= 0, \\ f(L(x_1)) &= 0, \\ &\vdots \\ f(L^{m-2}(x_1)) &= 0, \\ f(L^{m-1}(x_1)) &= 1. \end{aligned}$$

Note that it is possible to choose such an f as $x_1, L(x_1), ..., L^{m-1}(x_1)$ are linearly independent and hence part of a basis for V.

We now claim that $K|_{C_{x_1}} : C_{x_1} \to \mathbb{F}^m$ is an isomorphism. To see this we find the matrix representation for the restriction of K to C_{x_1}. Using the basis $x_1, L(x_1)$, ..., $L^{m-1}(x_1)$ for C_{x_1} and the canonical basis $e_1, ..., e_m$ for $\mathbb{F}^m$ we see that:

$$\begin{aligned} & \begin{bmatrix} K(x_1) & K(L(x_1)) & \cdots & K(L^{m-1}(x_1)) \end{bmatrix} \\ = & \begin{bmatrix} e_1 & e_2 & \cdots & e_m \end{bmatrix} \begin{bmatrix} 0 & 0 & & 1 \\ & & & * \\ 0 & 1 & & \\ 1 & * & & * \end{bmatrix} \end{aligned}$$

where $*$ indicates that we don't know or care what the entry is. Since the matrix representation is clearly invertible we have that $K|_{C_{x_1}} : C_{x_1} \to \mathbb{F}^m$ is an isomorphism.

Next we need to show that $\ker(K)$ is L invariant. Let $x \in \ker(K)$, i.e.,

$$K(x) = \begin{bmatrix} f(x) \\ f(L(x)) \\ \vdots \\ f\left(L^{m-1}(x)\right) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Then

$$K(L(x)) = \begin{bmatrix} f(L(x)) \\ f\left(L^2(x)\right) \\ \vdots \\ f\left(L^{m-1}(x)\right) \\ f(L^m(x)) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ f(L^m(x)) \end{bmatrix}.$$

Now use the assumption that $L^m(x)$ is a linear combination of $x, L(x), ..., L^{m-1}(x)$ for all x to conclude that also $f(L^m(x)) = 0$. Thus $L(x) \in \ker(K)$ as desired.

Finally we show that $V = C_{x_1} \oplus \ker(K)$. We have seen that $K|_{C_{x_1}} : C_{x_1} \to \mathbb{F}^m$ is an isomorphism. This implies that $C_{x_1} \cap \ker(K) = \{0\}$. From the dimension formula we then get that

$$\begin{aligned} \dim(V) &= \dim(\ker(K)) + \dim(\operatorname{im}(K)) \\ &= \dim(\ker(K)) + m \\ &= \dim(\ker(K)) + \dim(C_{x_1}) \\ &= \dim(\ker(K) + C_{x_1}). \end{aligned}$$

Thus $V = C_{x_1} + \ker(K) = C_{x_1} \oplus \ker(K)$.

To find the geometric multiplicity of λ, we need only observe that each of the blocks C_{p_i} has a one dimensional eigenspace corresponding to λ if λ is an eigenvalue for C_{p_i}. We know in turn that λ is an eigenvalue for C_{p_i} precisely when $p_i(\lambda) = 0$. □

It is important to understand that there can be several cyclic subspace decompositions. This fact, of course, makes our calculation of the geometric multiplicity of eigenvalues especially intriguing. A rather interesting example comes from companion matrices themselves. Clearly they have the desired decomposition, however, if they are diagonalizable then the space also has a different decomposition into cyclic subspaces given by the one dimensional eigenspaces. The issue of obtaining a unique decomposition is discussed in the next section and turns out to fall right out of our proof.

To see that this theorem really has something to say we should give examples of linear maps that force the space to have a nontrivial cyclic subspace decomposition. Since a companion matrix always has one dimensional eigenspaces this is of course not hard at all. A very natural choice is the linear operator $L_A(X) = AX$ on $\mathrm{Mat}_{n\times n}(\mathbb{C})$. In "Linear Maps as Matrices" in chapter 1 we showed that it had a block diagonal form with As on the diagonal. This shows that any eigenvalue for A has geometric multiplicity at least n. We can also see this more directly. Assume that $Ax = \lambda x$, where $x \in \mathbb{C}^n$ and consider $X = \begin{bmatrix} \alpha_1 x & \cdots & \alpha_n x \end{bmatrix}$. Then

$$\begin{aligned} L_A(X) &= A \begin{bmatrix} \alpha_1 x & \cdots & \alpha_n x \end{bmatrix} \\ &= \begin{bmatrix} \alpha_1 Ax & \cdots & \alpha_n Ax \end{bmatrix} \\ &= \lambda \begin{bmatrix} \alpha_1 x & \cdots & \alpha_n x \end{bmatrix} \\ &= \lambda X. \end{aligned}$$

Thus

$$M = \left\{ \begin{bmatrix} \alpha_1 x & \cdots & \alpha_n x \end{bmatrix} : \alpha_1, ..., \alpha_n \in \mathbb{C} \right\}$$

forms an n dimensional space of eigenvectors for L_A.

Another interesting example of a cyclic subspace decomposition comes from permutation matrices. We first recall that a permutation matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ is a matrix such that $Ae_i = e_{\sigma(i)}$, see also "Linear Maps as Matrices" in chapter 1. We claim that we can find a cyclic subspace decomposition by simply rearranging the canonical basis $e_1, ..., e_n$ for $\mathbb{F}^n$. The proof works by induction on n. When $n = 1$ there is nothing to prove. For $n > 1$, we consider $C_{e_1} = \mathrm{span}\left\{e_1, Ae_1, A^2e_1, ...\right\}$. Since all of the powers $A^m e_1$ all belong to the finite set $\{e_1, ..., e_n\}$, we can find integers $k > l > 0$ such that $A^k e_1 = A^l e_1$. Since A is invertible this implies that $A^{k-l}e_1 = e_1$. Now select the smallest integer $m > 0$ such that $A^m e_1 = e_1$. Then we have

$$C_{e_1} = \mathrm{span}\left\{e_1, Ae_1, A^2e_1, ..., A^{m-1}e_1\right\}.$$

Moreover, all of the vectors e_1, Ae_1, A^2e_1, ..., $A^{m-1}e_1$ must be distinct as we could otherwise find $l < k < m$ such that $A^{k-l}e_1 = e_1$. This contradicts minimality of m. Since all of e_1, Ae_1, A^2e_1, ..., $A^{m-1}e_1$ are also vectors from the basis $e_1, ..., e_n$, they must form a basis for C_{e_1}. In this basis A is represented by the companion matrix to $p(t) = t^m - 1$ and hence takes the form

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}.$$

The permutation that corresponds to $A : C_{e_1} \to C_{e_1}$ is also called a *cyclic permutation*. Evidently it maps the elements 1, $\sigma(1)$, ..., $\sigma^{m-1}(1)$ to themselves in a cyclic manner. One often refers to such permutations by listing the elements as $\left(1, \sigma(1), ..., \sigma^{m-1}(1)\right)$. This is not quite a unique representation as, e.g., $\left(\sigma^{m-1}(1), 1, \sigma(1), ..., \sigma^{m-2}(1)\right)$ clearly describes the same permutation.

We used m of the basis vectors $e_1, ..., e_n$ to span C_{e_1}. Rename and reindex the complementary basis vectors $f_1, ..., f_{n-m}$. To get our induction to work we need to show that $Af_i = f_{\tau(i)}$ for each $i = 1, ..., n-m$. We know that $Af_i \in \left\{e_1, ..., e_n\right\}$. If $Af_i \in \left\{e_1, Ae_1, A^2e_1, ..., A^{m-1}e_1\right\}$, then either $f_i = e_1$ or $f_i = A^k e_1$. The former is impossible since $f_i \notin \left\{e_1, Ae_1, A^2e_1, ..., A^{m-1}e_1\right\}$. The latter is impossible as A leaves $\left\{e_1, Ae_1, A^2e_1, ..., A^{m-1}e_1\right\}$ invariant. Thus it follows that $Af_i \in \{f_1, ..., f_{n-m}\}$ as desired. In this way we see that it is possible to rearrange the basis $e_1, .., e_n$ so as to get a cyclic subspace decomposition. Furthermore, on each cyclic subspace A is represented by a companion matrix corresponding to $p(t) = t^k - 1$ for some $k \leq n$. Recall that if $\mathbb{F} = \mathbb{C}$, then each of these companion matrices are diagonalizable, in particular, A is itself diagonalizable.

Note that the cyclic subspace decomposition for a permutation matrix also decomposes the permutation σ into cyclic permutations that are disjoint. This is a basic construction in the theory of permutations.

The cyclic subspace decomposition qualifies as a central result in linear algebra for many reasons. While somewhat difficult and tricky to prove it doesn't depend on quite a lot of our developments in this chapter. It could in fact be established without knowledge of eigenvalues, charateristic polynomials and minimal polynomials ect. Second, it gives a matrix representation which is in block diagonal form and where we have a very good understanding of each of the blocks. Therefore, all of our developements in this chapter could be considered consequences of this decomposition. Finally, several important and difficult results such as the Frobenius and Jordan canonical forms become relatively easy to prove using this decomposition.

6.1. Exercises.

(1) Find all invariant subspaces for the following two matrices and show that they are not diagonalizable.
   (a) $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$
   (b) $\begin{bmatrix} \alpha & 1 \\ 0 & \alpha \end{bmatrix}$

(2) We say that a linear map $L : V \to V$ is *reduced* by a direct sum decomposition $V = M \oplus N$ if both M and N are invariant under L. We also say that $L : V \to V$ is *decomposable* if we can find a nontrivial decomposition that reduces $L : V \to V$.
   (a) Show that for $L = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ with $M = \ker(L) = \operatorname{im}(L)$ it is not possible to find N such that $V = M \oplus N$ reduces L.
   (b) Show more generally that one cannot find a nontrivial decomposition that reduces L.

(3) Let $L : V \to V$ be a linear transformation and $M \subset V$ a subspace. Show
   (a) If E is a projection onto M and $ELE = LE$ then M is invariant under L.
   (b) If M is invariant under L then $ELE = LE$ for all projections onto M.
   (c) If $V = M \oplus N$ and E is the projection onto M along N, then $M \oplus N$ reduces L if and only if $EL = LE$.

(4) Assume $V = M \oplus N$.
   (a) Show that any linear map $L : V \to V$ has a 2×2 matrix type decomposition

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

   where $A : M \to M, B : M \to N, C : N \to M, D : N \to N$.
   (b) Show that the projection onto M along N looks like

$$E = 1_M \oplus 0_N = \begin{bmatrix} 1_M & 0 \\ 0 & 0_N \end{bmatrix}$$

   (c) Show that if $L(M) \subset M$, then $C = 0$.

(d) Show that if $L(M) \subset M$ and $L(N) \subset N$ then $B = 0$ and $C = 0$. In this case L is reduced by $M \oplus N$, and we write

$$\begin{aligned} L &= A \oplus D \\ &= L|_M \oplus L|_N. \end{aligned}$$

(5) Show that the space of $n \times n$ companion matrices form an affine subspace isomorphic to the space of monic polynomials of degree n. Affine subspaces are defined in the exercises to "Subspaces" in chapter 1.

(6) Given

$$A = \begin{bmatrix} \lambda_1 & 1 & & 0 \\ 0 & \lambda_2 & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_n \end{bmatrix}$$

find $x \in \mathbb{F}^n$ such that $C_x = \mathbb{F}^n$. Hint: try $n = 2, 3$ first.

(7) Given a linear operator $L : V \to V$ on a finite dimensional vector space and $x \in V$ show that

$$C_x = \{p(L)(x) : p(t) \in \mathbb{F}[t]\}.$$

(8) Let $p(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathbb{F}[t]$. Show that C_p and C_p^t are similar. Hint: Let

$$B = \begin{bmatrix} a_1 & a_2 & & a_{n-1} & 1 \\ a_2 & & & 1 & 0 \\ & & a_{n-1} & 0 & 0 \\ a_{n-1} & 1 & & & \\ 1 & 0 & & 0 & 0 \end{bmatrix}$$

and show

$$C_p B = B C_p^t.$$

(9) Use the previous exercise to show that $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ and its transpose are similar.

(10) If $V = C_x$ for some $x \in V$, then $\deg(\mu_L) = \dim(V)$.

(11) For each $n \geq 2$ construct a matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ such that $V \neq C_x$ for every $x \in V$.

(12) For each $n \geq 2$ construct a matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ such that $V = C_x$ for some $x \in V$.

(13) Let $L : V \to V$ be a diagonalizable linear operator. Show that $V = C_x$ if and only if there are no multiple eigenvalues.

(14) Assume that $V \neq C_{x_1}$, where C_{x_1} is the first cyclic subspace as constructed in the proof of the cyclic subspace decomposition. Show that it is possible to select another $y_1 \in V$ such that $\dim C_{y_1} = \dim C_{x_1} = m$, but $C_{x_1} \neq C_{y_1}$. This gives a different indication of why the cyclic subspace decomposition isn't unique.

(15) Assume that $V = C_x$ for some $x \in V$ and $L : V \to V$.

(a) Show that $K \circ L = L \circ K$ if and only if $K = p(L)$ for some $p \in \mathbb{F}[t]$.

(b) Show that all invariant subspaces for L are of the form $\ker(p(L))$ for some polynomial $p \in \mathbb{F}[t]$.

(c) Show that all invariant subspaces for L are of the form C_z for some $z \in V$.

(16) Define $\mathbb{F}[L] = \{p(L) : p(t) \in \mathbb{F}[t]\} \subset \hom(V,V)$ as the space of polynomials in L.
   (a) Show that $\mathbb{F}[L]$ is a subspace, that is also closed under composition of operators.
   (b) Show that $\dim(\mathbb{F}[L]) = \deg(\mu_L)$ and $\mathbb{F}[L] = \operatorname{span}\{1_V, L, ..., L^{k-1}\}$, where $k = \deg(\mu_L)$.
   (c) Show that the map $\Phi : \mathbb{F}[t] \to \hom(V,V)$ defined by $\Phi(p(t)) = p(L)$ is linear and a ring homomorphism (preserves multiplication and sends $1 \in \mathbb{F}[t]$ to $1_V \in \hom(V,V)$) with image $\mathbb{F}[L]$.
   (d) Show that $\ker(\Phi) = \{p(t)\mu_L(t) : p(t) \in \mathbb{F}[t]\}$.
   (e) Show that for any $p(t) \in \mathbb{F}[t]$ we have $q(L) = r(L)$ for some $r(t) \in \mathbb{F}[t]$ with $\deg r(t) < \deg \mu_L(t)$.
   (f) Given an eigenvector $x \in V$ for L show that x is an eigenvector for all $K \in \mathbb{F}[L]$ and that the map $\mathbb{F}[L] \to \mathbb{F}$ that sends K to the eigenvalue corresponding to x is a ring homomorphism.
   (g) Conversely show that any ring homomorphism $\phi : \mathbb{F}[L] \to \mathbb{F}$ is of the type described in f.

7. The Frobenius Canonical Form

As we already indicated, the above proof of the cyclic subspace decomposition actually proves quite a bit more than the result claims as it can actually lead us to a unique matrix representation for the operator. The Frobenius canonical form will be used in the next section to establish more refinesh canonical forms for complex operators.

THEOREM 24. (The Frobenius Canonical Form) *Let $L : V \to V$ be a linear operator on a finite dimensional vector space. Then V has a cyclic subspace decomposition such that the block diagonal form of L*

$$[L] = \begin{bmatrix} C_{p_1} & 0 & & 0 \\ 0 & C_{p_2} & & \\ & & \ddots & \\ 0 & & & C_{p_k} \end{bmatrix}$$

has the property that p_i divides p_{i-1} for each $i = 2, ..., k$. Moreover, the monic polynomials $p_1, ..., p_k$ are unique.

PROOF. We first establish that the polynomials constructed in the above version of the cyclic subspace decomposition have the desired divisibility properties.

Recall that $m \leq n$ is the largest dimension of a cyclic subspace, i.e., $\dim C_x \leq m$ for all $x \in V$ and there is an $x_1 \in V$ such that $\dim C_{x_1} = m$. In other words $L^m(x) \in \operatorname{span}\{x, L(x), ..., L^{m-1}(x)\}$ for all $x \in V$ and we can find $x_1 \in V$ such that x_1, $L(x_1)$, ..., $L^{m-1}(x_1)$ are linearly independent. With this choice of x_1 we also found an L-invariant complementary subspace M and we define

$$\begin{aligned} p_1(t) &= t^m - \alpha_{m-1}t^{m-1} - \cdots - \alpha_0, \text{ where} \\ L^m(x_1) &= \alpha_{m-1}L^{m-1}(x_1) + \cdots + \alpha_0 x_1. \end{aligned}$$

With these choices we claim that $p_1(L)(z) = 0$ for all $z \in V$. In other words, we are showing that $p_1(t) = \mu_L(t)$. Note that we already know this for $z = x_1$, and it is easy to also verify it for $z = L(x_1)$, ..., $L^{m-1}(x_1)$ by using that $p(L) \circ L^k =$

$L^k \circ p(L)$. Thus we only need to check the claim for $z \in M$. By construction of m we know that

$$L^m(x_1 + z) = \gamma_{m-1} L^{m-1}(x_1 + z) + \cdots + \gamma_0 (x_1 + z).$$

Now we rearrage the terms as follows

$$\begin{aligned} L^m(x_1) + L^m(z) &= L^m(x_1 + z) \\ &= \gamma_{m-1} L^{m-1}(x_1) + \cdots + \gamma_0 x_1 \\ &\quad + \gamma_{m-1} L^{m-1}(z) + \cdots + \gamma_0 z \end{aligned}$$

Since

$$L^m(x_1), \gamma_{m-1} L^{m-1}(x_1) + \cdots + \gamma_0 x_1 \in C_{x_1}$$

and

$$L^m(z), \gamma_{m-1} L^{m-1}(z) + \cdots + \gamma_0 z \in M$$

we must have that

$$\gamma_{m-1} L^{m-1}(x_1) + \cdots + \gamma_0 x_1 = L^m(x_1) = \alpha_{m-1} L^{m-1}(x_1) + \cdots + \alpha_0 x_1.$$

Since x_1, $L(x_1)$, ..., $L^{m-1}(x_1)$ are linearly independent this shows that $\gamma_i = \alpha_i$ for $i = 0, ..., m-1$. But then we have that

$$\begin{aligned} 0 &= p_1(L)(x_1 + z) \\ &= p_1(L)(x_1) + p_1(L)(z) \\ &= p_1(L)(z), \end{aligned}$$

which is what we wanted to prove.

Now $x_2 \in M$ and $p_2(t)$ are choosen in the same fashion as x_1 and p_1. We first note that $l = \deg p_2 \leq \deg p_1 = m$, this means that we can write $p_1 = q_1 p_2 + r$, where $\deg r < \deg p_2$. Thus

$$\begin{aligned} 0 &= p_1(L)(x_2) \\ &= q_1(L) \circ p_2(L)(x_2) + r(L)(x_2) \\ &= r(L)(x_2). \end{aligned}$$

Since $\deg r < l = \deg p_2$, the equation $r(L)(x_2) = 0$ takes the form

$$\begin{aligned} 0 &= r(L)(x_2) \\ &= \beta_0 x_2 + \cdots + \beta_{k-1} L^{l-1}(x_2). \end{aligned}$$

However, p_2 was choosen to that x_2, $L(x_1)$, ..., $L^{l-1}(x_2)$ are linearly independent, so

$$\beta_0 = \cdots = \beta_{l-1} = 0$$

and hence also $r = 0$. This shows that p_2 divides p_1.

We now show that p_1 and p_2 are unique, this, despite the fact that x_1 and x_2 need not be unique. To see that p_1 is unique we simply check that it is the minimal polynomial of L. We have already seen that $p_1(L)(z) = 0$ for all $z \in V$. Thus $p_1(L) = 0$ showing that $\deg \mu_L \leq \deg p_1$. On the other hand we also know that x_1, $L(x_1)$, ..., $L^{m-1}(x_1)$ are linearly independent, in particular 1_V, L, ..., L^{m-1} must also be linearly independent. This shows that $\deg \mu_L \geq m = \deg p_1$. Hence $\mu_L = p_1$ as they are both monic.

To see that p_2 is unique is a bit more tricky since the choice for C_{x_1} is not unique. We select two decompositions

$$C_{x_1'} \oplus M' = V = C_{x_1} \oplus M.$$

This yields two block diagonal matrix decompositions for L

$$\begin{bmatrix} C_{p_1} & 0 \\ 0 & [L|_{M'}] \end{bmatrix}$$
$$\begin{bmatrix} C_{p_1} & 0 \\ 0 & [L|_{M}] \end{bmatrix}$$

where the upper left hand block is the same for both representations as p_1 is unique. Moreover, these two matrices are similar. Therefore we only need to show that $\mu_{A_{22}} = \mu_{A'_{22}}$ if the two block diagonal matrices

$$\begin{bmatrix} A_{11} & 0 \\ 0 & A_{22} \end{bmatrix} \text{ and } \begin{bmatrix} A_{11} & 0 \\ 0 & A'_{22} \end{bmatrix}$$

are similar

$$\begin{bmatrix} A_{11} & 0 \\ 0 & A_{22} \end{bmatrix} = B^{-1} \begin{bmatrix} A_{11} & 0 \\ 0 & A'_{22} \end{bmatrix} B.$$

If p is any polynomial, then

$$\begin{aligned} \begin{bmatrix} p(A_{11}) & 0 \\ 0 & p(A_{22}) \end{bmatrix} &= p\left(\begin{bmatrix} A_{11} & 0 \\ 0 & A_{22} \end{bmatrix}\right) \\ &= p\left(B^{-1} \begin{bmatrix} A_{11} & 0 \\ 0 & A'_{22} \end{bmatrix} B\right) \\ &= B^{-1}\left(p\left(\begin{bmatrix} A_{11} & 0 \\ 0 & A'_{22} \end{bmatrix}\right)\right) B \\ &= B^{-1} \begin{bmatrix} p(A_{11}) & 0 \\ 0 & p(A'_{22}) \end{bmatrix} B. \end{aligned}$$

In particular, the two matrices

$$\begin{bmatrix} p(A_{11}) & 0 \\ 0 & p(A_{22}) \end{bmatrix} \text{ and } \begin{bmatrix} p(A_{11}) & 0 \\ 0 & p(A'_{22}) \end{bmatrix}$$

always have the same rank. Since the upper left hand corners are identical this shows that $p(A_{22})$ and $p(A'_{22})$ have the same rank. As a special case we see that $p(A_{22}) = 0$ if and only if $p(A'_{22}) = 0$. This shows that A_{22} and A'_{22} have the same minimal polynomials and hence that p_2 is uniquely defined. □

In some texts this is also known as the *rational canonical form*. The reason is that it will have rational entries if we start with an $n \times n$ matrix with rational entries. To see why this is, simply observe that the similarity invaraints have to be rational polynomials starting with p_1, the minimal polynomial. There can, however, be several rational canonical forms. Another comes from further factoring the characteristic or minimal polynomials and will have more blocks. The advantage of the Frobenius canonical from is that it does not depend on the scalar field. That is, if $A \in \mathrm{Mat}_{n\times n}(\mathbb{F}) \subset \mathrm{Mat}_{n\times n}(\mathbb{L})$ then the form doesn't depend on whether we compute it using $\mathbb{F}$ or $\mathbb{L}$.

The unique polynomials $p_1, ..., p_k$ are called the *similarity invariants, elementary divisors,* or *invariant factors* for L. Clearly two matrices are similar if they have the same similarity invariants as they have the same Frobenious canonical form. Conversely similar matrices are both similar to just one Frobenius canonical form and hence have the same similarity invariants. It is possible to calculate the similarity invariants using only the elementary row and column operations. The specific algorithm leads to the Smith Normal Form (see [**Hoffman-Kunze**] and [**Serre**].) The treatment here doesn't give us a good way of calculating the similarity invariants.

The following corollary shows that several of the matrices realted to companion matrices are in fact similar. Various exrcises have been devoted to establishing this fact, but using the Frobenius canonical form we get a very elegant characterization of when a linear map is similar to a companion matrix.

Corollary 17. *If two linear operators on an n-dimensional vector space have the same minimal polynomials of degree n, then they have the same Frobenius canonical form and are similar.*

Given that the similarity invariants are uniquely defined we can now define the characteristic polynomial as

$$\chi_L(t) = p_1(t) \cdots p_k(t).$$

This gives us a way of defining the characteristic polynomial, but it doesn't tells us how to compute it. For that the row reduction technique or determinants are the way to go. To be even more asinine we can now define the determinant as

$$\det L = (-1)^n \chi_L(0).$$

The problem is that one of the key properties of determinants

$$\det(K \circ L) = \det(K)\det(L)$$

does not follow easily from this definition. We do, however, get that similar matrices and linear operators have the same determinant

$$\det\left(K \circ L \circ K^{-1}\right) = \det(L).$$

As a general sort of example let us see what the Frobenius canonical form for

$$A = \begin{bmatrix} C_{q_1} & 0 \\ 0 & C_{q_2} \end{bmatrix}$$

is, when q_1 and q_2 are relatively prime. Note that if

$$0 = p(A) = \begin{bmatrix} p(C_{q_1}) & 0 \\ 0 & p(C_{q_2}) \end{bmatrix},$$

then both q_1 and q_2 divide p. Conversely if q_1 and q_2 both divide p it also follows that $p(A) = 0$. Since the least common multiple of q_1 and q_2 is $q_1 \cdot q_2$ we see that $\mu_A = q_1 \cdot q_2 = \chi_A$. Thus $p_1 = q_1 \cdot q_2$ and $p_2 = 1$. This shows that the Frobenius canonical form is simply $C_{q_1 \cdot q_2}$. The general case where there might be a nontrivial greatest common divisor is relegated to the exercises.

We now give a few examples showing that the characteristic and minimal polynomials alone are not sufficient information to determine all the similarity invariants when the dimension is ≥ 4 (see exercises for dimensions 2 and 3). We consider all canonical forms in dimension 4, where the characteristic polynomial is t^4. There are four nontrivial cases given by:

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

For the first we know that $\mu = p_1 = t^4$. For the second we have two blocks with $\mu = p_1 = t^3$ so $p_2 = t$. For the third we have $\mu = p_1 = t^2$ while $p_2 = p_3 = t$. Finally the fourth has $\mu = p_1 = p_2 = t^2$. The last two matrices clearly don't have the same canonical form, but they do have the same characteristic and minimal polynomials.

Lastly let us compute the Frobenius Canonical form for a projection $E : V \to V$. As we shall see this is clearly a situation where we should just stick to diagonalization as the Frobenius canonical form is far less informative. Apparently we just need to find all possible Frobenius canonical forms that are also projections. The simplest are of course just 0_V and 1_V. In all other cases the minimal polynomial is $t^2 - t$. The companion matrix for that polynomial is

$$\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

so we expect to have one or several of those blocks, but note that we can't have more than $\left\lfloor \frac{\dim V}{2} \right\rfloor$ of such blocks. The rest of the diagonal entries must now correspond to companion matrices for either t or $t - 1$. But we can't use both as these two polynomials don't divide each other. This gives us two types of Frobenius canonical forms

$$\begin{bmatrix} 0 & 0 & & & & & & \\ 1 & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 0 & & & \\ & & & 1 & 1 & & & \\ & & & & & 0 & & \\ & & & & & & \ddots & \\ & & & & & & & 0 \end{bmatrix}$$

or

$$\begin{bmatrix} 0 & 0 & & & & & & \\ 1 & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 0 & & & \\ & & & 1 & 1 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{bmatrix}$$

To find the correct canonical form for E we just select the Frobenius canonical form that gives us the correct rank. If $\operatorname{rank} E \leq \left\lfloor \frac{\dim V}{2} \right\rfloor$ it'll be of the first type and otherwise of the second.

7.1. Exercises.

(1) What are the similarity invariants for a companion matrix C_p?

(2) Let $A \in \text{Mat}_{n\times n}(\mathbb{R})$, and $n \geq 2$.
   (a) Show that when n is odd, then it is not possible to have $p_1(t) = t^2+1$.
   (b) Show by example that one can have $p_1(t) = t^2+1$ for all even n.
   (c) Show by example that one can have $p_1(t) = t^3+t$ for all odd n.

(3) If $L : V \to V$ is an operator on a 2-dimensional space, then either $p_1 = \mu_L = \chi_L$ (and $p_2 = 1$) or $L = \lambda 1_V$.

(4) If $L : V \to V$ is an operator on a 3-dimensional space, then either $p_1 = \mu_L = \chi_L$ (and $p_2 = 1$), $p_1 = (t-\alpha)(t-\beta)$ and $p_2 = (t-\beta)$, or $L = \lambda 1_V$. Note that in the second case you know that p_1 has degree 2, the key is to show that it factors as described.

(5) Let $L : V \to V$ be a linear operator a finite dimensional space. Show that $V = C_x$ for some $x \in V$ if and only if $\mu_L = \chi_L$.

(6) Consider two companion matrices C_p and C_q, show that the similarity invariants for the block diagonal matrix

$$\begin{bmatrix} C_p & 0 \\ 0 & C_q \end{bmatrix}$$

are $p_1 = \text{lcm}\{p,q\}$ and $p_2 = \gcd\{p,q\}$.

(7) Is it possible to find the similarity invariants for

$$\begin{bmatrix} C_p & 0 & 0 \\ 0 & C_q & 0 \\ 0 & 0 & C_r \end{bmatrix}?$$

Note that you can easily find $p_1 = \text{lcm}\{p,q,r\}$, so the issue is whether it is possible to decide what p_2 should be?

(8) Show that $A, B \in \text{Mat}_{n\times n}(\mathbb{F})$ are similar if and only if $\text{rank}(p(A)) = \text{rank}(p(B))$ for all $p \in \mathbb{F}[t]$. (Recall that two matrices have the same rank if and only if they are equivalent and that equivalent matrices certainly need not be similar. This is what makes the exercise interesting.)

(9) The previous exercise can be made into a checkable condition: Show that $A, B \in \text{Mat}_{n\times n}(\mathbb{F})$ are similar if and only if $\chi_A = \chi_B$ and $\text{rank}(p(A)) = \text{rank}(p(B))$ for all p that divide χ_A. (Using that as χ_A has a unique prime factorization this means that we only have to check a finite number of conditions.)

(10) Show that any linear map with the property that $\chi_L(t) = (t-\lambda_1)\cdots(t-\lambda_n) \in \mathbb{F}[t]$ for $\lambda_1, ..., \lambda_n \in \mathbb{F}$ has an upper triangular matrix representation. Hint: This was established for some matrices in an exercise from "Eigenvalues".

(11) Let $L : V \to V$ be a linear operator on a finite dimensional vector space. Use the Frobenius canonical from to show that $\text{tr}(L) = -a_{n-1}$, where $\chi_L(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$. This is the result mentioned in "Eigenvalues".

(12) Assume that $L : V \to V$ satisfies $(L - \lambda_0 1_V)^k = 0$, for some $k > 1$, but $(L-\lambda_0 1_V)^{k-1} \neq 0$. Show that $\ker(L-\lambda_0 1_V)$ is neither $\{0\}$ nor V. Show that $\ker(L-\lambda_0 1_V)$ does not have a complement in V that is L invariant.

(13) *(The Cayley-Hamilton Theorem)* Show the Hamilton-Cayley Theorem using the Frobenius canonical form.

8. The Jordan Canonical Form

In this section we freely use the Frobenius Canonical form to present a proof the Jordan canonical form. We start with a somewhat more general view point, that in the end is probably the most important feature of this special canonical form. It reuires the use of the last exercise in "Diagonalizability".

THEOREM 25. (The Jordan-Chevalley decomposition) *Let $L : V \to V$ be a linear operator on an n-dimensional complex vector space. Then $L = S + N$, where S is diagonalizable, $N^n = 0$, and $SN = NS$.*

PROOF. First we use the Fundamental theorem of algebra to decompose the minimal polynomial

$$m_L(t) = (t - \lambda_1)^{m_1} \cdots (t - \lambda_k)^{m_k}$$

The last exercise in "Diagonalizability" then gives us a corresponding L invariant decomposition of the vector space

$$V = \ker (L - \lambda_1 1_V)^{m_1} \oplus \cdots \oplus \ker (L - \lambda_k 1_V)^{m_k}$$

This means that we have reduced the problem to a situation where L has only one eigenvalue. Given the Frobenius canonical form the problem is then further reduced to proinge the statement for companion matrices, where the minimal polynomial has only one root.. Let C_p be a companion matrix with

$$p(t) = (t - \lambda)^n.$$

Then construct the matrix

$$\begin{aligned} A &= D + N \\ &= \begin{bmatrix} \lambda & 0 & \cdots & 0 \\ 0 & \lambda & & \\ \vdots & & \ddots & \\ 0 & & & \lambda \end{bmatrix} + \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \\ \vdots & & \ddots & 1 \\ 0 & & & 0 \end{bmatrix} \\ &= \begin{bmatrix} \lambda & 1 & \cdots & 0 \\ 0 & \lambda & \ddots & \\ \vdots & & \ddots & 1 \\ 0 & & & \lambda \end{bmatrix}. \end{aligned}$$

We know from "The Minimal Polynomial" that $\mu_A = \mu_{C_p} = p(t)$. Since the degree of the minimal polynomial is maximal we see that the Frobenius canonical from for A is C_p, showing that C_p is similar to A. Then it only remains to observe that D is diagonal, $N^n = 0$, and $DN = ND$ to establish the Jordan-Chevalley decomposition for C_p. □

It is in fact possible to show that the Jordan-Chevalley decomposition is unique. This hinges on showing that S and N are polynomials in L, i.e., $S = p(L)$ and $N = q(L)$, where p and q are polynomials that depend on L. We won't show this here, but knowing this makes it quite simple to establish uniqueness (see exercises).

As a corollary we obtain

LEMMA 17. *Let C_p be a companion matrix with $p(t) = (t-\lambda)^n$. Then C_p is similar to a* Jordan block

$$[L] = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 1 & 0 \\ \vdots & \vdots & \vdots & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{bmatrix}.$$

Moreover the eigenspace for λ is 1-dimensional and is generated by the first basis vector.

Note that in a Jordan block all of the diagonal entries are the same. This was not necessarily the case for the matrices in the Jordan-Chevalley decomposition.

We can now give a simple proof of the Jordan canonical form. Weierstrass evidently also proved this theorem at about the same time and so also deserves to get credit.

THEOREM 26. (The Jordan-Weierstrass Canonical form) *Let $L : V \to V$ be a complex linear operator on a finite dimensional vector space. Then we can find L-invariant subspaces $M_1, ..., M_s$ such that*

$$V = M_1 \oplus \cdots \oplus M_s$$

and each $L|_{M_i}$ has a matrix representation of the form

$$\begin{bmatrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 \\ 0 & 0 & \lambda_i & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & \cdots & \lambda_i \end{bmatrix}$$

where λ_i is an eigenvalue for L.

PROOF. First we use the Jordan-Chevalley decomposition $L = S + N$ to decompose the vector space into eigenspaces for S

$$V = \ker(S - \lambda_1 1_V) \oplus \cdots \oplus \ker(S - \lambda_k 1_V).$$

Each of these eigenspaces is invariant for N since S and N commute. Specifically if $S(x) = \lambda x$, then

$$S(N(x)) = N(S(x)) = N(\lambda x) = \lambda N(x),$$

showing that $N(x)$ is also an eigenvector for the eigenvalue λ.

This reduces the problem to showing that operators of the form $\lambda 1_W + N$, where $N^n = 0$ have the desired decomposition. Since the homothety $\lambda 1_W$ is always diagonal in any basis, we are further reduced to showing the theorem holds for operators N such that $N^n = 0$. The similarity invariants for such an operator all have to look like t^k so the blocks in the Frobenius canonical form must look like

$$\begin{bmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \ddots & \\ \vdots & \ddots & \ddots & 0 \\ 0 & & 1 & 0 \end{bmatrix}.$$

If $e_1, ..., e_k$ is the basis yielding this matrix representation then

$$\begin{aligned} N \begin{bmatrix} e_1 & \cdots & e_k \end{bmatrix} &= \begin{bmatrix} e_2 & \cdots & e_k & 0 \end{bmatrix} \\ &= \begin{bmatrix} e_1 & \cdots & e_k \end{bmatrix} \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \ddots & \\ \vdots & \ddots & \ddots & 0 \\ 0 & & 1 & 0 \end{bmatrix}. \end{aligned}$$

Reversing the basis to $e_k, ..., e_1$ then gives us the desired block

$$\begin{aligned} N \begin{bmatrix} e_k & \cdots & e_1 \end{bmatrix} &= \begin{bmatrix} 0 & e_k & \cdots & e_2 \end{bmatrix} \\ &= \begin{bmatrix} e_k & \cdots & e_1 \end{bmatrix} \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \\ \vdots & & \ddots & 1 \\ 0 & & & 0 \end{bmatrix}. \end{aligned}$$

□

In this decomposition it is possible for several of the subspaces M_i to correspond to the same eigenvalue. Given that the eigenspace for each Jordan block is one dimensional we see that each eigenvalue corresponds to as many blocks as the geometric multiplicity of the eigenvalue. It is only when L is similar to a companion matrix that the blocks must correspond to distinct eigenvalues. The job of calculating the Jordan canonical form is in general quite hard. Here we confine ourselves to the 2 and 3 dimensional situations.

COROLLARY 18. *Let $L : V \to V$ be a complex linear operator where* $\dim(V) = 2$. *Either L is diagonalizable and there is a basis where*

$$[L] = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix},$$

or L is not diagonalizable and there is a basis where

$$[L] = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}.$$

Note that in case L is diagonalizable we either have that $L = \lambda 1_V$ or that the eigenvalues are distinct. In the nondiagonalizable case there is only one eigenvalue.

COROLLARY 19. *Let $L : V \to V$ be a complex linear operator where* $\dim(V) = 3$. *Either L is diagonalizable and there is a basis where*

$$[L] = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix},$$

or L is not diagonalizable and there is a basis where one of the following two situations occur

$$[L] = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 1 \\ 0 & 0 & \lambda_2 \end{bmatrix},$$

or

$$[L] = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}.$$

It is possible to check which of these situations occur by knowing the minimal and characteristic polynomials. We note that the last case happens precisely when there is only one eigenvalue with geometric multiplicity 1. The second case happens if either L has two eigenvalues each with geometric multiplicity 1 or if L has one eigenvalue with geometric multiplicity 2.

8.1. Exercises.

(1) Find the Jordan canonical forms for the matrices

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & -1 \\ 4 & -2 \end{bmatrix}$$

(2) Find the basis that yields the Jordan canonical form for

$$\begin{bmatrix} \lambda & -1 \\ \lambda^2 & -\lambda \end{bmatrix}.$$

(3) Find the Jordan canonical form for the matrix

$$\begin{bmatrix} \lambda_1 & 1 \\ 0 & \lambda_2 \end{bmatrix}.$$

Hint: the answer depends on the relationship between λ_1 and λ_2.

(4) Find the Jordan canonical forms for the matrix

$$\begin{bmatrix} 0 & 1 \\ -\lambda_1\lambda_2 & \lambda_1 + \lambda_2 \end{bmatrix}.$$

(5) Find the Jordan canonical forms for the matrix

$$\begin{bmatrix} \lambda^2 & -2\lambda & 1 \\ \lambda^3 & -2\lambda^2 & \lambda \\ \lambda^4 & -2\lambda^3 & \lambda^2 \end{bmatrix}$$

(6) Find the Jordan canonical forms for the matrix

$$\begin{bmatrix} \lambda_1 & 1 & 0 \\ 0 & \lambda_2 & 1 \\ 0 & 0 & \lambda_3 \end{bmatrix}.$$

(7) Find the Jordan canonical forms for the matrix

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \lambda_1\lambda_2\lambda_3 & -\left(\lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_1\lambda_3\right) & \lambda_1 + \lambda_2 + \lambda_3 \end{bmatrix}.$$

(8) Find the Jordan canonical forms for the matrices

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & -5 & 4 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -3 & 3 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 6 & -11 & 6 \end{bmatrix}.$$

(9) An operator $L : V \to V$ is said to be *nilpotent* if $L^k = 0$ for some k.
 (a) Show that $\chi_L(t) = t^n$.
 (b) Show that L can be put in triangular form.
 (c) Show that L is diagonalizable if and only if $L = 0$.
 (d) Find a real matrix all of whose real eigenvalues are 0, but which is not nilpotent.

(10) Let $L : V \to V$ be a linear operator on an n-dimensional complex vector space. Show that for $p \in \mathbb{C}[t]$ the operator $p(L)$ is nilpotent if and only if the eigenvalues of L are roots of p. What goes wrong in the real case when $p(t) = t^2 + 1$ and $\dim V$ is odd?

(11) If

$$\ker\left((L - \lambda 1_V)^k\right) \neq \ker\left((L - \lambda 1_V)^{k-1}\right),$$

then the algebraic multiplicity of λ is $\geq k$. Given an example where the algebraic multiplicity $> k$ and

$$\ker\left((L - \lambda 1_V)^{k+1}\right) = \ker\left((L - \lambda 1_V)^k\right) \neq \ker\left((L - \lambda 1_V)^{k-1}\right).$$

(12) Show that if $L : V \to V$ is a linear operator such that

$$\begin{aligned} \chi_L(t) &= (t - \lambda_1)^{n_1} \cdots (t - \lambda_k)^{n_k}, \\ \mu_L(t) &= (t - \lambda_1)^{m_1} \cdots (t - \lambda_k)^{m_k}, \end{aligned}$$

then m_i corresponds to the largest Jordan block that has λ_i on the diagonal. Next show that m_i is the first integer such that

$$\ker\left((L - \lambda_i 1_V)^{m_i}\right) = \ker\left((L - \lambda_i 1_V)^{m_i + 1}\right).$$

(13) Show that if $L : V \to V$ is a linear operator on an n-dimensional complex vector space with distinct eigenvalues $\lambda_1, ..., \lambda_k$, then $p(L) = 0$, where

$$p(t) = (t - \lambda_1)^{n-k+1} \cdots (t - \lambda_k)^{n-k+1}.$$

Hint: Try $k = 2$.

(14) Assume that $L = S + N = S' + N'$ are two Jordan-Chevalley decompositions, i.e., $SN = NS$, $S'N' = N'S'$, S, S' are diagonalizable, and $N^n = (N')^n = 0$. Show that $S = S'$ and $N = N'$ if we know that $S = p(L)$ and $N = q(L)$ for polynomials p and q.

CHAPTER 3

Inner Product Spaces

So far we have only discussed vector spaces without adding any further structure to the space. In this chapter we shall study so called inner product spaces. These are vector spaces were in addition we know the length of each vector and the angle between two vectors. Since this is what we are used to from the plane and space it would seem like a reasonable extra layer of information.

We shall cover some of the basic constructions such as Gram-Schmidt orthogonalization, orthogonal projections, and orthogonal complements. In addition we prove the Cauchy-Schwarz and Bessel inequalities. In the last sections we cover the adjoint of linear maps and how it helps us understand the connections between inmage and kernel ultimately yielding a very interesting characterization of orthogonal projections. Finally we also explain matrix exponentials and how they can be used to solve systems of linear differential equations.

In this and the following chapter vector spaces always have either real or complex scalars.

1. Examples of Inner Products

1.1. Real Inner Products. We start by considering the (real) plane $\mathbb{R}^2 = \{(\alpha_1, \alpha_2) : \alpha_1, \alpha_2 \in \mathbb{R}\}$. The length of a vector is calculated via the Pythagorean theorem:

$$\|(\alpha_1, \alpha_2)\| = \sqrt{\alpha_1^2 + \alpha_2^2}.$$

The angle between two vectors $x = (\alpha_1, \alpha_2)$ and $y = (\beta_1, \beta_2)$ is a little trickier to compute. First we normalize the vectors

$$\frac{1}{\|x\|}x,$$
$$\frac{1}{\|y\|}y$$

so that they lie on the unit circle. We then trace the arc on the unit circle between the vectors in order to find the angle θ. If $x = (1, 0)$ the definitions of cosine and sine tell us that this angle can be computed via

$$\begin{aligned}\cos\theta &= \frac{\beta_1}{\|y\|},\\ \sin\theta &= \frac{\beta_2}{\|y\|}\end{aligned}$$

This suggests that, if we define

$$\begin{aligned}\cos\theta_1 &= \frac{\alpha_1}{\|x\|}, \sin\theta_1 = \frac{\alpha_2}{\|x\|},\\ \cos\theta_2 &= \frac{\beta_1}{\|y\|}, \sin\theta_2 = \frac{\beta_2}{\|y\|},\end{aligned}$$

then

$$\begin{aligned}\cos\theta &= \cos(\theta_2 - \theta_1)\\ &= \cos\theta_1\cos\theta_2 + \sin\theta_1\sin\theta_2\\ &= \frac{\alpha_1\beta_1 + \alpha_2\beta_2}{\|x\|\cdot\|y\|}.\end{aligned}$$

So if the inner or dot product of x and y is defined by

$$(x|y) = \alpha_1\beta_1 + \alpha_2\beta_2,$$

then we obtain the relationship

$$(x|y) = \|x\|\,\|y\|\cos\theta.$$

The length of vectors can also be calculated via

$$(x|x) = \|x\|^2.$$

The $(x|y)$ notation is used so as not to confuse the expression with pairs of vectors (x, y). One also often sees $\langle x, y\rangle$ or $\langle x|y\rangle$ used for inner products.

The key properties that we shall use to generalize the idea of an inner product are:

(1) $(x|x) = \|x\|^2 > 0$ unless $x = 0$.
(2) $(x|y) = (y|x)$.
(3) $x \to (x|y)$ is linear.

One can immediately generalize this algebraically defined inner product to $\mathbb{R}^3$ and even $\mathbb{R}^n$ by

$$\begin{aligned}(x|y) &= \left(\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{bmatrix}\middle|\begin{bmatrix}\beta_1\\ \vdots\\ \beta_n\end{bmatrix}\right)\\ &= x^t y\\ &= \begin{bmatrix}\alpha_1 & \cdots & \alpha_n\end{bmatrix}\begin{bmatrix}\beta_1\\ \vdots\\ \beta_n\end{bmatrix}\\ &= \alpha_1\beta_1 + \cdots + \alpha_n\beta_n.\end{aligned}$$

The three above mentioned properties still remain true, but we seem to have lost the connection with the angle. This is settled by observing that Cauchy's inequality holds:

$$\begin{aligned}(x|y)^2 &\leq (x|x)(y|y), \text{ or}\\ (\alpha_1\beta_1 + \cdots + \alpha_n\beta_n)^2 &\leq \left(\alpha_1^2 + \cdots + \alpha_n^2\right)\left(\beta_1^2 + \cdots + \beta_n^2\right).\end{aligned}$$

In other words

$$-1 \leq \frac{(x|y)}{\|x\|\,\|y\|} \leq 1.$$

This implies that the angle can be redefined up to sign through the equation

$$\cos\theta = \frac{(x|y)}{\|x\|\,\|y\|}.$$

In addition, as we shall see, the three properties can be used as axioms to prove everything we wish.

Two vectors are said to be *orthogonal* or *perpendicular* if their inner product vanishes. With this definition the proof of the Pythagorean Theorem becomes completely algebraic:

$$\|x\|^2 + \|y\|^2 = \|x+y\|^2,$$

if x and y are orthogonal. To see why this is true note that the properties of the inner product imply:

$$\begin{aligned}
\|x+y\|^2 &= (x+y|x+y) \\
&= (x|x) + (y|y) + (x|y) + (y|x) \\
&= (x|x) + (y|y) + 2\,(x|y) \\
&= \|x\|^2 + \|y\|^2 + 2\,(x|y)\,.
\end{aligned}$$

Thus the relation $\|x\|^2 + \|y\|^2 = \|x+y\|^2$ holds precisely when $(x|y) = 0$.

The inner product also comes in handy in expressing several other geometric constructions.

The *projection* of a vector x onto the line in the direction of y is given by

$$\begin{aligned}
\mathrm{proj}_y(x) &= \left(x\,\middle|\,\frac{y}{\|y\|}\right)\frac{y}{\|y\|} \\
&= \frac{(x|y)\,y}{(y|y)}.
\end{aligned}$$

All *planes* that have normal n, i.e., are perpendicular to n, are defined by an equation

$$(x|n) = c$$

for some c. The c is determined by any point x_0 that lies in the plane: $c = (x_0|n)$.

1.2. Complex Inner Products. Let us now see what happens if we try to use complex scalars. Our geometric picture seems to disappear, but we shall insist that the real part of a complex inner product must have the (geometric) properties we have already discussed. Let us start with the complex plane $\mathbb{C}$. Recall that if $z = \alpha_1 + \alpha_2 i$, then the complex conjugate is the reflection of z in the 1^{st} coordinate axis and is defined by $\bar{z} = \alpha_1 - \alpha_2 i$. Note that $z \to \bar{z}$ is not complex linear but only linear with respect to real scalar multiplication. Conjugation has some further important properties

$$\begin{aligned} \|z\| &= \sqrt{z \cdot \bar{z}}, \\ \overline{z \cdot w} &= \bar{z} \cdot \bar{w}, \\ z^{-1} &= \frac{\bar{z}}{\|z\|^2} \\ \operatorname{Re}(z) &= \frac{z + \bar{z}}{2} \\ \operatorname{Im}(z) &= \frac{z - \bar{z}}{2i} \end{aligned}$$

Given that $\|z\|^2 = z\bar{z}$ it seems natural to define the complex inner product by $(z|w) = z\bar{w}$. Thus it is not just complex multiplication. If we take the real part we also note that we retrieve the real inner product defined above

$$\begin{aligned} \operatorname{Re}(z|w) &= \operatorname{Re}(z\bar{w}) \\ &= \operatorname{Re}((\alpha_1 + \alpha_2 i)(\beta_1 - \beta_2 i)) \\ &= \alpha_1\beta_1 + \alpha_2\beta_2. \end{aligned}$$

Having established this we should be happy and just accept the nasty fact that complex inner products include conjugations.

The three important properties for complex inner products are

(1) $(x|x) = \|x\|^2 > 0$ unless $x = 0$.
(2) $(x|y) = \overline{(y|x)}$.
(3) $x \to (x|y)$ is complex linear.

The inner product on $\mathbb{C}^n$ is defined by

$$\begin{aligned} (x|y) &= \left(\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \middle| \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} \right) \\ &= x^t \bar{y} \\ &= \begin{bmatrix} \alpha_1 & \cdots & \alpha_n \end{bmatrix} \begin{bmatrix} \bar{\beta}_1 \\ \vdots \\ \bar{\beta}_n \end{bmatrix} \\ &= \alpha_1\bar{\beta}_1 + \cdots + \alpha_n\bar{\beta}_n. \end{aligned}$$

If we take the real part of this inner product we get the inner product on $\mathbb{R}^{2n} \simeq \mathbb{C}^n$.

We say that two complex vectors are orthogonal if their inner product vanishes. This is not quite the same as in the real case, as the two vectors 1 and i in $\mathbb{C}$ are not complex orthogonal even though they are orthogonal as real vectors. To spell this out a little further let us consider the Pythagorean Theorem for complex vectors.

Note that

$$\begin{aligned}\|x+y\|^2 &= (x+y|x+y)\\ &= (x|x)+(y|y)+(x|y)+(y|x)\\ &= (x|x)+(y|y)+(x|y)+\overline{(x|y)}\\ &= \|x\|^2+\|y\|^2+2\operatorname{Re}(x|y)\end{aligned}$$

Thus only the real part of the inner product needs to vanish for this theorem to hold. This should not come as a surprise as we already knew the result to be true in this case.

1.3. A Digression on Quaternions*. Another very interesting space that contains some new algebra as well as geometry is $\mathbb{C}^2 \simeq \mathbb{R}^4$. This is the space-time of special relativity. In this short section we mention some of the important features of this space.

In analogy with writing $\mathbb{C} = \operatorname{span}_{\mathbb{R}}\{1, i\}$ let us define

$$\begin{aligned}\mathbb{H} &= \operatorname{span}_{\mathbb{C}}\{1, j\}\\ &= \operatorname{span}_{\mathbb{R}}\{1, i, 1\cdot j, i\cdot j\}\\ &= \operatorname{span}_{\mathbb{R}}\{1, i, j, k\}.\end{aligned}$$

The three vectors i, j, k form the usual basis for the three dimensional space $\mathbb{R}^3$. The remaining coordinate in $\mathbb{H}$ is the time coordinate. In $\mathbb{H}$ we also have a conjugation that changes the sign in front of the imaginary numbers i, j, k

$$\begin{aligned}\bar{q} &= \overline{\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k}\\ &= \alpha_0-\alpha_1 i-\alpha_2 j-\alpha_3 k.\end{aligned}$$

To make perfect sense of things we need to figure out how to multiply i, j, k. In line with $i^2=-1$ we also define $j^2=-1$ and $k^2=-1$. As for the mixed products we have already defined $ij=k$. More generally we can decide how to compute these products by using the cross product in $\mathbb{R}^3$. Thus

$$\begin{aligned}ij &= k=-ji,\\ jk &= i=-kj,\\ ki &= j=-ik.\end{aligned}$$

This enables us to multiply $q_1, q_2 \in \mathbb{H}$. The multiplication is not commutative, but it is associative (unlike the cross product) and nonzero elements have inverses. The fact that the imaginary numbers i, j, k anti-commute shows that conjugation must reverse the order of multiplication (like taking inverses of matrices and quaternions)

$$\overline{pq}=\bar{q}\bar{p}.$$

As with real and complex numbers we have that

$$q\bar{q}=|q|^2=\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2.$$

This shows that every non-zero quaternion has an inverse given by

$$q^{-1}=\frac{\bar{q}}{|q|^2}.$$

The space $\mathbb{H}$ with usual vector addition and this multiplication is called the space of *quaternions*. The name was chosen by Hamilton who invented these numbers and wrote voluminous material on their uses.

As with complex numbers we have a real part, namely, the part without i, j, k, that can be calculated by

$$\operatorname{Re} q = \frac{q + \bar{q}}{2}$$

The usual real inner product on $\mathbb{R}^4$ can now be defined by

$$(p|q) = \operatorname{Re}(p \cdot \bar{q}).$$

If we ignore the conjugation but still take the real part we obtain something else entirely

$$\begin{aligned} (p|q)_{1,3} &= \operatorname{Re} pq \\ &= \operatorname{Re}(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k) \\ &= \alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3. \end{aligned}$$

We note that restricted to the time axis this is the usual inner product while if restrict to the space part it is the negative of the usual inner product. This *pseudo-inner* product is what is used in special relativity. The subscript 1,3 refers to the signs that appear in the formula, 1 plus and 3 minuses.

Note that one can have $(q|q)_{1,3} = 0$ without $q = 0$. The geometry of such an inner product is thus quite different from the usual ones we introduced above.

The purpose of this very brief encounter with quaternions and space-times is to show that they appear quite natuarlly in the context of linear algebra. While we won't use them here, they are used quite a bit in more advanced mathematics and physics..

1.4. Exercises.

(1) Using the algebraic properties of inner products show the law of cosines

$$c^2 = a^2 + b^2 - 2ab\cos\theta,$$

where a and b are adjacent sides in a triangle forming an angle θ and c is the opposite side.

(2) Here are some matrix constructions of both complex and quaternion numbers.

(a) Show that $\mathbb{C}$ is isomorphic (same addition and multiplication) to the set of real 2×2 matrices of the form

$$\begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}.$$

(b) Show that $\mathbb{H}$ is isomorphic to the set of complex 2×2 matrices of the form

$$\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}.$$

(c) Show that $\mathbb{H}$ is isomorphic to the set of real 4×4 matrices

$$\begin{bmatrix} A & B \\ -B^t & A^t \end{bmatrix}$$

that consists of 2×2 blocks

$$A = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}, B = \begin{bmatrix} \gamma & \delta \\ -\delta & \gamma \end{bmatrix}.$$

(d) Show that the quaternionic 2×2 matrices of the form

$$\begin{bmatrix} p & q \\ -\bar{q} & \bar{p} \end{bmatrix}$$

form a real vector space isomorphic to $\mathbb{R}^8$, but that matrix multiplication doesn't necessarily give us a matrix of this type.

(3) If $q \in \mathbb{H}$ consider the map $\mathrm{Ad}_q : \mathbb{H} \to \mathbb{H}$ defined by $\mathrm{Ad}_q(x) = qxq^{-1}$.
   (a) Show that $x = 1$ is an eigenvector with eigenvalue 1.
   (b) Show that Ad_q maps $\mathrm{span}_{\mathbb{R}}\{i, j, k\}$ to itself and defines an isometry on $\mathbb{R}^3$.
   (c) If we assume $|q|^2 = 1$, then $\mathrm{Ad}_{q_1} = \mathrm{Ad}_{q_2}$ if and only if $q_1 = \pm q_2$.

2. Inner Products

Recall that we only use real or complex vector spaces. Thus the field $\mathbb{F}$ of scalars is always $\mathbb{R}$ or $\mathbb{C}$. An *inner product* on a vector space V over $\mathbb{F}$ is an $\mathbb{F}$ valued pairing $(x|y)$ for $x, y \in V$, i.e., a map $(x|y) : V \times V \to \mathbb{F}$, that satisfies:

(1) $(x|x) \geq 0$ and vanishes only when $x = 0$.
(2) $(x|y) = \overline{(y|x)}$.
(3) For each $y \in V$ the map $x \to (x|y)$ is linear.

A vector space with an inner product is called an inner product space. In the real case the inner product is also called a *Euclidean structure*, while in the complex situation the inner product is known as a *Hermitian structure*. Observe that a complex inner product $(x|y)$ always defines a real inner product $\mathrm{Re}(x|y)$ that is symmetric and linear with respect to real scalar multiplication. One also uses the term *dot product* for the standard inner products in $\mathbb{R}^n$ and $\mathbb{C}^n$. The term *scalar product* is also used quite often as a substitute for inner product. In fact this terminology seems better as it explains that the product of two vectors becomes a scalar.

We note that the second property really only makes sense when the inner product is complex valued. If V is a real vector space, then the inner product is real valued and hence symmetric in x and y. In the complex case property 2 implies that $(x|x)$ is real, thus showing that the condition in property 1 makes sense. If we combine the second and third conditions we get the sesqui-linearity properties:

$$\begin{aligned} (\alpha_1 x_1 + \alpha_2 x_2 | y) &= \alpha_1 (x_1|y) + \alpha_2 (x_2|y), \\ (x|\beta_1 y_1 + \beta_2 y_2) &= \bar{\beta}_1 (x|y_1) + \bar{\beta}_2 (x|y_2). \end{aligned}$$

In particular we have the scaling property

$$\begin{aligned} (\alpha x|\alpha x) &= \alpha\bar{\alpha}(x|x) \\ &= |\alpha|^2 (x|x). \end{aligned}$$

We define the *length* or *norm* of a vector by

$$\|x\| = \sqrt{(x|x)}.$$

In case $(x|y)$ is complex we see that $(x|y)$ and $\mathrm{Re}(x|y)$ define the same norm. Note that $||x||$ is nonnegative and only vanishes when $x = 0$. We also have the scaling proerty $||\alpha x|| = |\alpha|\,||x||$. The triangle inequality $||x + y|| \leq ||x|| + ||y||$ will be established later in this section after some important preparatory work. Before studying the properties of inner products further let us list some important examples. We already have what we shall refer to as the standard inner product structures on $\mathbb{R}^n$ and $\mathbb{C}^n$.

EXAMPLE 63. *If we have an inner product on V, then we also get an inner product on all of the subspaces of V.*

EXAMPLE 64. *If we have inner products on V and W, both with respect to $\mathbb{F}$, then we get an inner product on $V \times W$ defined by*

$$((x_1, y_1) \,|\, (x_2, y_2)) = (x_1|x_2) + (y_1|y_2)\,.$$

Note that $(x, 0)$ and $(0, y)$ always have zero inner product.

EXAMPLE 65. *Given that $\mathrm{Mat}_{n\times m}(\mathbb{C}) = \mathbb{C}^{n\cdot m}$ we have an inner product on this space. As we shall see it has an interesting alternate construction. Let $A, B \in \mathrm{Mat}_{n\times m}(\mathbb{C})$ the transpose $B^t \in \mathrm{Mat}_{m\times n}(\mathbb{C})$ of B is simply the matrix were rows and columns are interchanged, i.e.,*

$$\begin{aligned} B^t &= \begin{bmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{bmatrix}^t \\ &= \begin{bmatrix} \beta_{11} & \cdots & \beta_{n1} \\ \vdots & \ddots & \vdots \\ \beta_{1m} & \cdots & \beta_{nm} \end{bmatrix}. \end{aligned}$$

The adjoint B^* is the transpose combined with conjugating each entry

$$B^* = \begin{bmatrix} \bar{\beta}_{11} & \cdots & \bar{\beta}_{n1} \\ \vdots & \ddots & \vdots \\ \bar{\beta}_{1m} & \cdots & \bar{\beta}_{nm} \end{bmatrix}.$$

The inner product $(A|B)$ can now be defined as

$$\begin{aligned} (A|B) &= \operatorname{tr} AB^* \\ &= \operatorname{tr} B^*A. \end{aligned}$$

In case $m = 1$ we have $\mathrm{Mat}_{n\times 1}(\mathbb{C}) = \mathbb{C}^n$ and we recover the standard inner product from the number B^*A. In the general case we note that it also defines the usual inner product as

$$\begin{aligned} (A|B) &= \operatorname{tr} AB^* \\ &= \sum_{i,j} \alpha_{ij}\bar{\beta}_{ij}. \end{aligned}$$

EXAMPLE 66. *Let $V = C^0([a, b], \mathbb{C})$ and define*

$$(f|g) = \int_a^b f(t)\,\bar{g}(t)\,dt.$$

Then

$$\|f\|_2 = \sqrt{(f, f)}.$$

If $V = C^0([a, b], \mathbb{R})$, then we have the real inner product

$$(f|g) = \int_a^b f(t)\,g(t)\,dt$$

In the above example it is often convenient to normalize the inner product so that the function $f = 1$ is of unit length. This normalized inner product is defined as

$$(f|g) = \frac{1}{b-a}\int_a^b f(t)\,\bar{g}(t)\,dt.$$

EXAMPLE 67. *Another important infinite dimensional inner product space is the space ℓ^2 first investigated by Hilbert. It is the collection of all real or complex sequences (α_n) such that $\sum_n |\alpha_n|^2 < \infty$. We have not specified the index set n, but we always think of it as being $\mathbb{N}$, $\mathbb{N}_0$, or $\mathbb{Z}$. If we wish to specify the index set we will use the notation $\ell^2(\mathbb{N})$ etc. Because these index sets are all bijectively equivalent they all the define the same space but with different indices for the coordinates α_n. Addition and scalar multiplication are defined by*

$$\begin{aligned} (\alpha_n) + (\beta_n) &= (\alpha_n + \beta_n), \\ \beta(\alpha_n) &= (\beta\alpha_n). \end{aligned}$$

Since

$$\begin{aligned} \sum_n |\beta\alpha_n|^2 &= |\beta|^2 \sum_n |\alpha_n|^2, \\ \sum_n |\alpha_n + \beta_n|^2 &\leq \sum_n \left(2|\alpha_n|^2 + 2|\beta_n|^2\right) \\ &= 2\sum_n |\alpha_n|^2 + 2\sum_n |\beta_n|^2 \end{aligned}$$

it follows that ℓ^2 is a subspace of the space of all sequences. The inner product $((\alpha_n)\,|\,(\beta_n))$ is defined by

$$((\alpha_n)\,|\,(\beta_n)) = \sum_n \alpha_n \bar{\beta}_n.$$

For that to make sense we need to know that

$$\sum_n \left|\alpha_n \bar{\beta}_n\right| < \infty.$$

This follows from

$$\begin{aligned} \left|\alpha_n \bar{\beta}_n\right| &= |\alpha_n|\left|\bar{\beta}_n\right| \\ &= |\alpha_n||\beta_n| \\ &\leq |\alpha_n|^2 + |\beta_n|^2 \end{aligned}$$

and the fact that

$$\sum_n \left(|\alpha_n|^2 + |\beta_n|^2\right) < \infty.$$

We declare that two vectors x and y are *orthogonal* or *perpendicular* if $(x|y) = 0$ and we denote this by $x \perp y$. The proof of the Pythagorean Theorem for both $\mathbb{R}^n$ and $\mathbb{C}^n$ clearly carries over to this more abstract situation. So if $(x|y) = 0$, then $\|x + y\|^2 = \|x\|^2 + \|y\|^2$.

The *orthogonal projection* of a vector x onto a nonzero vector y is defined by

$$\begin{aligned}\operatorname{proj}_y(x) &= \left(x \left| \frac{y}{\|y\|}\right.\right)\frac{y}{\|y\|} \\ &= \frac{(x|y)}{(y|y)}y.\end{aligned}$$

This projection creates a vector in the subspace spanned by y. The fact that it makes sense to call it the orthogonal projection is explained in the next proposition.

PROPOSITION 20. *Given a nonzero y the map $x \to \operatorname{proj}_y(x)$ is linear and a projection with the further property that $x - \operatorname{proj}_y(x)$ and $\operatorname{proj}_y(x)$ are orthogonal. In particular*

$$\|x\|^2 = \left\|x - \operatorname{proj}_y(x)\right\|^2 + \left\|\operatorname{proj}_y(x)\right\|^2,$$

and

$$\left\|\operatorname{proj}_y(x)\right\| \leq \|x\|.$$

PROOF. The definition of $\operatorname{proj}_y(x)$ immediately implies that it is linear from the linearity of the inner product. That it is a projection follows from

$$\begin{aligned}\operatorname{proj}_y\left(\operatorname{proj}_y(x)\right) &= \operatorname{proj}_y\left(\frac{(x|y)}{(y|y)}y\right) \\ &= \frac{(x|y)}{(y|y)}\operatorname{proj}_y(y) \\ &= \frac{(x|y)}{(y|y)}\frac{(y|y)}{(y|y)}y \\ &= \frac{(x|y)}{(y|y)}y \\ &= \operatorname{proj}_y(x).\end{aligned}$$

To check orthogonality simply compute

$$\begin{aligned}
\left(x-\operatorname{proj}_y(x)\,|\,\operatorname{proj}_y(x)\right) &= \left(x-\frac{(x,y)}{(y,y)}y\,\middle|\,\frac{(x,y)}{(y,y)}y\right)\\
&= \left(x\,\middle|\,\frac{(x|y)}{(y|y)}y\right)-\left(\frac{(x|y)}{(y|y)}y\,\middle|\,\frac{(x|y)}{(y|y)}y\right)\\
&= \frac{\overline{(x|y)}}{(y|y)}(x|y)-\frac{|(x|y)|^2}{|(y|y)|^2}(y|y)\\
&= \frac{|(x|y)|^2}{(y|y)}-\frac{|(x|y)|^2}{(y|y)}\\
&= 0.
\end{aligned}$$

The Pythagorean Theorem now implies the relationship

$$\|x\|^2=\left\|x-\operatorname{proj}_y(x)\right\|^2+\left\|\operatorname{proj}_y(x)\right\|^2.$$

Using $\left\|x-\operatorname{proj}_y(x)\right\|^2\geq 0$ we then obtain the inequality $\left\|\operatorname{proj}_y(x)\right\|\leq\|x\|$. □

Two important corollaries follow directly from this result..

Corollary 20. (The Cauchy-Schwarz Inequality)

$$|(x|y)|\leq\|x\|\,\|y\|.$$

Proof. If $y=0$ the inequality is trivial. Otherwise use

$$\begin{aligned}
\|x\| &\geq \left\|\operatorname{proj}_y(x)\right\|\\
&= \left|\frac{(x|y)}{(y|y)}\right|\|y\|\\
&= \frac{|(x|y)|}{\|y\|}.
\end{aligned}$$

□

Corollary 21. (The Triangle Inequality)

$$\|x+y\|\leq\|x\|+\|y\|.$$

Proof. We simply compute

$$\begin{aligned}
\|x+y\|^2 &= (x+y|x+y)\\
&= \|x\|^2+2\operatorname{Re}(x|y)+\|y\|^2\\
&\leq \|x\|^2+2\,|(x|y)|+\|y\|^2\\
&\leq \|x\|^2+2\,\|x\|\,\|y\|+\|y\|^2\\
&= (\|x\|+\|y\|)^2.
\end{aligned}$$

□

2.1. Exercises.

(1) Show that a hyperplane $H = \{x \in V : (a|x) = \alpha\}$ in a real n-dimensional inner product space V can be represented as an affine subspace

$$H = \{t_1 x_1 + \cdots + t_n x_n : t_1 + \cdots + t_n = 1\},$$

where $x_1, ..., x_n \in H$. Find conditions on $x_1, .., x_n$ so that they generate a hyperplane.

(2) Let $x = (2,1)$ and $y = (3,1)$ in $\mathbb{R}^2$. If $z \in \mathbb{R}^2$ satisfies $(z|x) = 1$ and $(z|y) = 2$, then find the coordinates for z.

(3) In $\mathbb{R}^n$ assume that we have $x_1, ..., x_k \in V$ with $\|x_i\| > 0$, $(x_i|x_j) < 0$, $i \neq j$.
   (a) Show that it is possible to have $k = n + 1$.
   (b) Show that if $k \leq n$ then $x_1, ..., x_k$ are linearly independent..

(4) In a real inner product space V select $y \neq 0$. For fixed $\alpha \in \mathbb{R}$ show that $H = \left\{x \in V : \operatorname{proj}_y(x) = \alpha y\right\}$ describes a hyperplane with normal y.

(5) Let V be an inner product space and let $y, z \in V$. Show that $y = z$ if and only if $(x|y) = (x|z)$ for all $x \in V$.

(6) Prove the Cauchy-Schwarz inequality by expanding the right hand side of the inequality

$$0 \leq \left\| x - \frac{(x|y)}{\|y\|^2} y \right\|^2$$

(7) Let V be an inner product space and x_1, ..., x_n, y_1, ..., $y_n \in V$. Show the following generalized Cauchy-Schwarz inequality

$$\left(\sum_{i=1}^{n} |(x_i|y_i)|\right)^2 \leq \left(\sum_{i=1}^{n} \|x_i\|^2\right)\left(\sum_{i=1}^{n} \|y_i\|^2\right)$$

(8) Let $S^{n-1} = \{x \in \mathbb{R}^n : \|x\| = 1\}$ be the unit sphere. When $n = 1$ it consists of two points. When $n = 2$ it is a circle etc. A finite subset $\{x_1, ..., x_k\} \in S^{n-1}$ is said to consist of equidistant points if $\measuredangle(x_i, x_j) = \theta$ for all $i \neq j$.
   (a) Show that this is equivalent to assuming that $(x_i|x_j) = \cos\theta$ for all $i \neq j$.
   (b) Show that S^0 contains a set of two equidistant points, S^1 a set of three equidistant points, and S^2 a set of four equidistant points.
   (c) Using induction on n show that a set of equidistant points in S^{n-1} contains no more than $n + 1$ elements.

(9) In an inner product space show the *parallelogram rule*

$$\|x - y\|^2 + \|x + y\|^2 = 2\|x\|^2 + 2\|y\|^2.$$

Here x and y describe the sides in a parallelogram and $x + y$ and $x - y$ the diagonals.

(10) In a complex inner product space show that

$$4(x|y) = \sum_{k=0}^{3} i^k \left\|x + i^k y\right\|^2.$$

3. Orthonormal Bases

Let us fix an inner product space V. A possibly infinite collection $e_1, ..., e_n, ...$ of vectors in V is said to be *orthogonal* if $(e_i|e_j) = 0$ for $i \neq j$. If in addition these vectors are of unit length, i.e., $(e_i|e_j) = \delta_{ij}$, then we call the collection *orthonormal*.

The usual bases for $\mathbb{R}^n$ and $\mathbb{C}^n$ are evidently orthonormal collections. Since they are also bases we call them *orthonormal bases*.

LEMMA 18. *Let $e_1, ..., e_n$ be orthonormal. Then $e_1, .., e_n$ are linearly independent and any element $x \in \operatorname{span}\{e_1, .., e_n\}$ has the expansion*

$$x = (x|e_1)\, e_1 + \cdots (x|e_n)\, e_n.$$

PROOF. Note that if $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$, then

$$\begin{aligned} (x|e_i) &= (\alpha_1 e_1 + \cdots + \alpha_n e_n|e_i) \\ &= \alpha_1 (e_1|e_i) + \cdots + \alpha_n (e_n|e_i) \\ &= \alpha_1 \delta_{1i} + \cdots + \alpha_n \delta_{ni} \\ &= \alpha_i. \end{aligned}$$

In case $x = 0$, this gives us linear independence and in case $x \in \operatorname{span}\{e_1, .., e_n\}$ we have computed the i^{th} coordinate using the inner product. □

This allows us to construct not only an isomorphism to $\mathbb{F}^n$ but an isomorphism that preserves inner products. We say that two inner product spaces V and W over $\mathbb{F}$ are *isometric*, if we can find an *isometry* $L : V \to W$, i.e., an isomorphism such that $(L(x)|L(y)) = (x|y)$.

LEMMA 19. *If V admits a basis that is orthonormal, then V is isometric to $\mathbb{F}^n$.*

PROOF. Choose an orthonormal basis $e_1, ..., e_n$ for V and define the usual isomorphism $L : \mathbb{F}^n \to V$ by

$$\begin{aligned} L\left(\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}\right) &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \\ &= \alpha_1 e_1 + \cdots + \alpha_n e_n. \end{aligned}$$

Note that by the above Lemma the inverse map that computes the coordinates of a vector is explicitly given by

$$L^{-1}(x) = \begin{bmatrix} (x|e_1) \\ \vdots \\ (x|e_n) \end{bmatrix}.$$

If we take two vectors x, y and expand them

$$\begin{aligned} x &= \alpha_1 e_1 + \cdots + \alpha_n e_n, \\ y &= \beta_1 e_1 + \cdots + \beta_n e_n, \end{aligned}$$

then we can compute

$$\begin{aligned}(x|y) &= (\alpha_1 e_1 + \cdots + \alpha_n e_n | y) \\ &= \alpha_1 (e_1|y) + \cdots + \alpha_n (e_n|y) \\ &= \alpha_1 \overline{(y|e_1)} + \cdots + \alpha_n \overline{(y|e_n)} \\ &= \alpha_1 \overline{\beta_1} + \cdots + \alpha_n \overline{\beta_n} \\ &= \left(\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \middle| \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} \right) \\ &= \left(L^{-1}(x) | L^{-1}(y) \right).\end{aligned}$$

This proves that L^{-1} is an isometry. This implies that L is also an isometry. □

We are now left with the nagging possibility that orthonormal bases might be very special and possibly not exist.

The procedure for constructing orthonormal collections is known as the *Gram-Schmidt procedure*. It is not clear who invented the process, but these two people definitely promoted and used it to great effect. Gram was in fact an actuary and as such was mainly interested in applied statistics.

Given a linearly independent set $x_1, ..., x_m$ in an inner product space V it is possible to construct an orthonormal collection $e_1, ..., e_m$ such that

$$\text{span}\{x_1, ..., x_m\} = \text{span}\{e_1, ..., e_m\}.$$

The procedure is actually iterative and creates $e_1, ..., e_m$ in such a way that

$$\begin{aligned}\text{span}\{x_1\} &= \text{span}\{e_1\}, \\ \text{span}\{x_1, x_2\} &= \text{span}\{e_1, e_2\}, \\ &\vdots \\ \text{span}\{x_1, ..., x_m\} &= \text{span}\{e_1, ..., e_m\}.\end{aligned}$$

This basically forces us to define e_1 as

$$e_1 = \frac{1}{\|x_1\|} x_1.$$

Then e_2 is constructed by considering

$$\begin{aligned}z_2 &= x_2 - \text{proj}_{x_1}(x_2) \\ &= x_2 - \text{proj}_{e_1}(x_2) \\ &= x_2 - (x_2|e_1) e_1,\end{aligned}$$

and defining

$$e_2 = \frac{1}{\|z_2\|} z_2.$$

Having constructed an orthonormal set $e_1, ..., e_k$ we can then define

$$z_{k+1} = x_{k+1} - (x_{k+1}|e_1) e_1 - \cdots - (x_{k+1}|e_k) e_k.$$

As

$$\begin{aligned}\text{span}\{x_1, ..., x_k\} &= \text{span}\{e_1, ..., e_k\}, \\ x_{k+1} &\notin \text{span}\{x_1, ..., x_k\}\end{aligned}$$

we have that $z_{k+1} \neq 0$. Thus we can define

$$e_{k+1} = \frac{1}{\|z_{k+1}\|} z_{k+1}.$$

To see that e_{k+1} is perpendicular to $e_1, ..., e_k$ we note that

$$\begin{aligned}
(e_{k+1}|e_i) &= \frac{1}{\|z_{k+1}\|}(z_{k+1}|e_i) \\
&= \frac{1}{\|z_{k+1}\|}(x_{k+1}|e_i) - \frac{1}{\|z_{k+1}\|}\left(\sum_{j=1}^{k}(x_{k+1}|e_j)\,e_j \middle| e_i\right) \\
&= \frac{1}{\|z_{k+1}\|}(x_{k+1}|e_i) - \frac{1}{\|z_{k+1}\|}\sum_{j=1}^{k}(x_{k+1}|e_j)(e_j|e_i) \\
&= \frac{1}{\|z_{k+1}\|}(x_{k+1}|e_i) - \frac{1}{\|z_{k+1}\|}\sum_{j=1}^{k}(x_{k+1}|e_j)\,\delta_{ij} \\
&= \frac{1}{\|z_{k+1}\|}(x_{k+1}|e_i) - \frac{1}{\|z_{k+1}\|}(x_{k+1}|e_i) \\
&= 0.
\end{aligned}$$

Since

$$\begin{aligned}
\operatorname{span}\{x_1\} &= \operatorname{span}\{e_1\}, \\
\operatorname{span}\{x_1, x_2\} &= \operatorname{span}\{e_1, e_2\}, \\
&\vdots \\
\operatorname{span}\{x_1, ..., x_m\} &= \operatorname{span}\{e_1, ..., e_m\}
\end{aligned}$$

we have constructed $e_1, ..., e_m$ in such a way that

$$\begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix} = \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} B,$$

where B is an upper triangular $m \times m$ matrix with positive diagonal entries. Conversely we have

$$\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} = \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix} R,$$

where $R = B^{-1}$ is also upper triangular with positive diagonal entries. Given that we have a formula for the expansion of each x_k in terms of $e_1, ..., e_k$ we see that

$$R = \begin{bmatrix}
(x_1|e_1) & (x_2|e_1) & (x_3|e_1) & \cdots & (x_m|e_1) \\
0 & (x_2|e_2) & (x_3|e_2) & \cdots & (x_m|e_2) \\
0 & 0 & (x_3|e_3) & \cdots & (x_m|e_3) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & (x_m|e_m)
\end{bmatrix}$$

We often abbreviate

$$\begin{aligned}
A &= \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix}, \\
Q &= \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix},
\end{aligned}$$

and obtain the *QR-factorization* $A = QR$. In case V is $\mathbb{R}^n$ or $\mathbb{C}^n$ A is a general $n \times m$ matrix of rank m, Q is also an $n \times m$ matrix of rank m with the added feature that its columns are orthonormal, and R is an upper triangular $m \times m$ matrix. Note that in this interpretation the QR-factorization is an improved Gauss elimination: $A = PU$, with $P \in Gl_n$ and U upper triangular.

With that in mind it is not surprising that the QR-factorization gives us a way of inverting the linear map

$$\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} : \mathbb{F}^n \to V$$

when $x_1, ..., x_n$ is a basis. First recall that the isometry

$$\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} : \mathbb{F}^n \to V$$

is easily inverted and the inverse can be symbolically represented as

$$\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^{-1} = \begin{bmatrix} \overline{(e_1|\cdot)} \\ \vdots \\ \overline{(e_n|\cdot)} \end{bmatrix},$$

or more precisely

$$\begin{aligned} \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^{-1}(x) &= \begin{bmatrix} \overline{(e_1|x)} \\ \vdots \\ \overline{(e_n|x)} \end{bmatrix} \\ &= \begin{bmatrix} (x|e_1) \\ \vdots \\ (x|e_n) \end{bmatrix} \end{aligned}$$

This is the great feature of orthonormal bases, namely, that one has an explicit formula for the coordinates in such a basis. Next on the agenda is the invertibility of R. Given that it is upper triangular this is a reasonably easy problem in the theory of solving linear systems. However, having found the orthonormal basis through Gram-Schmidt we have already found this inverse since

$$\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} = \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} R$$

implies that

$$\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} R^{-1}$$

and the goal of the process was to find $e_1, ..., e_n$ as a linear combination of $x_1, ..., x_n$. Thus we obtain the formula

$$\begin{aligned} \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^{-1} &= R^{-1} \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^{-1} \\ &= R^{-1} \begin{bmatrix} \overline{(e_1|\cdot)} \\ \vdots \\ \overline{(e_n|\cdot)} \end{bmatrix}. \end{aligned}$$

The Gram-Schmidt process, therefore, not only gives us an orthonormal basis but it also gives us a formula for the coordinates of a vector with respect to the original basis.

It should also be noted that if we start out with a set $x_1, ..., x_m$ that is not linearly independent, then this will be revealed in the process of constructing $e_1, ..., e_m$. What will happen is that either $x_1 = 0$ or there is a smallest k such that x_{k+1} is a linear combination of $x_1, ..., x_k$. In the latter case we get to construct $e_1, ..., e_k$ since $x_1, ..., x_k$ were linearly independent. As $x_{k+1} \in \operatorname{span}\{e_1, ..., e_k\}$ we must have that

$$z_{k+1} = x_{k+1} - (x_{k+1}|e_1)\, e_1 - \cdots - (x_{k+1}|e_k)\, e_k = 0$$

since the way in which x_{k+1} is expanded in terms of $e_1, ..., e_k$ is given by

$$x_{k+1} = (x_{k+1}|e_1)\, e_1 + \cdots + (x_{k+1}|e_k)\, e_k.$$

Thus we fail to construct the unit vector e_{k+1}.

With all this behind us we have proved the important result.

THEOREM 27. (Uniqueness of Inner Product Spaces) *An n-dimensional inner product space over $\mathbb{R}$, respectively $\mathbb{C}$, is isometric to $\mathbb{R}^n$, respectively $\mathbb{C}^n$.*

The *operator norm*, for a linear operator $L : V \to W$ between inner product spaces is defined so that

$$\|L(x)\| \leq \|L\| \, \|x\| .$$

Using the scaling properties of the norm and linearity of L this is the same as saying

$$\left\| L\left(\frac{x}{\|x\|}\right)\right\| \leq \|L\| , \text{ for } x \neq 0.$$

Since $\left\|\frac{x}{\|x\|}\right\| = 1$, we can define the operator norm by

$$\|L\| = \sup_{\|x\|=1} \|L(x)\| .$$

This operator norm is finite provided V is finite dimensional.

THEOREM 28. *Let $L : V \to W$ be a linear map. If V is a finite dimensional inner product space, then*

$$\|L\| = \sup_{\|x\|=1} \|L(x)\| < \infty.$$

PROOF. Start by selecting an orthonormal basis $e_1, ..., e_n$ for V. Then observe that

$$\begin{aligned} \|L(x)\| &= \left\| L\left(\sum_{i=1}^{n} (x|e_i)\, e_i\right)\right\| \\ &= \left\| \sum_{i=1}^{n} (x|e_i)\, L(e_i)\right\| \\ &\leq \sum_{i=1}^{n} |(x|e_i)| \, \|L(e_i)\| \\ &\leq \sum_{i=1}^{n} \|x\| \, \|L(e_i)\| \\ &= \left(\sum_{i=1}^{n} \|L(e_i)\|\right) \|x\| . \end{aligned}$$

Thus

$$\|L\| \leq \sum_{i=1}^{n} \|L(e_i)\| .$$

□

To finish the section let us try to do a few concrete examples.

EXAMPLE 68. *Consider the vectors* $x_1 = (1,1,0)$, $x_2 = (1,0,1)$, *and* $x_3 = (0,1,1,)$ *in* $\mathbb{R}^3$. *If we perform Gram-Schmidt then the QR factorization is*

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{3}} \end{bmatrix} \begin{bmatrix} \sqrt{2} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & \frac{3}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ 0 & 0 & \frac{2}{\sqrt{3}} \end{bmatrix}$$

EXAMPLE 69. *The Legendre polynomials of degrees 0, 1, and 2 on* $[-1,1]$ *are by definition the polynomials obtained via Gram-Schmidt from* $1, t, t^2$ *with respect to the inner product*

$$(f|g) = \int_{-1}^{1} f(t)\,\overline{g(t)}dt.$$

We see that $||1|| = \sqrt{2}$ *so the first polynomial is*

$$p_0(t) = \frac{1}{\sqrt{2}}.$$

To find $p_1(t)$ *we first find*

$$\begin{aligned} z_1 &= t - (t|p_0)\,p_0 \\ &= t - \left(\int_{-1}^{1} t\frac{1}{\sqrt{2}}dt\right)\frac{1}{\sqrt{2}} \\ &= t. \end{aligned}$$

Then

$$p_1(t) = \frac{t}{\|t\|} = \sqrt{\frac{3}{2}}t.$$

Finally for p_2 *we find*

$$\begin{aligned} z_2 &= t^2 - (t^2|p_0)\,p_0 - (t^2|p_1)\,p_1 \\ &= t^2 - \left(\int_{-1}^{1} t^2\frac{1}{\sqrt{2}}dt\right)\frac{1}{\sqrt{2}} - \left(\int_{-1}^{1} t^2\sqrt{\frac{3}{2}}tdt\right)\sqrt{\frac{3}{2}}t \\ &= t^2 - \frac{1}{3}. \end{aligned}$$

Thus

$$\begin{aligned} p_2(t) &= \frac{t^2 - \frac{1}{3}}{\|t^2 - \frac{1}{3}\|} \\ &= \sqrt{\frac{45}{8}}\left(t^2 - \frac{1}{3}\right). \end{aligned}$$

EXAMPLE 70. *A system of real equations* $Ax = b$ *can be interpreted geometrically as* n *equations*

$$\begin{aligned} (a_1|x) &= \beta_1, \\ &\vdots \\ (a_n|x) &= \beta_n, \end{aligned}$$

where a_k *is the* k^{th} *row in* A *and* β_k *the* k^{th} *coordinate for* b. *The solutions will be the intersection of the* n *hyperplanes* $H_k = \{z : (a_k|z) = \beta_k\}$.

EXAMPLE 71. *We wish to show that the trigonometric functions*

$$1 = \cos(0 \cdot t), \cos(t), \cos(2t), ..., \sin(t), \sin(2t), ...$$

are orthogonal in $C^{\infty}_{2\pi}(\mathbb{R}, \mathbb{R})$ *with respect to the inner product*

$$(f|g) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\, g(t)\, dt.$$

First observe that $\cos(mt)\sin(nt)$ *is an odd function. This proves that*

$$(\cos(mt) \,|\, \sin(nt)) = 0.$$

Thus we are reduced to showing that each of the two sequences

$$\begin{array}{c} 1, \cos(t), \cos(2t), .. \\ \sin(t), \sin(2t), ... \end{array}$$

are orthogonal. Using integration by parts we see

$$\begin{aligned}
& (\cos(mt) \,|\, \cos(nt)) \\
= & \frac{1}{2\pi}\int_{-\pi}^{\pi} \cos(mt)\cos(nt)\, dt \\
= & \frac{1}{2\pi}\left.\frac{\sin(mt)}{m}\cos(nt)\right|_{-\pi}^{\pi} - \frac{1}{2\pi}\int_{-\pi}^{\pi}\frac{\sin(mt)}{m}(-n)\sin(nt)\, dt \\
= & \frac{n}{m}\frac{1}{2\pi}\int_{-\pi}^{\pi}\sin(mt)\sin(nt)\, dt \\
= & \frac{n}{m}(\sin(mt) \,|\, \sin(nt)) \\
= & \frac{n}{m}\frac{1}{2\pi}\left.\frac{-\cos(mt)}{m}\sin(nt)\right|_{-\pi}^{\pi} - \frac{n}{m}\frac{1}{2\pi}\int_{-\pi}^{\pi}\frac{-\cos(mt)}{m}n\cos(nt)\, dt \\
= & \left(\frac{n}{m}\right)^2\frac{1}{2\pi}\int_{-\pi}^{\pi}\cos(mt)\cos(nt)\, dt \\
= & \left(\frac{n}{m}\right)^2(\cos(mt) \,|\, \cos(nt)).
\end{aligned}$$

When $n \neq m$ *and* $m > 0$ *this clearly proves that* $(\cos(mt) \,|\, \cos(nt)) = 0$ *and in addition that* $(\sin(mt) \,|\, \sin(nt)) = 0$*. Finally let us compute the norm of these functions. Clearly* $\|1\| = 1$*. We just proved that* $\|\cos(mt)\| = \|\sin(mt)\|$*. This combined with the fact that*

$$\sin^2(mt) + \cos^2(mt) = 1$$

shows that

$$\|\cos(mt)\| = \|\sin(mt)\| = \frac{1}{\sqrt{2}}$$

EXAMPLE 72. *Let us try to do Gram-Schmidt on* 1, $\cos t$, $\cos^2 t$ *using the above inner product. We already know that the first two functions are orthogonal so*

$$\begin{aligned} e_1 &= 1, \\ e_2 &= \sqrt{2}\cos(t). \end{aligned}$$

$$\begin{aligned} z_2 &= \cos^2(t) - \left(\cos^2(t)\,|1\right)1 - \left(\cos^2(t)\,|\sqrt{2}\cos(t)\right)\sqrt{2}\cos(t) \\ &= \cos^2(t) - \frac{1}{2\pi}\left(\int_{-\pi}^{\pi}\cos^2(t)\,dt\right) - \frac{2}{2\pi}\left(\int_{-\pi}^{\pi}\cos^2(t)\cos(t)\,dt\right)\cos t \\ &= \cos^2(t) - \frac{1}{2} - \frac{1}{\pi}\left(\int_{-\pi}^{\pi}\cos^3(t)\,dt\right)\cos t \\ &= \cos^2(t) - \frac{1}{2} \end{aligned}$$

Thus the third function is

$$\begin{aligned} e_3 &= \frac{\cos^2(t) - \frac{1}{2}}{\left\|\cos^2(t) - \frac{1}{2}\right\|} \\ &= 2\sqrt{2}\cos^2(t) - \sqrt{2}. \end{aligned}$$

3.1. Exercises.

(1) Use Gram-Schmidt on the vectors

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \end{bmatrix} = \begin{bmatrix} \sqrt{5} & -2 & 4 & e & 3 \\ 0 & 8 & \pi & 2 & -10 \\ 0 & 0 & 1+\sqrt{2} & 3 & -4 \\ 0 & 0 & 0 & -2 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

to obtain an orthonormal basis for $\mathbb{F}^5$.

(2) Find an orthonormal basis for $\mathbb{R}^3$ where the first vector is proportional to $(1,1,1)$.

(3) Use Gram-Schmidt on the collection $x_1 = (1,0,1,0)$, $x_2 = (1,1,1,0)$, $x_3 = (0,1,0,0)$.

(4) Use Gram-Schmidt on the collection $x_1 = (1,0,1,0)$, $x_2 = (0,1,1,0)$, $x_3 = (0,1,0,1)$ and complete to an orthonormal basis for $\mathbb{R}^4$.

(5) Use Gram-Schmidt on $\sin t, \sin^2 t, \sin^3 t$.

(6) Given an arbitrary collection of vectors $x_1, ..., x_m$ in an inner product space V, show that it is possible to find orthogonal vectors $z_1, ..., z_n \in V$ such that

$$\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} = \begin{bmatrix} z_1 & \cdots & z_n \end{bmatrix} A_{\text{ref}},$$

where A_{ref} is an $n \times m$ matrix in row echelon form. Explain how this can be used to solve systems of the form

$$\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_m \end{bmatrix} = b.$$

(7) The goal of this exercise is to construct a dual basis to a basis $x_1, ..., x_n$ for an inner product space V. We call $x_1^*, ..., x_n^*$ a dual basis if $\left(x_i | x_j^*\right) = \delta_{ij}$.

(a) Show that if $x_1^*, ..., x_n^*$ exist then it is a basis for V.

(b) Show that if $x_1, ..., x_n$ is a basis, then we have an isomorphism $L : V \to \mathbb{F}^n$ defined by

$$L(x) = \begin{bmatrix} (x|x_1) \\ \vdots \\ (x|x_n) \end{bmatrix}.$$

(c) Show that each basis has a unique dual basis (you have to show it exists and that there is only one such basis).
(d) Show that a basis is orthonormal if and only if it is *self-dual*, i.e., it is its own dual basis.
(e) Given $(1,1,0), (1,0,1), (0,1,1) \in \mathbb{R}^3$ find the dual basis.
(f) Find the dual basis for $1, t, t^2 \in P_2$ with respect to the inner product

$$(f|g) = \int_{-1}^{1} f(t) g(t) dt$$

(8) Using the inner product

$$(f|g) = \int_{0}^{1} f(t) g(t) dt$$

on $\mathbb{R}[t]$ and Gram-Schmidt on $1, t, t^2$ find an orthonormal basis for P_2.
(9) *(Legendre Polynomials)* Consider the inner product

$$(f|g) = \int_{a}^{b} f(t) g(t) dt$$

on $\mathbb{R}[t]$ and define

$$\begin{aligned} q_{2n}(t) &= (t-a)^n (t-b)^n, \\ p_n(t) &= \frac{d^n}{dt^n}(q_{2n}(t)). \end{aligned}$$

(a) Show that

$$\begin{aligned} q_{2n}(a) &= q_{2n}(b) = 0, \\ &\vdots \\ \frac{d^{n-1}q_{2n}}{dt^{n-1}}(a) &= \frac{d^{n-1}q_{2n}}{dt^{n-1}}(b) = 0. \end{aligned}$$

(b) Show that p_n has degree n.
(c) Use induction on n to show that $p_n(t)$ is perpendicular to $1, t, ..., t^{n-1}$. Hint: Use integration by parts.
(d) Show that $p_0, p_1, ..., p_n, ...$ are orthogonal to each other.
(10) *(Lagrange Interpolation)* Select $n+1$ distinct points $t_0, ..., t_n \in \mathbb{C}$ and consider

$$(p(t)|q(t)) = \sum_{i=0}^{n} p(t_i) \overline{q(t_i)}.$$

(a) Show that this defines an inner product on P_n but not on $\mathbb{C}[t]$.

(b) Consider

$$\begin{aligned} p_0(t) &= \frac{(t-t_1)(t-t_2)\cdots(t-t_{n-1})}{(t_0-t_1)(t_0-t_2)\cdots(t_0-t_{n-1})}, \\ p_1(t) &= \frac{(t-t_0)(t-t_2)\cdots(t-t_{n-1})}{(t_1-t_0)(t_1-t_2)\cdots(t_1-t_{n-1})}, \\ &\vdots \\ p_{n-1}(t) &= \frac{(t-t_0)(t-t_1)\cdots(t-t_{n-2})}{(t_{n-1}-t_0)(t_{n-1}-t_1)\cdots(t_{n-1}-t_{n-2})}. \end{aligned}$$

Show that $p_i(t_j) = \delta_{ij}$ and that $p_0, ..., p_n$ form an orthonormal basis for P_n.

(c) Use $p_0, ..., p_n$ to solve the problem of finding a polynomial $p \in P_n$ such that $p(t_i) = b_i$.

(d) Let $\lambda_1, ..., \lambda_n \in \mathbb{C}$ (they may not be distinct) and $f : \mathbb{C} \to \mathbb{C}$ a function. Show that there is a polynomial $p(t) \in \mathbb{C}[t]$ such that $p(\lambda_1) = f(\lambda_1), ..., p(\lambda_n) = f(\lambda_n)$.

(11) *(P. Enflo)* Let V be a finite dimensional inner product space and x_1, ..., x_n, y_1, ..., $y_n \in V$.Show Enflo's inequality

$$\left(\sum_{i,j=1}^{n} |(x_i|y_j)|^2\right)^2 \leq \left(\sum_{i,j=1}^{n} |(x_i|x_j)|^2\right)\left(\sum_{i,j=1}^{n} |(y_i|y_j)|^2\right).$$

Hint: Use an orthonormal basis and start expanding on the left hand side.

(12) Let $L : V \to V$ be an operator on a finite dimensional inner product space.

(a) If λ is an eigenvalue for L, then

$$|\lambda| \leq \|L\|.$$

(b) Given examples of 2×2 matrices where strict inequality always holds.

(13) Let $L : V_1 \to V_2$ and $K : V_2 \to V_3$ be linear maps between finite dimensional inner product spaces. Show that

$$||K \circ L|| \leq ||K||\,||L||.$$

(14) Let $L, K : V \to V$ be operators on a finite dimensional inner product space. If K is invertible show that

$$||L|| = \left|\left|K \circ L \circ K^{-1}\right|\right|.$$

(15) Let $L, K : V \to W$ be lienar maps between finite dimensional inner product spaces. Show that

$$||L + K|| \leq ||L|| + ||K||.$$

(16) Let $A \in \text{Mat}_{n\times m}(\mathbb{F})$. Show that

$$|\alpha_{ij}| \leq ||A||,$$

where $||A||$ is the operator norm of the linear map $A : \mathbb{F}^m \to \mathbb{F}^n$. Give examples where

$$||A|| \neq \sqrt{\text{tr}(AA^*)} = \sqrt{(A|A)}.$$

4. Orthogonal Complements and Projections

The goal of this section is to figure out if there is a best possible projection onto a subspace of a vector space. In general there are quite a lot of projections, but if we have an inner product on the vector space we can imagine that there should be a projection where the image of a vector is as close as possible to the original vector.

Let $M \subset V$ be a finite dimensional subspace of an inner product space. From the previous section we know that it is possible to find an orthonormal basis $e_1, ..., e_m$ for M. Using that basis we define $E : V \to V$ by

$$E(x) = (x|e_1)\, e_1 + \cdots + (x|e_m)\, e_m.$$

Note that $E(z) \in M$ for all $z \in V$. Moreover, if $x \in M$, then $E(x) = x$. Thus $E^2(z) = E(z)$ for all $z \in V$. This shows that E is a projection whose image is M. Next let us identify the kernel. If $x \in \ker(E)$, then

$$\begin{aligned} 0 &= E(x) \\ &= (x|e_1)\, e_1 + \cdots + (x|e_m)\, e_m. \end{aligned}$$

Since $e_1, ..., e_m$ is a basis this means that $(x|e_1) = \cdots = (x|e_m) = 0$. This in turn is equivalent to the condition

$$(x|z) = 0 \text{ for all } z \in M,$$

since any $z \in M$ is a linear combination of $e_1, ..., e_m$. The set of all such vectors is denoted

$$M^{\perp} = \{x \in V : (x|z) = 0 \text{ for all } z \in M\}$$

and is called the *orthogonal complement* to M in V. Given that $\ker(E) = M^{\perp}$ we have a formula for the kernel that does not depend on E. Thus E is simply the projection of V onto M along $M^{\perp}$. The only problem with this characterization is that we don't know from the outset that $V = M \oplus M^{\perp}$. In case M is finite dimensional, however, the existence of the projection E insures us that this must be the case as

$$x = E(x) + (1_V - E)(x)$$

and $(1_V - E)(x) \in \ker(E) = M^{\perp}$. In case we have an orthogonal direct sum decomposition: $V = M \oplus M^{\perp}$ we call the projection onto M along $M^{\perp}$ the *orthogonal projection* onto M and denote it by $\text{proj}_M : V \to V$.

The vector $\text{proj}_M(x)$ also solves our problem of finding the vector in M that is closest to x. To see why this is true, choose $z \in M$ and consider the triangle that has the three vectors x, $\text{proj}_M(x)$, and z as vertices. The sides are given by $x - \text{proj}_M(x)$, $\text{proj}_M(x) - z$, and $z - x$. Since $\text{proj}_M(x) - z \in M$ and $x - \text{proj}_M(x) \in M^{\perp}$ these two vectors are perpendicular and hence we have

$$\begin{aligned} \|x - \text{proj}_M(x)\|^2 &\leq \\ \|x - \text{proj}_M(x)\|^2 + \|\text{proj}_M(x) - z\|^2 &= \|x - z\|^2, \end{aligned}$$

where equality holds only when $\|\text{proj}_M(x) - z\|^2 = 0$, i.e., $\text{proj}_M(x)$ is the one and only point closest to x among all points in M.

Let us collect the above information in a theorem.

THEOREM 29. (Orthogonal Sum Decomposition) *Let V be an inner product space and $M \subset V$ a finite dimensional subspace. Then $V = M \oplus M^{\perp}$ and for any orthonormal basis $e_1, ..., e_m$ for M, the projection onto M along $M^{\perp}$ is given by:*

$$\mathrm{proj}_M(x) = (x|e_1)\, e_1 + \cdots + (x|e_m)\, e_m.$$

COROLLARY 22. *If V is finite dimensional and $M \subset V$ is a subspace, then*

$$\begin{aligned} V &= M \oplus M^{\perp}, \\ \left(M^{\perp}\right)^{\perp} &= M^{\perp\perp} = M, \\ \dim V &= \dim M + \dim M^{\perp}. \end{aligned}$$

Orthogonal projections can also be characterized as follows.

THEOREM 30. (Characterization of Orthogonal Projections) *Assume that V is a finite dimensional inner product space and $E : V \to V$ a projection on to $M \subset V$. Then the following conditions are equivalent.*

(1) $E = \mathrm{proj}_M$.
(2) $\mathrm{im}(E)^{\perp} = \ker(E)$.
(3) $\|E(x)\| \leq \|x\|$ *for all* $x \in V$.

PROOF. We have already seen that 1 and 2 are equivalent. These conditions imply 3 as $x = E(x) + (1-E)(x)$ is an orthogonal decomposition. So

$$\begin{aligned} \|x\|^2 &= \|E(x)\|^2 + \|(1-E)(x)\|^2 \\ &\geq \|E(x)\|^2. \end{aligned}$$

It remains to be seen that 3 implies that E is orthogonal. To prove this choose $x \in \ker(E)^{\perp}$ and observe that $E(x) = x - (1_V - E)(x)$ is an orthogonal decomposition since $(1_V - E)(z) \in \ker(E)$ for all $z \in V$. Thus

$$\begin{aligned} \|x\|^2 &\geq \|E(x)\|^2 \\ &= \|x - (1-E)(x)\|^2 \\ &= \|x\|^2 + \|(1-E)(x)\|^2 \\ &\geq \|x\|^2 \end{aligned}$$

This means that $(1_V - E)(x) = 0$ and hence $x = E(x) \in \mathrm{im}(E)$. Thus $\ker(E)^{\perp} \subset \mathrm{im}(E)$. We also know from the Dimension Formula that

$$\begin{aligned} \dim(\mathrm{im}(E)) &= \dim(V) - \dim(\ker(E)) \\ &= \dim\left(\ker(E)^{\perp}\right). \end{aligned}$$

This shows that $\ker(E)^{\perp} = \mathrm{im}(E)$. □

EXAMPLE 73. *Let* $V = \mathbb{R}^n$ *and* $M = \operatorname{span}\{(1,...,1)\}$. *Since* $\|(1,...,1)\|^2 = n$, *we see that*

$$\begin{aligned}
\operatorname{proj}_M(x) &= \operatorname{proj}_M\left(\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_1\end{bmatrix}\right)\\
&= \frac{1}{n}\left(\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_1\end{bmatrix}\middle|\begin{bmatrix}1\\ \vdots\\ 1\end{bmatrix}\right)\begin{bmatrix}1\\ \vdots\\ 1\end{bmatrix}\\
&= \frac{\alpha_1+\cdots+\alpha_n}{n}\begin{bmatrix}1\\ \vdots\\ 1\end{bmatrix}\\
&= \bar{\alpha}\begin{bmatrix}1\\ \vdots\\ 1\end{bmatrix},
\end{aligned}$$

where $\bar{\alpha}$ *is the* average *or* mean *of the values* $\alpha_1,...,\alpha_n$. *Since* $\operatorname{proj}_M(x)$ *is the closest element in* M *to* x *we get a geometric interpretation of the average of* $\alpha_1,...,\alpha_n$. *If in addition we use that* $\operatorname{proj}_M(x)$ *and* $x-\operatorname{proj}_M(x)$ *are perpendicular we arrive at a nice formula for the* variance*:*

$$\begin{aligned}
\|x-\operatorname{proj}_M(x)\|^2 &= \sum_{i=1}^n|\alpha_i-\bar{\alpha}|^2\\
&= \|x\|^2-\|\operatorname{proj}_M(x)\|^2\\
&= \sum_{i=1}^n|\alpha_i|^2-\sum_{i=1}^n|\bar{\alpha}|^2\\
&= \left(\sum_{i=1}^n|\alpha_i|^2\right)-n|\bar{\alpha}|^2\\
&= \left(\sum_{i=1}^n|\alpha_i|^2\right)-\frac{\left(\sum_{i=1}^n\alpha_i\right)^2}{n}
\end{aligned}$$

As above let $M \subset V$ be a finite dimensional subspace of an inner product space and $e_1,...,e_m$ an orthonormal basis for M. Using the formula

$$\begin{aligned}
\operatorname{proj}_M(x) &= (x|e_1)\,e_1+\cdots+(x|e_m)\,e_m\\
&= \alpha_1e_1+\cdots+\alpha_ne_m,
\end{aligned}$$

we see that the inequality $\|\operatorname{proj}_M(x)\| \leq \|x\|$ translates into the *Bessel inequality*

$$|\alpha_1|^2+\cdots+|\alpha_n|^2 \leq \|x\|^2.$$

This follows by observing that the map $\begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix} : \mathbb{F}^m \to M$ is an isometry and therefore

$$\begin{aligned}
\|x\|^2 &\geq \|\operatorname{proj}_M(x)\|^2\\
&= |\alpha_1|^2+\cdots+|\alpha_n|^2.
\end{aligned}$$

Note that when $m = 1$ this was the inequality used to establish the Cauchy-Schwarz inequality.

4.1. Exercises.

(1) Consider $\mathrm{Mat}_{n\times n}(\mathbb{C})$ with the inner product $(A|B) = \mathrm{tr}(AB^*)$. Describe the orthogonal complement to the space of all diagonal matrices.

(2) If $M = \mathrm{span}\{z_1, ..., z_m\}$, then
$$M^\perp = \{x \in V : (x|z_1) = \cdots = (x|z_m) = 0\}$$

(3) Assume $V = M \oplus M^\perp$, show that
$$x = \mathrm{proj}_M(x) + \mathrm{proj}_{M^\perp}(x)$$

(4) Find the element in $\mathrm{span}\{1, \cos t, \sin t\}$ that is closest to $\sin^2 t$.

(5) Assume $V = M \oplus M^\perp$ and that $L : V \to V$ is a linear operator. Show that both M and $M^\perp$ are L invariant if and only if $\mathrm{proj}_M \circ L = L \circ \mathrm{proj}_M$.

(6) Let $A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$.
   (a) Show that the row vectors of A are in the orthogonal complement of $\ker(A)$.
   (b) Use this to show that the row rank and column rank of A are the same.

(7) Let $M, N \subset V$ be subspaces of a finite dimensional inner product space. Show that
$$\begin{aligned}(M+N)^\perp &= M^\perp \cap N^\perp,\\ (M \cap N)^\perp &= M^\perp + N^\perp.\end{aligned}$$

(8) Find the orthogonal projection onto $\mathrm{span}\{(2,-1,1), (1,-1,0)\}$ by first computing the orthogonal projection onto the orthogonal complement.

(9) Find the polynomial $p(t) \in P_2$ such that
$$\int_0^{2\pi} |p(t) - \cos t|^2 \, dt$$
is smallest possible.

(10) Show that the decomposition into even and odd functions on $C^0([-a,a], \mathbb{C})$ is orthogonal if we use the inner product
$$(f|g) = \int_{-a}^{a} f(t)\overline{g(t)}dt.$$

(11) Find the orthogonal projection from $\mathbb{C}[t]$ onto $\mathrm{span}\{1, t\} = P_1$. Given any $p \in \mathbb{C}[t]$ you should express the orthogonal projection in terms of the coefficients of p.

(12) Find the orthogonal projection from $\mathbb{C}[t]$ onto $\mathrm{span}\{1, t, t^2\} = P_2$.

(13) Compute the orthogonal projection onto the following subspaces:
   (a) $\mathrm{span}\left\{\begin{bmatrix}1\\1\\1\\1\end{bmatrix}\right\}$
   (b) $\mathrm{span}\left\{\begin{bmatrix}1\\-1\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\\0\end{bmatrix}, \begin{bmatrix}2\\0\\1\\1\end{bmatrix}\right\}$

(c) span $\left\{ \begin{bmatrix} 1 \\ i \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -i \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ i \\ 0 \end{bmatrix} \right\}$

(14) *(Selberg)* Let $x, y_1, ..., y_n \in V$, where V is an inner product space. Show Selberg's "generalization" of Bessel's inequality

$$\sum_{i=1}^{n} |(x|y_i)|^2 \leq \|x\|^2 \sum_{i,j=1}^{n} |(y_i|y_j)|$$

5. Adjoint Maps

To introduce the concept of *adjoints* of linear maps we start with the construction for matrices, i.e., linear maps $A : \mathbb{F}^m \to \mathbb{F}^n$, where $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ and $\mathbb{F}^m, \mathbb{F}^n$ are equipped with their standard inner products. We can write A as an $n \times m$ matrix and we define the adjoint $A^* = \bar{A}^t$, i.e., A^* is the transposed and conjugate of A. In case $\mathbb{F} = \mathbb{R}$, conjugation is irrelevant so $A^* = A^t$. Note that since A^* is an $m \times n$ matrix it corresponds to a linear map $A^* : \mathbb{F}^n \to \mathbb{F}^m$. The adjoint satisfies the crucial property

$$(Ax|y) = (x|A^*y) .$$

To see this we simply think of x as an $m \times 1$ matrix, y as an $n \times 1$ matrix and then observe that

$$\begin{aligned} (Ax|y) &= (Ax)^t \bar{y} \\ &= x^t A^t \bar{y} \\ &= x^t \overline{\left(\bar{A}^t y\right)} \\ &= (x|A^*y) . \end{aligned}$$

In the general case of a linear map $L : V \to W$ we can try to define the adjoint through matrix representations. To this end select orthonormal bases for V and W so that we have a diagram

$$\begin{array}{ccc} V & \xrightarrow{L} & W \\ \updownarrow & & \updownarrow \\ \mathbb{F}^m & \xrightarrow{[L]} & \mathbb{F}^n \end{array}$$

where the vertical double-arrows are isometries. Then define $L^* : W \to V$ as the linear map whose matrix representation is $[L]^*$. In other words $[L^*] = [L]^*$ and the following diagram commutes

$$\begin{array}{ccc} V & \xleftarrow{L^*} & W \\ \updownarrow & & \updownarrow \\ \mathbb{F}^m & \xleftarrow{[L]^*} & \mathbb{F}^n \end{array}$$

Because the vertical arrows are isometries we also have

$$(Lx|y) = (x|L^*y) .$$

There is a similar construction of L^* that uses only a basis for $e_1, ..., e_m$ for V. To define $L^*(y)$ we need to know the inner products $(L^*y|e_j)$. The relationship

$(Lx|y) = (x|L^*y)$ indicates that $(L^*y|e_j)$ can be calculated as

$$\begin{aligned}(L^*y|e_j) &= \overline{(e_j|L^*y)} \\ &= \overline{(Le_j|y)} \\ &= (y|Le_j).\end{aligned}$$

So let us define

$$L^*y = \sum_{j=1}^{m} (y|Le_j)\, e_j.$$

This clearly defines a linear map $L^* : W \to V$ satisfying

$$(Le_j|y) = (e_j|L^*y).$$

The more general condition

$$(Lx|y) = (x|L^*y)$$

follows immediately by writing x as a linear combination of $e_1, ..., e_m$ and using linearity in x on both sides of the equation.

Next we address the issue of whether the adjoint is uniquely defined, i.e., could there be two linear maps $K_i : W \to V$, $i = 1, 2$ such that

$$(x|K_1y) = (Lx|y) = (x|K_2y)?$$

This would imply

$$\begin{aligned}0 &= (x|K_1y) - (x|K_2y) \\ &= (x|K_1y - K_2y).\end{aligned}$$

If $x = K_1y - K_2y$, then

$$||K_1y - K_2y||^2 = 0$$

and hence $K_1y = K_2y$.

The adjoint has the following useful elementary properties.

Proposition 21. *Let $L, K : V \to W$ and $L_1 : V_1 \to V_2$, $L_2 : V_2 \to V_3$, then*

(1) $(L + K)^* = L^* + K^*$.
(2) $L^{**} = L$
(3) $(\lambda 1_V)^* = \bar{\lambda} 1_V$.
(4) $(L_2 L_1)^* = L_1^* L_2^*$.
(5) *If L is invertible, then* $\left(L^{-1}\right)^* = (L^*)^{-1}$.

Proof. The key observation for the proofs of these properties is that any $L' : W \to V$ with the property that $(Lx|y) = (x|L'y)$ for all x must satisfy $L'y = L^*y$.

To check the first property we calculate

$$\begin{aligned}\left(x|\,(L+K)^*\, y\right) &= ((L+K)\, x|y) \\ &= (Lx|y) + (Kx|y) \\ &= (x|L^*y) + (x|K^*y) \\ &= (x|\,(L^* + K^*)\, y).\end{aligned}$$

The second is immediate from

$$\begin{aligned}(Lx|y) &= (x|L^*y) \\ &= \overline{(L^*y|x)} \\ &= \overline{(y|L^{**}x)} \\ &= (L^{**}x|y).\end{aligned}$$

The third property follows from

$$\begin{aligned}(\lambda 1_V(x)|y) &= (\lambda x|y) \\ &= \left(x|\bar{\lambda}y\right) \\ &= \left(x|\bar{\lambda}1_V(y)\right).\end{aligned}$$

The fourth property

$$\begin{aligned}\left(x|(L_2L_1)^* y\right) &= ((L_2L_1)(x)|z) \\ &= (L_2(L_1(x))|z) \\ &= (L_1(x)|L_2^*(z)) \\ &= (x|L_1^*(L_2^*(z))) \\ &= (x|(L_1^*L_2^*)(z)).\end{aligned}$$

And finally $1_V = L^{-1}L$ implies that

$$\begin{aligned}1_V &= (1_V)^* \\ &= \left(L^{-1}L\right)^* \\ &= L^*\left(L^{-1}\right)^*\end{aligned}$$

as desired. □

Example 74. *As an example let us find the adjoint to*

$$\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} : \mathbb{F}^n \to V,$$

when $e_1, ..., e_n$ is an orthonormal basis. Recall that we have already found a simple formula for the inverse

$$\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^{-1}(x) = \begin{bmatrix} (x|e_1) \\ \vdots \\ (x|e_n) \end{bmatrix}$$

and we proved that $\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}$ preserves inner products. If we let $x \in \mathbb{F}^n$ and $y \in V$, then we can write $y = \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}(z)$ for some $z \in \mathbb{F}^n$. With that in mind we can calculate

$$\begin{aligned}\left(\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}(x)|y\right) &= \left(\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}(x)|\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}(z)\right) \\ &= (x|z) \\ &= \left(x|\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^{-1}(y)\right).\end{aligned}$$

Thus we have

$$\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^* = \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^{-1}.$$

Below we shall generalize this relationship to all isomorphisms that preserve inner products.

This relationship simplifies the job of calculating matrix representations with respect to orthonormal bases. Assume that $L : V \to W$ is a linear map between finite dimensional inner product spaces and that we have orthonormal bases $e_1, ..., e_m$ for V and $f_1, ..., f_n$ for W. Then

$$\begin{aligned} L &= \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} [L] \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix}^*, \\ [L] &= \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix} L \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix}^*. \end{aligned}$$

or in diagram form

$$\begin{array}{ccc} V & \xrightarrow{L} & W \\ \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix}^* \downarrow & & \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} \uparrow \\ \mathbb{F}^m & \xrightarrow{[L]} & \mathbb{F}^n \end{array}$$

$$\begin{array}{ccc} V & \xrightarrow{L} & W \\ \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix} \uparrow & & \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix}^* \downarrow \\ \mathbb{F}^m & \xrightarrow{[L]} & \mathbb{F}^n \end{array}$$

From this we see that the matrix definition of the adjoint is justified since the properties of the adjoint now tell us that:

$$\begin{aligned} L^* &= \left(\begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} [L] \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix}^* \right)^* \\ &= \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix} [L]^* \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix}^*. \end{aligned}$$

A linear map and its adjoint have some remarkable relationships between their images and kernels. These properties are called the *Fredholm alternatives* and named after Fredholm who first used these properties to clarify when certain linear systems $L(x) = b$ can be solved.

THEOREM 31. (The Fredholm Alternative) *Let $L : V \to W$ be a linear map between finite dimensional inner product spaces. Then*

$$\begin{aligned} \ker(L) &= \operatorname{im}(L^*)^{\perp}, \\ \ker(L^*) &= \operatorname{im}(L)^{\perp}, \\ \ker(L)^{\perp} &= \operatorname{im}(L^*), \\ \ker(L^*)^{\perp} &= \operatorname{im}(L). \end{aligned}$$

PROOF. Since $L^{**} = L$ and $M^{\perp\perp} = M$ we see that all of the four statements are equivalent to each other. Thus we need only prove the first. The two subspaces are characterized by

$$\begin{aligned} \ker(L) &= \{x \in V : Lx = 0\}, \\ \operatorname{im}(L^*)^{\perp} &= \{x \in V : (x|L^*z) = 0 \text{ for all } z \in W\}. \end{aligned}$$

Now fix $x \in V$ and use that $(Lx|z) = (x|L^*z)$ for all $z \in V$. This implies first that if $x \in \ker(L)$, then also $x \in \operatorname{im}(L^*)^{\perp}$. Conversely, if $0 = (x|L^*z) = (Lx|z)$ for all $z \in W$ it must follow that $Lx = 0$ and hence $x \in \ker(L)$. □

COROLLARY 23. (The Rank Theorem) *Let $L : V \to W$ be a linear map between finite dimensional inner product spaces. Then*

$$\operatorname{rank}(L) = \operatorname{rank}(L^*).$$

PROOF. Using The Dimension formula for linear maps and that orthogonal complements have complementary dimension together with the Fredholm alternative we see

$$\begin{aligned}\dim V &= \dim(\ker(L)) + \dim(\operatorname{im}(L)) \\ &= \dim(\operatorname{im}(L^*))^{\perp} + \dim(\operatorname{im}(L)) \\ &= \dim V - \dim(\operatorname{im}(L^*)) + \dim(\operatorname{im}(L)).\end{aligned}$$

This implies the result. □

COROLLARY 24. *For a real or complex $n \times m$ matrix A the column rank equals the row rank.*

PROOF. First note that $\operatorname{rank}(B) = \operatorname{rank}(\bar{B})$ for all complex matrices B. Secondly, we know that $\operatorname{rank}(A)$ is the same as the column rank. Thus $\operatorname{rank}(A^*)$ is the row rank of $\bar{A}$. This proves the result. □

COROLLARY 25. *Let $L : V \to V$ be a linear operator on a finite dimensional inner product space. Then λ is an eigenvalue for L if and only if $\bar{\lambda}$ is an eigenvalue for L^*. Moreover these eigenvalue pairs have the same geometric multiplicity:*

$$\dim(\ker(L - \lambda 1_V)) = \dim\left(\ker\left(L^* - \bar{\lambda} 1_V\right)\right).$$

PROOF. Note that $(L - \lambda 1_V)^* = L^* - \bar{\lambda} 1_V$. Thus the result follows if we can show

$$\dim(\ker(K)) = \dim(\ker(K^*))$$

for $K : V \to V$. This comes from

$$\begin{aligned}\dim(\ker(K)) &= \dim V - \dim(\operatorname{im}(K)) \\ &= \dim V - \dim(\operatorname{im}(K^*)) \\ &= \dim(\ker(K^*)).\end{aligned}$$

□

5.1. Exercises.

(1) Let V and W be finite dimensional inner product spaces.
   (a) Show that we can define an inner product on $\hom_{\mathbb{F}}(V, W)$ by $(L|K) = \operatorname{tr}(LK^*) = \operatorname{tr}(K^*L)$.
   (b) Show that $(K|L) = (L^*|K^*)$.
   (c) If $e_1, ..., e_m$ is an orthonormal basis for V show that

$$(K|L) = (K(e_1)|L(e_1)) + \cdots + (K(e_m)|L(e_m)).$$

(2) Assume that V is a complex inner product space. Recall from the exercises to "Vector Spaces" in chapter 1 that we have a vector space V^* with the same addition as in V but scalar multiplication is altered by conjugating the scalar. Show that the map $F : V^* \to \hom(V, \mathbb{C})$ defined by $F(x) = (\cdot|x)$ is complex linear and an isomorphism when V is finite dimensional. Use this to give another definition of the adjoint. Here

$$f = (\cdot|x) \in \hom(V, \mathbb{C})$$

is the linear map such that $f(z) = (z|x)$.

(3) On $\mathrm{Mat}_{n\times n}(\mathbb{C})$ use the inner product $(A|B) = \mathrm{tr}(AB^*)$. For $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ consider the two linear operators on $\mathrm{Mat}_{n\times n}(\mathbb{C})$ defined by $L_A(X) = AX$, $R_A(X) = XA$. Show that $(L_A)^* = L_{A^*}$ and $(R_A)^* = R_{A^*}$.

(4) Let $x_1, ..., x_k \in V$, where V is a finite dimensional inner product space.
   (a) Show that
$$G(x_1, ..., x_k) = \begin{bmatrix} x_1 & \cdots & x_k \end{bmatrix}^* \begin{bmatrix} x_1 & \cdots & x_k \end{bmatrix}$$
   where $G(x_1, ..., x_k)$ is a $k \times k$ matrix whose ij entry is $(x_j|x_i)$. It is called the Gram matrix or Grammian.
   (b) Show that $G = G(x_1, ..., x_k)$ is positive definite in the sense that $(Gx|x) \geq 0$ for all $x \in \mathbb{F}^k$.

(5) Find image and kernel for $A \in \mathrm{Mat}_{3\times 3}(\mathbb{R})$ where the ij entry is $\alpha_{ij} = (-1)^{i+j}$.

(6) Find image and kernel for $A \in \mathrm{Mat}_{3\times 3}(\mathbb{C})$ where the kl entry is $\alpha_{kl} = (i)^{k+l}$.

(7) Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ be symmetric, i.e., $A^* = A$, and assume A has rank $k \leq n$.
   (a) If the first k columns are linearly independent then the principal $k\times k$ minor of A is invertible. The principal $k \times k$ minor of A is the $k \times k$ matrix one obtains by deleting the last $n-k$ columns and rows. Hint: use a block decomposition
$$A = \begin{bmatrix} B & C \\ C^t & D \end{bmatrix}$$
   and write
$$\begin{bmatrix} C \\ D \end{bmatrix} = \begin{bmatrix} B \\ C^t \end{bmatrix} X, \ X \in \mathrm{Mat}_{k\times(n-k)}(\mathbb{R})$$
   i.e., the last $n-k$ columns are linear combinations of the first k.
   (b) If rows $i_1, ..., i_k$ are linearly independent, then the $k \times k$ minor obtained by deleting all columns and rows not indexed by $i_1, ..., i_k$ is invertible. Hint: Note that $I_{kl}AI_{kl}$ is symmetric so one can use part a.
   (c) Give examples showing that a. need not hold for $n \times n$ matrices in general.

(8) Let $L : V \to V$ be a linear operator on a finite dimensional inner product space.
   (a) If $M \subset V$ is an L invariant subspace, then $M^\perp$ is L^* invariant.
   (b) If $M \subset V$ is an L invariant subspace, then
$$(L|_M)^* = \mathrm{proj}_M \circ L^*|_M.$$
   (c) Give an example where M is not L^* invariant.

(9) Let $L : V \to W$ be a linear operator between finite dimensional vector spaces. Show that
   (a) L is one-to-one if and only if L^* is onto.
   (b) L^* is one-to-one if and only if L is onto.

(10) Let $M, N \subset V$ be subspaces of a finite dimensional inner product space and consider $L : M \times N \to V$ defined by $L(x, y) = x - y$.
   (a) Show that $L^*(z) = (\mathrm{proj}_M(z), -\mathrm{proj}_N(z))$.

(b) Show that

$$\begin{aligned}\ker(L^*) &= M^\perp \cap N^\perp,\\ \operatorname{im}(L) &= M + N.\end{aligned}$$

(c) Using the Fredholm alternative show that

$$(M+N)^\perp = M^\perp \cap N^\perp.$$

(d) Replace M and N by $M^\perp$ and $N^\perp$ and conclude

$$(M \cap N)^\perp = M^\perp + N^\perp.$$

(11) Assume that $L : V \to W$ is a linear map between inner product spaces.

(a) Show that

$$\dim(\ker(L)) - \dim(\operatorname{im}(L))^\perp = \dim V - \dim W.$$

(b) If $V = W = \ell^2(\mathbb{Z})$ then for each integer $n \in \mathbb{Z}$ it is possible to find a linear operator L_n with finite dimensional $\ker(L_n)$ and $(\operatorname{im}(L_n))^\perp$ so that

$$\operatorname{Ind}(L) = \dim(\ker(L)) - \dim(\operatorname{im}(L))^\perp = n.$$

Hint: Consider linear maps that take (a_k) to (a_{k+l}) for some $l \in \mathbb{Z}$. An operator with finite dimensional $\ker(L)$ and $(\operatorname{im}(L))^\perp$ is called a *Fredholm operator*. The integer $\operatorname{Ind}(L) = \dim(\ker(L)) - \dim(\operatorname{im}(L))^\perp$ is the *index* of the operator and is an important invariant in functional analysis.

(12) Let $L : V \to V$ be an operator on a finite dimensional inner product space. Show that

$$\overline{\operatorname{tr}(L)} = \operatorname{tr}(L^*).$$

(13) Let $L : V \to W$ be a linear map between inner product spaces. Show that

$$L : \ker(L^*L - \lambda 1_V) \to \ker(LL^* - \lambda 1_V)$$

and

$$L^* : \ker(LL^* - \lambda 1_V) \to \ker(L^*L - \lambda 1_V).$$

(14) Let $L : V \to V$ be a linear operator on a finite dimensional inner product space. If $L(x) = \lambda x$, $L^*(y) = \mu y$, and $\lambda \neq \bar{\mu}$, then x and y are perpendicular.

(15) Let V be a subspace of $C^0([0,1], \mathbb{R})$ and consider the linear functionals $f_{t_0}(x) = x(t_0)$ and

$$f_y(x) = \int_0^1 x(t)\, y(t)\, dt.$$

(a) If V is finite dimensional show that $f_{t_0}|_V = f_y|_V$ for some $y \in V$.

(b) If $V = P_2$ = polynomials of degree ≤ 2, then find an explicit $y \in V$ as in part a.

(c) If $V = C^0([0,1], \mathbb{R})$, show that it is not possible to find $y \in C^0([0,1], \mathbb{R})$ such that $f_{t_0} = f_y$. The illusory function δ_{t_0} invented by Dirac to solve this problem is called Dirac's δ-function. It is defined as

$$\delta_{t_0}(t) = \begin{cases} 0 & \text{if } t \neq t_0 \\ \infty & \text{if } t = t_0 \end{cases}$$

so as to give the impression that

$$\int_0^1 x(t)\,\delta_{t_0}(t)\,dt = x(t_0).$$

(16) Find $q(t) \in P_2$ such that

$$p(5) = (p|q) = \int_0^1 p(t)\,\overline{q(t)}dt$$

for all $p \in P_2$.

(17) Find $f(t) \in \operatorname{span}\{1, \sin(t), \cos(t)\}$ such that

$$\begin{aligned}(g|f) &= \frac{1}{2\pi}\int_0^{2\pi} g(t)\,\overline{f(t)}dt \\ &= \frac{1}{2\pi}\int_0^{2\pi} g(t)\left(1+t^2\right)dt\end{aligned}$$

for all $g \in \operatorname{span}\{1, \sin(t), \cos(t)\}$.

6. Orthogonal Projections Revisited*

In this section we shall give a new formula for an orthogonal projection. Instead of using Gram-Schmidt to create an orthonormal basis for the subspace it gives a direct formula using an arbitrary basis for the subspace.

First we need a new characterization of orthogonal projections using adjoints.

Lemma 20. (Characterization of Orthogonal Projections) *A projection $E : V \to V$ is orthogonal if and only if $E = E^*$.*

Proof. The Fredholm alternative tells us that $\operatorname{im}(E) = \ker(E^*)^{\perp}$ so if $E = E^*$ we have shown that $\operatorname{im}(E) = \ker(E)^{\perp}$, which implies that E is orthogonal.

Conversely we can assume that $\operatorname{im}(E) = \ker(E)^{\perp}$ since E is an orthogonal projection. Using the Fredholm alternative again then tells us that

$$\begin{aligned}\operatorname{im}(E) &= \ker(E)^{\perp} = \operatorname{im}(E^*), \\ \ker(E^*)^{\perp} &= \operatorname{im}(E) = \ker(E)^{\perp}.\end{aligned}$$

As $(E^*)^2 = \left(E^2\right)^* = E^*$ it follows that E^* is a projection with the same image and kernel as E. Hence $E = E^*$. □

Using this characterization of orthogonal projections it is possible find a formula for proj_M using a general basis for $M \subset V$. Let $M \subset V$ be finite dimensional with a basis $x_1, ..., x_m$. This yields an isomorphism

$$\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} : \mathbb{F}^m \to M$$

which can also be thought of as a one-to-one map $A : \mathbb{F}^m \to V$ whose image is M. This yields a linear map

$$A^*A : \mathbb{F}^m \to \mathbb{F}^m.$$

Since

$$\begin{aligned}(A^*Ay|y) &= (Ay|Ay) \\ &= \|Ay\|^2\end{aligned}$$

the kernel satisfies

$$\ker(A^*A) = \ker(A) = \{0\}.$$

In particular, A^*A is an isomorphism. This means that

$$E = A\left(A^*A\right)^{-1}A^*.$$

defines linear operator $E : V \to V$. It is easy to check that $E = E^*$ and since

$$\begin{aligned} E^2 &= A\left(A^*A\right)^{-1}A^*A\left(A^*A\right)^{-1}A^* \\ &= A\left(A^*A\right)^{-1}A^* \\ &= E, \end{aligned}$$

it is a projection. Finally we must check that $\operatorname{im}(E) = M$. Since $\left(A^*A\right)^{-1}$ is an isomorphism and

$$\operatorname{im}(A^*) = (\ker(A))^{\perp} = (\{0\})^{\perp} = \mathbb{F}^m,$$

we have

$$\operatorname{im}(E) = \operatorname{im}(A) = M$$

as desired.

To better understand this construction we note that

$$A^*(x) = \begin{bmatrix} (x|x_1) \\ \vdots \\ (x|x_m) \end{bmatrix}.$$

This follows from

$$\begin{aligned} \left(\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} \middle| \begin{bmatrix} (x|x_1) \\ \vdots \\ (x|x_m) \end{bmatrix}\right) &= \alpha_1\overline{(x|x_1)} + \cdots + \alpha_m\overline{(x|x_m)} \\ &= \alpha_1(x_1|x) + \cdots + \alpha_m(x_m|x) \\ &= (\alpha_1x_1 + \cdots + \alpha_mx_m|x) \\ &= \left(A\left(\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}\right) \middle| x\right) \end{aligned}$$

The matrix form of A^*A can now be calculated

$$\begin{aligned} A^*A &= A^* \circ \begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \\ &= \begin{bmatrix} A^*(x_1) & \cdots & A^*(x_m) \end{bmatrix} \\ &= \begin{bmatrix} (x_1|x_1) & \cdots & (x_m|x_1) \\ \vdots & \ddots & \vdots \\ (x_1|x_m) & \cdots & (x_m|x_m) \end{bmatrix}. \end{aligned}$$

This is also called the *Gram matrix* of $x_1, ..., x_m$. This information specifies explicitly all of the components of the formula

$$E = A\left(A^*A\right)^{-1}A^*.$$

The only hard calculation is the inversion of A^*A. The calculation of $A\left(A^*A\right)^{-1}A^*$ should also be compared to using the Gram-Schmidt procedure for finding the orthogonal projection onto M.

6.1. Exercises.

(1) Using the inner product $\int_0^1 p(t)\bar{q}(t)\,dt$ find the orthogonal projection from $\mathbb{C}[t]$ onto $\mathrm{span}\{1,t\} = P_1$. Given any $p \in \mathbb{C}[t]$ you should express the orthogonal projection in terms of the coefficients of p.

(2) Using the inner product $\int_0^1 p(t)\bar{q}(t)\,dt$ find the orthogonal projection from $\mathbb{C}[t]$ onto $\mathrm{span}\left\{1,t,t^2\right\} = P_2$.

(3) Compute the orthogonal projection onto the following subspaces:

(a) $\mathrm{span}\left\{\begin{bmatrix}1\\1\\1\\1\end{bmatrix}\right\}$

(b) $\mathrm{span}\left\{\begin{bmatrix}1\\-1\\0\\1\end{bmatrix},\begin{bmatrix}1\\1\\1\\0\end{bmatrix},\begin{bmatrix}2\\0\\1\\1\end{bmatrix}\right\}$

(c) $\mathrm{span}\left\{\begin{bmatrix}1\\i\\0\\0\end{bmatrix},\begin{bmatrix}-i\\1\\0\\0\end{bmatrix},\begin{bmatrix}0\\1\\i\\0\end{bmatrix}\right\}$

(4) Given an orthonormal basis $e_1,\dots,e_k$ for the subspace $M \subset V$, show that the orthorgonal projection onto M can be computed as

$$\mathrm{proj}_M = \begin{bmatrix} e_1 & \cdots & e_k \end{bmatrix}\begin{bmatrix} e_1 & \cdots & e_k \end{bmatrix}^*.$$

Hint: Show that

$$\begin{bmatrix} e_1 & \cdots & e_k \end{bmatrix}^*\begin{bmatrix} e_1 & \cdots & e_k \end{bmatrix} = 1_{\mathbb{F}^k}.$$

7. Matrix Exponentials*

In this section we shall show that the initial value problem: $\dot{x} = Ax$, $x(t_0) = x_0$ where A is a square matrix with complex (or real) scalars as entries can be solved using matrix exponentials. Recall that more algebraic approaches are also available by using the Frobenius canonical form, the Jordan canonical form, and later in chapter 4 in "Triagulability" Schur's theorem will give us a very effectiveway of solving such systems.

Recall that in the one dimensional situation the solution is $x = x_0\exp(A(t-t_0))$. If we could make sense of this for square matrices A as well we would have a possible way of writing down the solutions. The concept of operator norms introduced in "Orthonormal Bases" naturally leads to a norm of matrices as well. One key observation about this norm is that if $A = [\alpha_{ij}]$, then $|\alpha_{ij}| \leq ||A||$, i.e., the entries are bounded by the norm. Moreover we also have that

$$\begin{aligned} \|AB\| &\leq \|A\|\,\|B\|, \\ \|A+B\| &\leq \|A\| + \|B\| \end{aligned}$$

as

$$\begin{aligned} \|AB(x)\| &\leq \|A\|\,\|B(x)\| \\ &\leq \|A\|\,\|B\|\,\|x\|, \end{aligned}$$

$$\|(A+B)(x)\| \leq \|A(x)\| + \|B(x)\|.$$

Now consider the series

$$\sum_{n=0}^{\infty} \frac{A^n}{n!}.$$

Since

$$\left\| \frac{A^n}{n!} \right\| \leq \frac{\|A\|^n}{n!},$$

and

$$\sum_{n=0}^{\infty} \frac{\|A\|^n}{n!}$$

is convergent it follows that any given entry in

$$\sum_{n=0}^{\infty} \frac{A^n}{n!}$$

is bounded by a convergent series. Thus the matrix series also converges leading us to define

$$\exp(A) = \sum_{n=0}^{\infty} \frac{A^n}{n!}.$$

It is not hard to check that if $L \in \hom(V, V)$, where V is a finite dimensional inner product space, then we can similarily define

$$\exp(L) = \sum_{n=0}^{\infty} \frac{L^n}{n!}.$$

Now consider the matrix valued function

$$\exp(At) = \sum_{n=0}^{\infty} \frac{A^n t^n}{n!}$$

and with it the vector valued function

$$x(t) = \exp(A(t - t_0)) x_0.$$

It still remains to be seen that this defines a differentiable function that solves $\dot{x} = Ax$. At least we have the correct initial value as $\exp(0) = 1_{\mathbb{F}^n}$ from our formula. To check differentiability we consider the matrix function $t \to \exp(At)$ and study $\exp(A(t+h))$. In fact we claim that

$$\exp(A(t+h)) = \exp(At)\exp(Ah).$$

To establish this we prove a more general version together with another useful fact.

Proposition 22. *Let $L, K : V \to V$ be linear operators on a finite dimensional inner product space.*

(1) *If $KL = LK$, then* $\exp(K+L) = \exp(K) \circ \exp(L)$.
(2) *If K is invertible, then* $\exp\left(K \circ L \circ K^{-1}\right) = K \circ \exp(L) \circ K^{-1}$.

Proof. 1. This formula hinges on proving the binomial formula for commuting operators:

$$\begin{aligned} (L+K)^n &= \sum_{k=0}^{n} \binom{n}{k} L^k K^{n-k}, \\ \binom{n}{k} &= \frac{n!}{(n-k)!k!} \end{aligned}$$

This formula is obvious for $n = 1$. Suppose that the formula holds for n. Using the conventions

$$\begin{aligned} \binom{n}{n+1} &= 0, \\ \binom{n}{-1} &= 0, \end{aligned}$$

together with the formula from Pascal's triangle

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k},$$

it follows that

$$\begin{aligned} (L+K)^{n+1} &= (L+K)^n (L+K) \\ &= \left(\sum_{k=0}^{n} \binom{n}{k} L^k K^{n-k}\right)(L+K) \\ &= \sum_{k=0}^{n} \binom{n}{k} L^k K^{n-k} L + \sum_{k=0}^{n} \binom{n}{k} L^k K^{n-k} K \\ &= \sum_{k=0}^{n} \binom{n}{k} L^{k+1} K^{n-k} + \sum_{k=0}^{n} \binom{n}{k} L^k K^{n-k+1} \\ &= \sum_{k=0}^{n+1} \binom{n}{k-1} L^k K^{n+1-k} + \sum_{k=0}^{n+1} \binom{n}{k} L^k K^{n+1-k} \\ &= \sum_{k=0}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k}\right) L^k K^{n+1-k} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} L^k K^{n+1-k}. \end{aligned}$$

We can then compute

$$\begin{aligned} \sum_{n=0}^{N} \frac{(K+L)^n}{n!} &= \sum_{n=0}^{N} \sum_{k=0}^{n} \frac{1}{n!} \binom{n}{k} L^k K^{n-k} \\ &= \sum_{n=0}^{N} \sum_{k=0}^{n} \frac{1}{(n-k)!k!} L^k K^{n-k} \\ &= \sum_{n=0}^{N} \sum_{k=0}^{n} \left(\frac{1}{k!} L^k\right) \left(\frac{1}{(n-k)!} K^{n-k}\right) \\ &= \sum_{k,l=0,k+l\leq N}^{N} \left(\frac{1}{k!} L^k\right) \left(\frac{1}{l!} K^l\right) \end{aligned}$$

The last term is unfortunately not quite the same as the product

$$\sum_{k,l=0}^{N} \left(\frac{1}{k!} L^k\right) \left(\frac{1}{l!} K^l\right) = \left(\sum_{k=0}^{N} \frac{1}{k!} L^k\right) \left(\sum_{l=0}^{N} \frac{1}{l!} K^l\right),$$

However the difference between these two sums can be estimated the following way:

$$\begin{aligned}
& \left\| \sum_{k,l=0}^{N} \left(\frac{1}{k!}L^k\right)\left(\frac{1}{l!}K^l\right) - \sum_{k,l=0,k+l\leq N}^{N} \left(\frac{1}{k!}L^k\right)\left(\frac{1}{l!}K^l\right) \right\| \\
= & \left\| \sum_{k,l=0,k+l>N}^{N} \left(\frac{1}{k!}L^k\right)\left(\frac{1}{l!}K^l\right) \right\| \\
\leq & \sum_{k,l=0,k+l>N}^{N} \left(\frac{1}{k!}\|L\|^k\right)\left(\frac{1}{l!}\|K\|^l\right) \\
\leq & \sum_{k=0,l=N/2}^{N} \left(\frac{1}{k!}\|L\|^k\right)\left(\frac{1}{l!}\|K\|^l\right) + \sum_{l=0,k=N/2}^{N} \left(\frac{1}{k!}\|L\|^k\right)\left(\frac{1}{l!}\|K\|^l\right) \\
= & \left(\sum_{k=0}^{N}\frac{1}{k!}\|L\|^k\right)\left(\sum_{l=N/2}^{N}\frac{1}{l!}\|K\|^l\right) + \left(\sum_{k=N/2}^{N}\frac{1}{k!}\|L\|^k\right)\left(\sum_{l=0}^{N}\frac{1}{l!}\|K\|^l\right) \\
\leq & \exp\left(\|L\|\right)\left(\sum_{l=N/2}^{N}\frac{1}{l!}\|K\|^l\right) + \exp\left(\|K\|\right)\left(\sum_{k=N/2}^{N}\frac{1}{k!}\|L\|^k\right).
\end{aligned}$$

Since

$$\begin{aligned}
\lim_{N\to\infty}\sum_{l=N/2}^{N}\frac{1}{l!}\|K\|^l &= 0, \\
\lim_{N\to\infty}\sum_{k=N/2}^{N}\frac{1}{k!}\|L\|^k &= 0
\end{aligned}$$

it follows that

$$\lim_{N\to\infty}\left\|\sum_{n=0}^{N}\frac{(K+L)^n}{n!} - \left(\sum_{k=0}^{N}\frac{1}{k!}L^k\right)\left(\sum_{l=0}^{N}\frac{1}{l!}K^l\right)\right\| = 0.$$

Thus

$$\sum_{n=0}^{\infty}\frac{(K+L)^n}{n!} = \sum_{k=0}^{\infty}\left(\frac{1}{k!}L^k\right)\sum_{l=0}^{\infty}\left(\frac{1}{l!}K^l\right)$$

as desired.

2. This is considerably simpler and uses that

$$\left(K\circ L\circ K^{-1}\right)^n = K\circ L^n\circ K^{-1}.$$

This is again proven by induction. First observe it is trivial for $n=1$ and then that

$$\begin{aligned}
\left(K\circ L\circ K^{-1}\right)^{n+1} &= \left(K\circ L\circ K^{-1}\right)^n\circ K\circ L\circ K^{-1} \\
&= K\circ L^n\circ K^{-1}\circ K\circ L\circ K^{-1} \\
&= K\circ L^n\circ L\circ K^{-1} \\
&= K\circ L^{n+1}\circ K^{-1}.
\end{aligned}$$

Thus

$$\begin{aligned}\sum_{n=0}^{N}\frac{\left(K\circ L\circ K^{-1}\right)^{n}}{n!} &= \sum_{n=0}^{N}\frac{K\circ L^{n}\circ K^{-1}}{n!}\\ &= K\circ\left(\sum_{n=0}^{N}\frac{L^{n}}{n!}\right)\circ K^{-1}.\end{aligned}$$

By letting $N\to\infty$ we get the desired formula. □

To calculate the derivative of $\exp(At)$ we observe that

$$\begin{aligned}\frac{\exp(A(t+h))-\exp(At)}{h} &= \frac{\exp(Ah)\exp(At)-\exp(At)}{h}\\ &= \left(\frac{\exp(Ah)-1_{\mathbb{F}^n}}{h}\right)\exp(At).\end{aligned}$$

Using the definition of $\exp(Ah)$ it follows that

$$\begin{aligned}\frac{\exp(Ah)-1_{\mathbb{F}^n}}{h} &= \sum_{n=1}^{\infty}\frac{1}{h}\frac{A^{n}h^{n}}{n!}\\ &= \sum_{n=1}^{\infty}\frac{A^{n}h^{n-1}}{n!}\\ &= A+\sum_{n=2}^{\infty}\frac{A^{n}h^{n-1}}{n!}.\end{aligned}$$

Since

$$\begin{aligned}\left\|\sum_{n=2}^{\infty}\frac{A^{n}h^{n-1}}{n!}\right\| &\leq \sum_{n=2}^{\infty}\frac{\|A\|^{n}|h|^{n-1}}{n!}\\ &= \|A\|\sum_{n=2}^{\infty}\frac{\|A\|^{n-1}|h|^{n-1}}{n!}\\ &= \|A\|\sum_{n=2}^{\infty}\frac{\|Ah\|^{n-1}}{n!}\\ &\leq \|A\|\sum_{n=1}^{\infty}\|Ah\|^{n}\\ &= \|A\|\,\|Ah\|\,\frac{1}{1-\|Ah\|}\\ &\to 0 \text{ as } |h|\to 0\end{aligned}$$

we get that

$$\begin{aligned}\lim_{|h|\to 0}\frac{\exp(A(t+h))-\exp(At)}{h} &= \left(\lim_{|h|\to 0}\frac{\exp(Ah)-1_{\mathbb{F}^n}}{h}\right)\exp(At)\\ &= A\exp(At).\end{aligned}$$

Therefore, if we define

$$x(t)=\exp(A(t-t_0))\,x_0,$$

then

$$\begin{aligned}\dot{x} &= A\exp\left(A\left(t-t_0\right)\right)x_0\\ &= Ax.\end{aligned}$$

The other problem we should solve at this point is uniqueness of solutions. To be more precise, if we have that both x and y solve the initial value problem $\dot{x} = Ax$, $x(t_0) = x_0$, then we wish to prove that $x = y$. Inner products can be used quite effectively to prove this as well. We consider the nonnegative function

$$\begin{aligned}\phi(t) &= \|x(t) - y(t)\|^2\\ &= (x_1 - y_1)^2 + \cdots + (x_n - y_n)^2.\end{aligned}$$

In the complex situation simply identify $\mathbb{C}^n = \mathbb{R}^{2n}$ and use the $2n$ real coordinates to define this norm. Recall that this norm comes from the usual inner product on Euclidean space. The derivative satisfies

$$\begin{aligned}\frac{d\phi}{dt}(t) &= 2(\dot{x}_1 - \dot{y}_1)(x_1 - y_1) + \cdots + 2(\dot{x}_n - \dot{y}_n)(x_n - y_n)\\ &= 2((\dot{x} - \dot{y})\,|\,(x-y))\\ &= 2(A(x-y)\,|\,(x-y))\\ &\leq 2\|A(x-y)\|\,\|x-y\|\\ &\leq 2\|A\|\,\|x-y\|^2\\ &= 2\|A\|\,\phi(t).\end{aligned}$$

Thus we have

$$\frac{d\phi}{dt}(t) - 2\|A\|\,\phi(t) \leq 0.$$

If we multiply this by the positive integrating factor $\exp(-2\,||A||\,(t - t_0))$ and use Leibniz' rule in reverse we obtain

$$\frac{d}{dt}\left(\phi(t)\exp\left(-2\|A\|(t-t_0)\right)\right) \leq 0$$

Together with the initial condition $\phi(t_0) = 0$ this yields

$$\phi(t)\exp\left(-2\|A\|(t-t_0)\right) \leq 0, \text{ for } t \geq t_0.$$

Since the integrating factor is positive and ϕ is nonnegative it must follow that $\phi(t) = 0$ for $t \geq t_0$. A similar argument using $-\exp(-2\|A\|(t-t_0))$ can be used to show that $\phi(t) = 0$ for $t \leq t_0$. Altogether we have established that the initial value problem $\dot{x} = Ax$, $x(t_0) = x_0$ always has a unique solution for matrices A with real (or complex) scalars as entries.

To explicitly solve these linear differential equations it is often best to understand higher order equations first and then use the cyclic subspace decomposition from chapter 2 to reduce systems to higher order equations. At the end of chapter 4 we shall give another method for solving systems of equations that does not use higher order equations.

7.1. Exercises.

(1) Let $f(z) = \sum_{n=0}^{\infty} a_n z^n$ define a power series and $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$. Show that one can define $f(A)$ as long as $\|A\| <$ radius of convergence.

(2) Let $L : V \to V$ be an operator on a finite dimensional inner product space.

(a) If $\|L\| < 1$, then $1_V + L$ has an inverse. Hint:

$$(1_V + L)^{-1} = \sum_{n=1}^{\infty} (-1)^n L^n.$$

(b) With L as above show

$$\begin{aligned} \left\|L^{-1}\right\| &\leq \frac{1}{1 - \|L\|}, \\ \left\|(1_V + L)^{-1} - 1_V\right\| &\leq \frac{\|L\|}{1 - \|L\|}. \end{aligned}$$

(c) If $\left\|L^{-1}\right\| \leq \varepsilon^{-1}$ and $\|L - K\| < \varepsilon$, then K is invertible and

$$\begin{aligned} \left\|K^{-1}\right\| &\leq \frac{\left\|L^{-1}\right\|}{1 - \|L^{-1}(K - L)\|}, \\ \left\|L^{-1} - K^{-1}\right\| &\leq \frac{\left\|L^{-1}\right\|^2}{(1 - \|L^{-1}\| \|L - K\|)^2} \|L - K\|. \end{aligned}$$

(3) Let $L : V \to V$ be an operator on a finite dimensional inner product space.

(a) If λ is an eigenvalue for L, then

$$|\lambda| \leq \|L\|.$$

(b) Give examples of 2×2 matrices where strict inequality always holds.

(4) Show that

$$x(t) = \left(\exp(A(t - t_0)) \int_{t_0}^{t} \exp(-A(s - t_0)) f(s)\, ds\right) x_0$$

solves the initial value problem $\dot{x} = Ax + f(t)$, $x(t_0) = x_0$.

(5) Let $A = B + C \in \mathrm{Mat}_{n \times n}(\mathbb{R})$ where B is invertible and $\|C\|$ is very small compared to $\|B\|$.

(a) Show that $B^{-1} - B^{-1}CB^{-1}$ is a good approximation to A^{-1}.

(b) Use this to approximate the inverse to

$$\begin{bmatrix} 1 & 0 & 1000 & 1 \\ 0 & -1 & 1 & 1000 \\ 2 & 1000 & -1 & 0 \\ 1000 & 3 & 2 & 0 \end{bmatrix}.$$

CHAPTER 4

Linear Operators on Inner Product Spaces

In this chapter we are going to study linear operators on inner product spaces. In the last chapter we introduced adjoints of linear maps between possibly different inner product spaces. Here we shall see how the adjoint can be used to understand linear operators on a fixed inner product space. The important opeartors we study here are the self-adjoint, skew-adjoint, normal, orthogonal and unitary operators. We shall spend several sections on the existence of eigenvalues, diagonalizability and canonical forms for these special but important linear operators. Having done that we go back to the study of general linear maps and operators and establish the singular value and polar decompositions. We also show Schur's theorem to the effect that complex linear operators have upper triangular matrix representations. It is possible to start this chapter by proving Schur's theorem and then use it to prove the Spectral theorems. The chapter finishes with a section on quadratic forms and how they tie in with the theory of self-adjoint operators. The second derivative test for critical points is also discussed.

We want to emphasize again that it is possible to cover the material in this chapter without first having been through chapter 2.

1. Self-adjoint Maps

A linear operator $L : V \to V$ is called *self-adjoint* if $L^* = L$. These were precisely the maps that were investigated in the previous section in the context of studying the differential of $f(x) = (L(x)|x)$. Note that a real $m \times m$ matrix A is self-adjoint precisely when it is symmetric, i.e., $A = A^t$. The 'opposite' of being self-adjoint is *skew-adjoint*: $L^* = -L$.

When the inner product is real we also say the operator is *symmetric* or *skew-symmetric*. In case the inner product is complex these operators are also called *Hermitian* or *skew-Hermitian*.

Example 75.

(1) $\begin{bmatrix} 0 & -\beta \\ \beta & 0 \end{bmatrix}$ *is skew-adjoint if β is real.*

(2) $\begin{bmatrix} \alpha & -i\beta \\ i\beta & \alpha \end{bmatrix}$ *is self-adjoint if α and β are real.*

(3) $\begin{bmatrix} i\alpha & -\beta \\ \beta & i\alpha \end{bmatrix}$ *is skew-adjoint if α and β are real.*

(4) *In general, a complex 2×2 self-adjoint matrix looks like*

$$\begin{bmatrix} \alpha & \beta + i\gamma \\ \beta - i\gamma & \delta \end{bmatrix}, \alpha, \beta, \gamma, \delta \in \mathbb{R}.$$

(5) *In general, a complex* 2×2 *skew-adjoint matrix looks like*

$$\begin{bmatrix} i\alpha & i\beta - \gamma \\ i\beta + \gamma & i\delta \end{bmatrix}, \alpha, \beta, \gamma, \delta \in \mathbb{R}.$$

EXAMPLE 76. *We saw in chapter 3 "Orthogonal Projections Revisited" that self-adjoint projections are precisely the orthogonal projections.*

EXAMPLE 77. *If* $L : V \to W$ *is a linear map we can create two self-adjoint maps* $L^*L : V \to V$ *and* $LL^* : W \to W$.

EXAMPLE 78. *Consider the space of periodic functions* $C^{\infty}_{2\pi}(\mathbb{R}, \mathbb{C})$ *with the inner product*

$$(x|y) = \frac{1}{2\pi}\int_0^{2\pi} x(t)\overline{y(t)}dt.$$

The linear operator

$$D(x) = \frac{dx}{dt}$$

can be seen to be skew-adjoint even though we haven't defined the adjoint of maps on infinite dimensional spaces. In general we say that a map is self-adjoint or skew-adjoint if

$$\begin{aligned} (L(x)|y) &= (x|L(y)), \text{ or} \\ (L(x)|y) &= -(x|L(y)) \end{aligned}$$

for all x, y. *Using that definition we note that integration by parts implies our claim:*

$$\begin{aligned} (D(x)|y) &= \frac{1}{2\pi}\int_0^{2\pi}\left(\frac{dx}{dt}(t)\right)\overline{y(t)}dt \\ &= \frac{1}{2\pi}x(t)\overline{y(t)}|_0^{2\pi} - \frac{1}{2\pi}\int_0^{2\pi} x(t)\overline{\frac{dy}{dt}(t)}dt \\ &= -(x|D(y)). \end{aligned}$$

In quantum mechanics one often makes D *self-adjoint by instead considering* iD.

In analogy with the formulae

$$\begin{aligned} \exp(x) &= \frac{\exp(x) + \exp(-x)}{2} + \frac{\exp(x) - \exp(-x)}{2} \\ &= \cosh(x) + \sinh(x), \end{aligned}$$

we have

$$\begin{aligned} L &= \frac{1}{2}(L + L^*) + \frac{1}{2}(L - L^*), \\ L^* &= \frac{1}{2}(L + L^*) - \frac{1}{2}(L - L^*) \end{aligned}$$

where $\frac{1}{2}(L + L^*)$ is self-adjoint and $\frac{1}{2}(L - L^*)$ is skew-adjoint. In the complex case we also have

$$\begin{aligned} \exp(ix) &= \frac{\exp(ix) + \exp(-ix)}{2} + \frac{\exp(ix) - \exp(-ix)}{2} \\ &= \frac{\exp(ix) + \exp(-ix)}{2} + i\frac{\exp(ix) - \exp(-ix)}{2i} \\ &= \cos(x) + i\sin(x), \end{aligned}$$

which is a nice analogy for

$$\begin{aligned} L &= \frac{1}{2}(L+L^*) + i\frac{1}{2i}(L-L^*), \\ L^* &= \frac{1}{2}(L+L^*) - i\frac{1}{2i}(L-L^*) \end{aligned}$$

where now also $\frac{1}{2i}(L-L^*)$ is self-adjoint. The idea behind this formula is that multiplication by i takes skew-adjoint maps to self-adjoints maps and vice versa.

Self- and skew-adjoint maps are clearly quite special by virtue of their definitions. The above decomposition which has quite a lot in common with dividing functions into odd and even parts or dividing complex numbers into real and imaginary parts seems to give some sort of indication that these maps could be central to the understanding of general linear maps. This is not quite true, but we shall be able to get a grasp on quite a lot of different maps.

Aside from these suggestive properties, self- and skew-adjoint maps are both *completely reducible* or *semi-simple*. This means that for each invariant subspace one can always find a complementary invariant subspace. Recall that maps like

$$L = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} : \mathbb{R}^2 \to \mathbb{R}^2$$

can have invariant subspaces without having complementary subspaces that are invariant.

PROPOSITION 23. (Reducibility of Self- or Skew-adjoint Operators) *Let $L : V \to V$ be a linear operator on a finite dimensional inner product space. If L is self- or skew-adjoint, then for each invariant subspace $M \subset V$ the orthogonal complement is also invariant, i.e., if $L(M) \subset M$, then $L\left(M^{\perp}\right) \subset M^{\perp}$.*

PROOF. Assume that $L(M) \subset M$. Let $x \in M$ and $z \in M^{\perp}$. Since $L(x) \in M$ we have

$$\begin{aligned} 0 &= (z|L(x)) \\ &= (L^*(z)|x) \\ &= \pm(L(z)|x). \end{aligned}$$

As this holds for all $x \in M$ it follows that $L(z) \in M^{\perp}$. □

This property almost tells us that these operators are diagonalizable. Certainly in the case where we have complex scalars it must follow that such maps are diagonalizable. In the case of real scalars the problem is that it is not clear that self- and/or skew-adjoint maps have any invariant subspaces whatsoever. The map which is rotation by 90° in the plane is clearly skew-symmetric, but it has no nontrivial invariant subspaces. Thus we can't make the map any simpler. We shall see below that this is basically the worst scenario that we will encounter for such maps.

1.1. Exercises.

(1) Let $L : P_n \to P_n$ be a linear map on the space of real polynomials of degree $\leq n$ such that $[L]$ with respect to the standard basis $1, t, ..., t^n$ is self-adjoint. Is L self-adjoint if we use the inner product

$$(p|q) = \int_a^b p(t)\, q(t)\, dt\ ?$$

(2) If V is finite dimensional show that the three subsets of $\hom(V,V)$ defined by

$$\begin{aligned} M_1 &= \operatorname{span}\{1_V\}, \\ M_2 &= \{L : L \text{ is skew-adjoint}\}, \\ M_3 &= \{L : \operatorname{tr} L = 0 \text{ and } L \text{ is self-adjoint}\} \end{aligned}$$

are subspaces over $\mathbb{R}$, are mutually orthogonal with respect to the real inner product $\operatorname{Re}(L,K) = \operatorname{Re}(\operatorname{tr}(L^*K))$, and yield a direct sum decomposition of $\hom(V,V)$.

(3) Let E be an orthogonal projection and L a linear operator. Recall from exercises to "Cyclic Subspaces" in chapter 2 and "Orthogonal Complements and Projections" in chapter 3 that L leaves $M = \operatorname{im}(E)$ invariant if and only if $ELE = LE$ and that $M \oplus M^\perp$ reduces L if and only if $EL = LE$. Show that if L is skew- or self-adjoint and $ELE = LE$, then $EL = LE$.

(4) Let V be a complex inner product space. Show that multiplication by i yields a bijection between self-adjoint and skew-adjoint operators on V. Is this map linear?

(5) Show that $D^{2k} : C^\infty_{2\pi}(\mathbb{R},\mathbb{C}) \to C^\infty_{2\pi}(\mathbb{R},\mathbb{C})$ is self-adjoint and that $D^{2k+1} : C^\infty_{2\pi}(\mathbb{R},\mathbb{C}) \to C^\infty_{2\pi}(\mathbb{R},\mathbb{C})$ is skew-adjoint.

(6) Let $x_1, ..., x_k$ be vectors in an inner product space V. Show that the $k \times k$ matrix $G(x_1, ..., x_k)$ whose ij entry is $(x_j|x_i)$ is self-adjoint and that all its eigenvalues are nonnegative.

(7) Let $L : V \to V$ be a self-adjoint operator on a finite dimensional inner product space and $p \in \mathbb{R}[t]$ a real polynomial. Show that $p(L)$ is also self adjoint.

(8) Assume that $L : V \to V$ is self-adjoint and $\lambda \in \mathbb{R}$. Show
   (a) $\ker(L) = \ker(L^k)$ for any $k \geq 1$. Hint: Start with $k = 2$.
   (b) $\operatorname{im}(L) = \operatorname{im}(L^k)$ for any $k \geq 1$.
   (c) $\ker(L - \lambda 1_V) = \ker\left((L - \lambda 1_V)^k\right)$ for any $k \geq 1$.
   (d) $m_L(t)$ has no multiple roots.

(9) Assume that $L : V \to V$ is self-adjoint.
   (a) Show that the eigenvalues of L are real.
   (b) In case V is complex show that L has an eigenvalue.
   (c) In case V is real show that L has an eigenvalue. Hint: Choose an orthonormal basis and observe that $[L] \in \operatorname{Mat}_{n\times n}(\mathbb{R}) \subset \operatorname{Mat}_{n\times n}(\mathbb{C})$ is also self-adjoint as a complex matrix. Thus all roots of $\chi_{[L]}(t)$ must be real by a.

(10) Assume that $L_1, L_2 : V \to V$ are both self-adjoint or skew-adjoint.
   (a) Show that L_1L_2 is skew-adjoint if and only if $L_1L_2 + L_2L_1 = 0$.
   (b) Show that L_1L_2 is self-adjoint if and only if $L_1L_2 = L_2L_1$.
   (c) Give an example where L_1L_2 is neither self-adjoint nor skew-adjoint.

2. Polarization and Isometries

The idea of *polarization* is that many bilinear expressions such as $(x|y)$ can be expressed as a sum of quadratic terms $||z||^2 = (z|z)$ for suitable z.

Let us start with a real inner product on V. Then

$$(x+y|x+y) = (x|x) + 2(x|y) + (y|y)$$

so

$$\begin{aligned}(x|y) &= \frac{1}{2}((x+y|x+y) - (x|x) - (y|y)) \\ &= \frac{1}{2}\left(\|x+y\|^2 - \|x\|^2 - \|y\|^2\right).\end{aligned}$$

Since complex inner products are only conjugate symmetric we only get

$$(x+y|x+y) = (x|x) + 2\operatorname{Re}(x|y) + (y|y),$$

which implies

$$\operatorname{Re}(x|y) = \frac{1}{2}\left(||x+y||^2 - ||x||^2 - ||y||^2\right).$$

Nevertheless the real part of the complex inner product determines the entire inner product as

$$\begin{aligned}\operatorname{Re}(x|iy) &= \operatorname{Re}(-i(x|y)) \\ &= \operatorname{Im}(x|y).\end{aligned}$$

In particular we have

$$\operatorname{Im}(x|y) = \frac{1}{2}\left(\|x+iy\|^2 - \|x\|^2 - \|iy\|^2\right).$$

We can use these ideas to check when linear operators $L : V \to V$ are zero. First we note that $L = 0$ if and only if $(L(x)|y) = 0$ for all $x, y \in V$. To check the "if" part just let $y = L(x)$ to see that $\|L(x)\|^2 = 0$ for all $x \in V$. When L is self-adjoint this can be improved.

PROPOSITION 24. (Characterization of Self-adjoint Operators) *Let $L : V \to V$ be self-adjoint. Then $L = 0$ if and only if $(L(x)|x) = 0$ for all $x \in V$.*

PROOF. There is nothing to prove when $L = 0$.

Conversely assume that $(L(x)|x) = 0$ for all $x \in V$. The polarization trick from above implies

$$\begin{aligned}0 &= (L(x+y)|x+y) \\ &= (L(x)|x) + (L(x)|y) + (L(y)|x) + (L(y)|y) \\ &= (L(x)|y) + (y|L^*(x)) \\ &= (L(x)|y) + (y|L(x)) \\ &= 2\operatorname{Re}(L(x)|y).\end{aligned}$$

Next insert $y = L(x)$ to see that

$$\begin{aligned}0 &= \operatorname{Re}(L(x)|L(x)) \\ &= \|L(x)\|^2\end{aligned}$$

as desired. □

If L is not self-adjoint there is no reason to think that such a result should hold. For instance when V is a real inner product space and L is skew-adjoint, then we have

$$\begin{aligned} (L(x)|x) &= -(x|L(x)) \\ &= -(L(x)|x) \end{aligned}$$

so $(L(x)|x) = 0$ for all x. It is therefore somewhat surprising that we can use the complex polarization trick to prove the next result.

PROPOSITION 25. *Let $L : V \to V$ be a linear operator on a complex inner product space. Then $L = 0$ if and only if $(L(x)|x) = 0$ for all $x \in V$.*

PROOF. There is nothing to prove when $L = 0$.

Conversely assume that $(L(x)|x) = 0$ for all $x \in V$. We use the complex polarization trick from above.

$$\begin{aligned} 0 &= (L(x+y)|x+y) \\ &= (L(x)|x) + (L(x)|y) + (L(y)|x) + (L(y)|y) \\ &= (L(x)|y) + (L(y)|x) \end{aligned}$$

$$\begin{aligned} 0 &= (L(x+iy)|x+iy) \\ &= (L(x)|x) + (L(x)|iy) + (L(iy)|x) + (L(iy)|iy) \\ &= -i(L(x)|y) + i(L(y)|x) \end{aligned}$$

This yields a system

$$\begin{bmatrix} 1 & 1 \\ -i & i \end{bmatrix} \begin{bmatrix} (L(x)|y) \\ (L(y)|x) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Since the columns of $\begin{bmatrix} 1 & 1 \\ -i & i \end{bmatrix}$ are linearly independent the only solution is the trivial one. In particular $(L(x)|y) = 0$. □

Polarization can also be used to give a nice characterization of isometries. These properties tie in nicely with our observation that

$$\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^* = \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^{-1}$$

when $e_1, ..., e_n$ is an orthonormal basis.

PROPOSITION 26. *Let $L : V \to W$ be a linear map between inner product spaces, then the following are equivalent.*

(1) $\|L(x)\| = \|x\|$ *for all* $x \in V$.
(2) $(L(x)|L(y)) = (x|y)$ *for all* $x, y \in V$.
(3) $L^*L = 1_V$
(4) L *takes orthonormal sets of vectors to orthonormal sets of vectors.*

PROOF. $1 \Longrightarrow 2$: Depending on whether we are in the complex or real case simply write $(L(x)|L(y))$ and $(x|y)$ in terms of norms and use 1 to see that both terms are the same.

$2 \Longrightarrow 3$: Just use that $(L^*L(x)|y) = (L(x)|L(y)) = (x|y)$ for all $x, y \in V$.

$3 \Longrightarrow 4$: We are assuming $(x|y) = (L^*L(x)|y) = (L(x)|L(y))$, which immediately implies 4.

$4 \Longrightarrow 1$: Evidently L takes unit vectors to unit vectors. So 1 holds if $||x|| = 1$. Now use the scaling property of norms to finish the argument. □

Recall the definition of the operator norm for linear maps $L : V \to W$

$$\|L\| = \max_{\|x\|=1} \|L(x)\|.$$

It was shown in "Orthonormal Bases" in chapter 3 that this norm is finite. It is important to realize that this operator norm is not the same as the norm we get from the inner product $(L|K) = \operatorname{tr}(LK^*)$ defined on $\hom(V, W)$. To see this it suffices to consider 1_V. Clearly $\|1_V\| = 1$, but $(1_V|1_V) = \operatorname{tr}(1_V 1_V) = \dim(V)$.

Corollary 26. *Let $L : V \to W$ be a linear map between inner product spaces such that $\|L(x)\| = \|x\|$ for all $x \in V$, then $\|L\| = 1$.*

Corollary 27. (Characterization of Isometries) *Let $L : V \to W$ be an isomorphism, then L is an isometry if and only if $L^* = L^{-1}$.*

Proof. If L is an isometry then it satisfies all of the above 4 conditions. In particular, $L^*L = 1_V$ so if L is invertible it must follow that $L^{-1} = L^*$.

Conversely, if $L^{-1} = L^*$, then $L^*L = 1_V$ and it follows from the previous result that L is an isometry. □

Just as for self-adjoint and skew-adjoint operators we have that isometries are completely reducible or semi-simple.

Corollary 28. (Reducibility of Isometries) *Let $L : V \to V$ be a linear operator that is also an isometry. If $M \subset V$ is L invariant, then so is $M^\perp$.*

Proof. If $x \in M$ and $y \in M^\perp$, then we note that

$$0 = (L(x)|y) = (x|L^*(y)).$$

Therefore $L^*(y) = L^{-1}(y) \in M^\perp$ for all $y \in M^\perp$. Now observe that $L^{-1}|_{M^\perp} : M^\perp \to M^\perp$ must be an isomorphism as its kernel is trivial. This implies that each $z \in M^\perp$ is of the form $z = L^{-1}(y)$ for $y \in M^\perp$. Thus $L(z) = y \in M^\perp$ and hence $M^\perp$ is L invariant. □

In the special case where $V = W = \mathbb{R}^n$ we call the linear isometries *orthogonal* matrices. The collection of orthogonal matrices is denoted O_n. Note that these matrices are a *subgroup* of $Gl_n(\mathbb{R}^n)$, i.e., if $O_1, O_2 \in O_n$ then $O_1 O_2 \in O_n$. In particular, we see that O_n is itself a group. Similarly when $V = W = \mathbb{C}^n$ we have the subgroup of *unitary* matrices $U_n \subset Gl_n(\mathbb{C}^n)$ consisting of complex matrices that are also isometries.

2.1. Exercises.

(1) On $\mathrm{Mat}_{n\times n}(\mathbb{R})$ use the inner product $(A|B) = \operatorname{tr}(AB^t)$. Consider the linear operator $L(X) = X^t$. Show that L is orthogonal. Is it skew- or self-adjoint?

(2) On $\mathrm{Mat}_{n\times n}(\mathbb{C})$ use the inner product $(A|B) = \operatorname{tr}(AB^*)$. For $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ consider the two linear operators on $\mathrm{Mat}_{n\times n}(\mathbb{C})$ defined by $L_A(X) = AX$, $R_A(X) = XA$. Show that
   (a) L_A and R_A are unitary if A is unitary.
   (b) L_A and R_A are self- or skew-adjoint if A is self- or skew-adjoint.

(3) Show that the operator D defines an isometry on both $\text{span}_{\mathbb{C}}\{\exp(it), \exp(-it)\}$ and $\text{span}_{\mathbb{R}}\{\cos(t), \sin(t)\}$ if we use the inner product inherited from $C_{2\pi}^{\infty}(\mathbb{R}, \mathbb{C})$.

(4) Let $L : V \to V$ be a complex operator on a complex inner product space. Show that L is self-adjoint if and only if $(L(x)|x)$ is real for all $x \in V$.

(5) Let $L : V \to V$ be a real operator on a real inner product space. Show that L is skew-adjoint if and only if $(L(x)|x) = 0$ for all $x \in V$.

(6) Let $e_1, ..., e_n$ be an orthonormal basis for V and assume that $L : V \to W$ has the property that $L(e_1), ..., L(e_n)$ is an orthonormal basis for W. Show that L is an isometry.

(7) Let $L : V \to V$ be a linear operator on a finite dimensional inner product space. Show that if $L \circ K = K \circ L$ for all isometries $K : V \to V$, then $L = \lambda 1_V$.

(8) Let $L : V \to V$ be a linear operator on an inner product space such that $(L(x)|L(y)) = 0$ if $(x|y) = 0$.
   (a) Show that if $\|x\| = \|y\|$ and $(x|y) = 0$, then $\|L(x)\| = \|L(y)\|$. Hint: Use and show that $x + y$ and $x - y$ are perpendicular.
   (b) Show that $L = \lambda U$, where U is an isometry.

(9) Let V be a finite dimensional real inner product space and $F : V \to V$ be a bijective map that preserves distances, i.e., for all $x, y \in V$
$$\|F(x) - F(y)\| = \|x - y\|.$$
   (a) Show that $G(x) = F(x) - F(0)$ also preserves distances and that $G(0) = 0$.
   (b) Show that $\|G(x)\| = \|x\|$ for all $x \in V$.
   (c) Using polarization to show that $(G(x)|G(y)) = (x|y)$ for all $x, y \in V$. (See also next the exercise for what can happen in the complex case.)
   (d) If $e_1, ..., e_n$ is an orthonormal basis, then show that $G(e_1), ..., G(e_n)$ is also an orthonormal basis.
   (e) Show that
$$G(x) = (x|e_1)G(e_1) + \cdots + (x|e_n)G(e_n),$$
   and conclude that G is linear.
   (f) Conclude that $F(x) = L(x) + F(0)$ for a linear isometry L.

(10) On $\text{Mat}_{n\times n}(\mathbb{C})$ use the inner product $(A|B) = \text{tr}(AB^*)$. Consider the map $L(X) = X^*$.
   (a) Show that L is real linear but not complex linear.
   (b) Show that
$$\|L(X) - L(Y)\| = \|X - Y\|$$
   for all X, Y but that
$$(L(X)|L(Y)) \neq (X|Y)$$
   for some choices of X, Y.

3. The Spectral Theorem

We are now ready to present and prove the most important theorem about when it is possible to find a basis that diagonalizes a special class of operators. There are several reasons for why this particular result is important. Firstly, it forms the foundation for all of our other results for linear maps between inner product spaces, including isometries, skew-adjoint maps and general linear maps between inner product spaces. Secondly, it is the one result of its type that has a truly satisfying generalization to infinite dimensional spaces. In the infinite dimensional setting it becomes a corner stone for several developments in analysis, functional analysis, partial differential equations, representation theory and much more. First we revisit some material from "Diagonalizability" in chapter 2.

Our general goal for linear operators $L : V \to V$ is to find a basis such that the matrix representation for L is as simple as possible. Since the simplest matrices are the diagonal matrices one might well ask if it is always possible to find a basis x_1, ..., x_m that diagonalizes L, i.e., $L(x_1) = \lambda_1 x_1$, ..., $L(x_m) = \lambda_m x_m$? The central idea behind finding such a basis is quite simple and reappears in several proofs in this chapter. Given some special information about the vector space V or the linear operator L on V we show that L^* has an eigenvector $x \neq 0$ and that the orthogonal complement to x in V is L invariant. The existence of this invariant subspace of V then indicates that the procedure for establishing a particular result about exhibiting a nice matrix representation for L is a simple induction on the dimension of the vector space.

A rotation by 90° in $\mathbb{R}^2$ does not have a basis of eigenvectors. However, if we interpret it as a complex map on $\mathbb{C}$ it is just multiplication by i and therefore of the desired form. We could also view the 2×2 matrix as a map on $\mathbb{C}^2$. As such we can also diagonalize it by using $x_1 = (i, 1)$ and $x_2 = (-i, 1)$ so that x_1 is mapped to ix_1 and x_2 to $-ix_2$.

A much worse example is the linear map represented by

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

Here $x_1 = (1, 0)$ does have the property that $Ax_1 = 0$, but it is not possible to find x_2 linearly independent from x_1 so that $Ax_2 = \lambda x_2$. In case $\lambda = 0$ we would just have $A = 0$ which is not true. So $\lambda \neq 0$, but then $x_2 \in \operatorname{im}(A) = \operatorname{span}\{x_1\}$. Note that using complex scalars cannot alleviate this situation due to the very general nature of the argument.

At this point it should be more or less clear that the first goal is to show that self-adjoint operators have eigenvalues. Recall that in chapter 2 we constructed a characteristic polynomial for L with the property that any eigenvalue must be a root of this polynomial. This is fine if we work with complex scalars, but less satisfactory if we use real scalars although it is in fact not hard to deal with by passing to suitable matrix representations (see exercises to "Self-adjoint Maps"). It is possible to give a very elegant proof that self-adjoint operators have eigenvalues using Lagrange multipliers.We shall give a similar proof here that doesn't use multivariable derivatives.

Theorem 32. (Existence of Eigenvalues for Self-adjoint Operators) *Let $L : V \to V$ be self-adjoint and V finite dimensional, then L has a real eigenvalue.*

Proof. As in the Lagrange multiplier proof we use the compact set $S = \{x \in V : (x|x) = 1\}$ and the real valued function $x \to (Lx|x)$ on S. Select $x_1 \in S$ so that

$$(Lx|x) \leq (Lx_1|x_1)$$

for all $x \in S$. If we define $\lambda_1 = (Lx_1|x_1)$, then this implies that

$$(Lx|x) \leq \lambda_1, \text{ for all } x \in S.$$

Consequently

$$(Lx|x) \leq \lambda_1 (x|x) = \lambda_1 ||x||^2, \text{ for all } x \in V.$$

This shows that the function

$$f(x) = \frac{(Lx|x)}{||x||^2}$$

has a maximum at $x = x_1$ and that the value there is λ_1.

This implies that for any $y \in V$, the function $t \to f(x_1 + ty)$ has a maximum at $t = 0$ and and hence the derivative at $t = 0$ is zero. To be able to use this we need to compute the derivative of the quotient

$$\frac{(L(x_1 + ty)|x_1 + ty)}{||x_1 + ty||^2}$$

with respect to t at $t = 0$. We start by computing the derivative of the numerator at $t = 0$ using the definition of a derivative

$$\begin{aligned}
& \lim_{h \to 0} \frac{(L(x_1 + hy)|x_1 + hy) - (L(x_1)|x_1)}{h} \\
= & \lim_{h \to 0} \frac{(L(hy)|x_1) + (L(x_1)|hy) + (L(hy)|hy)}{h} \\
= & \lim_{h \to 0} \frac{(hy|L(x_1)) + (L(x_1)|hy) + (L(hy)|hy)}{h} \\
= & (y|L(x_1)) + (L(x_1)|y) + \lim_{h \to 0} (L(y)|hy) \\
= & 2\operatorname{Re}(L(x_1)|y).
\end{aligned}$$

The derivate of the denominator is computed the same way simply observing that we can let $L = 1_V$. The derivative of the quotient $f(x_1 + ty)$ at $t = 0$ is then

$$\begin{aligned}
0 &= \frac{2\operatorname{Re}(L(x_1)|y)||x_1||^2 - 2\operatorname{Re}(x_1|y)(L(x_1)|x_1)}{||x_1||^4} \\
&= 2\operatorname{Re}(L(x_1)|y) - 2\operatorname{Re}(x_1|y)\lambda_1 \\
&= 2\operatorname{Re}(L(x_1) - \lambda_1 x_1|y).
\end{aligned}$$

By using $y = L(x_1) - \lambda_1 x_1$ we then see that λ_1 and x_1 form an eigenvalue/vector pair. □

We can now prove.

THEOREM 33. (The Spectral Theorem) *Let $L : V \to V$ be a self-adjoint operator on a finite dimensional inner product space. Then there exists an orthonormal basis $e_1, ..., e_n$ of eigenvectors, i.e., $L(e_1) = \lambda_1 e_1, ..., L(e_n) = \lambda_n e_n$. Moreover, all eigenvalues $\lambda_1, ..., \lambda_n$ are real.*

PROOF. We just proved that we can find an eigenvalue/vector pair $L(e_1) = \lambda_1 e_1$. Recall that λ_1 was real and we can, if necessary, multiply e_1 by a suitable scalar to make it a unit vector.

Next we use self-adjointness of L again to see that L leaves the orthogonal complement to e_1 invariant, i.e., $L(M) \subset M$, where $M = \{x \in V : (x|e_1) = 0\}$. To see this let $x \in M$ and calculate

$$\begin{aligned} (L(x)|e_1) &= (x|L^*(e_1)) \\ &= (x|L(e_1)) \\ &= (x|\lambda_1 e_1) \\ &= \bar{\lambda}_1 (x|e_1) \\ &= 0. \end{aligned}$$

Now we have a new operator $L : M \to M$ on a space of dimension $\dim M = \dim V - 1$. We note that this operator is also self-adjoint. Thus we can use induction on $\dim V$ to prove the theorem. Alternatively we can extract an eigenvalue/vector pair $L(e_2) = \lambda_2 e_2$, where $e_2 \in M$ is a unit vector and then pass down to the orthogonal complement of e_2 inside M. This procedure will end in $\dim V$ steps and will also generate an orthonormal basis of eigenvectors as the vectors are chosen successively to be orthogonal to each other. □

In the notation of "Linear Maps as Matrices" from chapter 1 we have proven.

COROLLARY 29. *Let $L : V \to V$ be a self-adjoint operator on a finite dimensional inner product space. There exists an orthonormal basis $e_1, ..., e_n$ of eigenvectors and a real $n \times n$ diagonal matrix D such that*

$$\begin{aligned} L &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} D \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^* \\ &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^* \end{aligned}$$

The same eigenvalue can apparently occur several times, just think of 1_V. Recall that the geometric multiplicity of an eigenvalue is $\dim(\ker(L - \lambda 1_V))$. This is clearly the same as the number of times it occurs in the above diagonal form of the operator. Thus the basis vectors that correspond to λ in the diagonalization yield a basis for $\ker(L - \lambda 1_V)$. With this in mind we can rephrase the Spectral theorem.

THEOREM 34. *Let $L : V \to V$ be a self-adjoint operator on a finite dimensional inner product space and $\lambda_1, ..., \lambda_k$ the distinct eigenvalues for L. Then*

$$1_V = \mathrm{proj}_{\ker(L-\lambda_1 1_V)} + \cdots + \mathrm{proj}_{\ker(L-\lambda_k 1_V)}$$

and

$$L = \lambda_1 \,\mathrm{proj}_{\ker(L-\lambda_1 1_V)} + \cdots + \lambda_k \,\mathrm{proj}_{\ker(L-\lambda_k 1_V)}.$$

PROOF. The missing piece that we need to establish is that the eigenspaces are mutually orthogonal to each other. This actually follows from our constructions in the proof of the spectral theorem. Nevertheless it is desirable to have a direct proof of this. Let $L(x) = \lambda x$ and $L(y) = \mu y$, then

$$\begin{aligned} \lambda (x|y) &= (L(x)|y) \\ &= (x|L(y)) \\ &= (x|\mu y) \\ &= \mu (x|y) \text{ since } \mu \text{ is real.} \end{aligned}$$

If $\lambda \neq \mu$, then we get

$$(\lambda - \mu)(x|y) = 0,$$

which implies $(x|y) = 0$.

We this in mind we can now see that if $x_i \in \ker(L - \lambda_i 1_V)$, then

$$\mathrm{proj}_{\ker(L-\lambda_j 1_V)}(x_i) = \begin{cases} x_j & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

as x_i is perpendicular to $\ker(L - \lambda_j 1_V)$ in case $i \neq j$. Since we can write $x = x_1 + \cdots + x_k$, where $x_i \in \ker(L - \lambda_i 1_V)$ we have

$$\mathrm{proj}_{\ker(L-\lambda_i 1_V)}(x) = x_i$$

This shows that

$$x = \mathrm{proj}_{\ker(L-\lambda_1 1_V)}(x) + \cdots + \mathrm{proj}_{\ker(L-\lambda_k 1_V)}(x)$$

as well as

$$L(x) = \left(\lambda_1 \mathrm{proj}_{\ker(L-\lambda_1 1_V)} + \cdots + \lambda_k \mathrm{proj}_{\ker(L-\lambda_k 1_V)}\right)(x).$$

□

The fact that we can diagonalize self-adjoint operators has an immediate consequence for complex skew-adjoint operators as they become self-adjoint by multiplying them by $i = \sqrt{-1}$. Thus we have.

COROLLARY 30. (The Spectral Theorem for Complex Skew-adjoint Operators) *Let $L : V \to V$ be a skew-adjoint operator on a complex finite dimensional space. Then we can find an orthonormal basis such that $L(e_1) = i\mu_1 e_1, ..., L(e_n) = i\mu_n e_n$, where $\mu_1, ..., \mu_n \in \mathbb{R}$.*

It is worth pondering this statement. Apparently we haven't said anything about skew-adjoint real linear operators. The statement, however, does cover both real and complex matrices as long as we view them as maps on $\mathbb{C}^n$. It just so happens that the corresponding diagonal matrix has purely imaginary entries, unless they are 0, and hence is forced to be complex.

Before doing several examples it is worthwhile trying to find a way of remembering the formula

$$L = \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} D \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^*.$$

If we solve it for D instead it reads

$$D = \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^* L \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}.$$

This is quite natural as

$$L \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} = \begin{bmatrix} \lambda_1 e_1 & \cdots & \lambda_n e_n \end{bmatrix}$$

and then observing that

$$\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^* \begin{bmatrix} \lambda_1 e_1 & \cdots & \lambda_n e_n \end{bmatrix}$$

is the matrix whose ij entry is $(\lambda_j e_j | e_i)$ since the rows $\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^*$ correspond to the colomns in $\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}$. This gives a quick check for whether we have the change of basis matrices in the right places.

EXAMPLE 79. *Let*

$$A=\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}.$$

Then A is both self-adjoint and unitary. This shows that ± 1 are the only possible eigenvalues. We can easily find nontrivial solutions to both equations $(A \mp 1_{\mathbb{C}^2})(x) = 0$ by observing that

$$\begin{aligned}(A-1_{\mathbb{C}^2})\begin{bmatrix} -i \\ 1 \end{bmatrix} &= \begin{bmatrix} -1 & -i \\ i & -1 \end{bmatrix}\begin{bmatrix} -i \\ 1 \end{bmatrix}=0 \\ (A+1_{\mathbb{C}^2})\begin{bmatrix} 1 \\ i \end{bmatrix} &= \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}\begin{bmatrix} i \\ 1 \end{bmatrix}=0\end{aligned}$$

The vectors

$$z_1=\begin{bmatrix} -i \\ 1 \end{bmatrix}, z_2=\begin{bmatrix} i \\ 1 \end{bmatrix}$$

form an orthogonal set that we can normalize to an orthonormal basis of eigenvectors

$$x_1=\begin{bmatrix} \frac{-i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}, x_2=\begin{bmatrix} \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}.$$

This means that

$$A=\begin{bmatrix} x_1 & x_2 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} x_1 & x_2 \end{bmatrix}^{-1},$$

or more concretely that

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}=\begin{bmatrix} \frac{-i}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

EXAMPLE 80. *Let*

$$B=\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

The corresponding self-adjoint matrix is

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}.$$

Using the identity

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}=\begin{bmatrix} \frac{-i}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$

and then multiplying by $-i$ to get back to

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

we obtain

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}=\begin{bmatrix} \frac{-i}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}\begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}\begin{bmatrix} \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

It is often more convenient to find the eigenvalues using the characteristic polynomial, to see why this is let us consider some more complicated examples.

EXAMPLE 81. *We consider the real symmetric operator*

$$A = \begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix}, \alpha, \beta \in \mathbb{R}.$$

This time one can more or less readily see that

$$x_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, x_2 = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

are eigenvectors and that the corresponding eigenvalues are $(\alpha \pm \beta)$. *But if one didn't guess that then computing the characteristic polynomial is clearly the way to go.*

Even with relatively simple examples such as

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

things quickly get out of hand. Clearly the method of using Gauss elimination on the system $A - \lambda 1_{\mathbb{C}^n}$ and then finding conditions on λ that ensure that we have nontrivial solutions is more useful in finding all eigenvalues/vectors.

EXAMPLE 82. *Let us try this with*

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

Thus we consider

$$\begin{bmatrix} 1-\lambda & 1 & 0 \\ 1 & 2-\lambda & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2-\lambda & 0 \\ 1-\lambda & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & (2-\lambda) & 0 \\ 0 & -(1-\lambda)(2-\lambda)+1 & 0 \end{bmatrix}$$

Thus there is a nontrivial solution precisely when

$$-(1-\lambda)(2-\lambda)+1 = -1+3\lambda-\lambda^2 = 0.$$

The roots of this polynomial are $\lambda_{1,2} = \frac{3}{2} \pm \frac{1}{2}\sqrt{5}$. *The corresponding eigenvectors are found by inserting the root and then finding a nontrivial solution. Thus we are trying to solve*

$$\begin{bmatrix} 1 & (2-\lambda_{1,2}) & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

which means that

$$x_{1,2} = \begin{bmatrix} \lambda_{1,2} - 2 \\ 1 \end{bmatrix}.$$

We should normalize this to get a unit vector

$$\begin{aligned} e_{1,2} &= \frac{1}{\sqrt{5 - 4\lambda_{1,2} + (\lambda_{1,2})^2}} \begin{bmatrix} \lambda_{1,2} - 2 \\ 1 \end{bmatrix} \\ &= \frac{1}{\sqrt{\left(34 \mp 10\sqrt{5}\right)}} \begin{bmatrix} -1 \pm \sqrt{5} \\ 1 \end{bmatrix} \end{aligned}$$

3.1. Exercises.

(1) Let L be self- or skew-adjoint on a complex finite dimensional inner product space.
   (a) Show that $L = K^2$ for some $K : V \to V$.
   (b) Show by example that K need not be self-adjoint if L is self-adjoint.
   (c) Show by example that K need not be skew-adjoint if L is skew-adjoint.

(2) Diagonalize the matrix that is zero everywhere except for 1s on the antidiagonal.
$$\begin{bmatrix} 0 & \cdots & 0 & 1 \\ \vdots & & 1 & 0 \\ 0 & & & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix}$$

(3) Diagonalize the real matrix that has αs on the diagonal and βs everywhere else.
$$\begin{bmatrix} \alpha & \beta & \cdots & \beta \\ \beta & \alpha & & \beta \\ \vdots & & \ddots & \vdots \\ \beta & \beta & \cdots & \alpha \end{bmatrix}$$

(4) Let $K, L : V \to V$ be self-adjoint operators on a finite dimensional vector space. If $KL = LK$, then show that there is an orthonormal basis diagonalizing both K and L.

(5) Let $L : V \to V$ be self-adjoint. If there is a unit vector $x \in V$ such that
$$\|L(x) - \mu x\| \leq \varepsilon,$$
then L has an eigenvalue λ so that $|\lambda - \mu| \leq \varepsilon$.

(6) Let $L : V \to V$ be self-adjoint. Show that either $\|L\|$ or $-\|L\|$ are eigenvalues for L.

(7) If an operator $L : V \to V$ on a finite dimensional inner product space satisfies one of the following 4 conditions, then it is said to be *positive*. Show that these conditions are equivalent.
   (a) L is self-adjoint with positivee eigenvalues.
   (b) L is self-adjoint and $(L(x)|x) > 0$ for all $x \in V - \{0\}$.
   (c) $L = K^* \circ K$ for an injective operator $K : V \to W$, where W is also an inner product space.
   (d) $L = K \circ K$ for an invertible self-adjoint operator $K : V \to V$.

(8) Let $P : V \to V$ be a positive operator.
   (a) If $L : V \to V$ is self-adjoint, then PL is diagonalizable and has real eigenvalues. (Note that PL is not necessarily selfadjoint).
   (b) If $Q : V \to V$ is positive, then QP is diagonalizable and has positive eigenvalues.

(9) Let P, Q be two positive operators. If $P^2 = Q^2$, then show that $P = Q$.

(10) Let P be a nonnegative operator, i.e., self-adjoint with nonnegative eigenvalues.
   (a) Show that $\operatorname{tr} P \geq 0$.
   (b) Show that $P = 0$ if and only if $\operatorname{tr} P = 0$.

(11) Let $L : V \to V$ be a linear operator on an inner product space.

(a) If L is self-adjoint, show that L^2 is self-adjoint and has nonnegative eigenvalues.
(b) If L is skew-adjoint, show that L^2 is self-adjoint and has nonpositive eigenvalues.

(12) Consider the *Killing form* on $\hom(V, V)$, where V is a finite dimensional vector space of dimension > 1, defined by

$$\mathrm{K}(L, K) = \operatorname{tr} L \operatorname{tr} K - \operatorname{tr}(LK).$$

(a) Show that $\mathrm{K}(L, K) = \mathrm{K}(K, L)$.
(b) Show that $K \to \mathrm{K}(L, K)$ is linear.
(c) Assume in addition that V is an inner product space. Show that $\mathrm{K}(L, L) > 0$ if L is skew-adjoint and $L \neq 0$.
(d) Show that $\mathrm{K}(L, L) < 0$ if L is self-adjoint and $L \neq 0$.
(e) Show that K is nondegenerate, i.e., if $L \neq 0$, then we can find $K \neq 0$, so that $\mathrm{K}(L, K) \neq 0$.

4. Normal Operators

The concept of a normal operator is somewhat more general than the previous special types of operators we have seen. The definition is quite simple and will be motivated below. We say that an operator $L : V \to V$ on an inner product space is *normal* if $LL^* = L^*L$. With this definition it is clear that all self-adjoint, skew-adjoint and isometric operators are normal.

First let us show that any operator that is diagonalizable with respect to an orthonormal basis must be normal. Suppose that L is diagonalized in the orthonormal basis $e_1, ..., e_n$ and that D is the diagonal matrix representation in this basis, then

$$\begin{aligned} L &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} D \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^* \\ &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^*, \end{aligned}$$

and

$$\begin{aligned} L^* &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} D^* \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^* \\ &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} \begin{bmatrix} \bar{\lambda}_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \bar{\lambda}_n \end{bmatrix} \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^* \end{aligned}$$

Thus

$$\begin{aligned} LL^* &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} \bar{\lambda}_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \bar{\lambda}_n \end{bmatrix} \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^* \\ &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} \begin{bmatrix} |\lambda_1|^2 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & |\lambda_n|^2 \end{bmatrix} \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^* \\ &= L^*L \end{aligned}$$

since $DD^* = D^*D$.

For real operators we have already observed that they must be self-adjoint in order to be diagonalizable with respect to an orthonormal basis. For complex operators things are a little different as also skew-symmetric operators are diagonalizable with respect to an orthonormal basis. Below we shall generalize the spectral theorem to normal operators and show that in the complex case these are precisely the operators that can be diagonalized with respect to an orthonormal basis. The canonical form for real normal operators is somewhat more complicated and will be studied in "Real Forms" below.

EXAMPLE 83.

$$\begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$$

is not normal since

$$\begin{aligned} \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} &= \begin{bmatrix} 2 & 2 \\ 2 & 4 \end{bmatrix}, \\ \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} &= \begin{bmatrix} 1 & 1 \\ 1 & 5 \end{bmatrix}. \end{aligned}$$

Nevertheless it is diagonalizable with respect to the basis

$$x_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, x_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

as

$$\begin{aligned} \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \\ \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} &= \begin{bmatrix} 2 \\ 2 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \end{aligned}$$

While we can normalize x_2 to be a unit vector there is nothing we can do about x_1 and x_2 not being perpendicular.

EXAMPLE 84. *Let*

$$A = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} : \mathbb{C}^2 \to \mathbb{C}^2.$$

Then

$$\begin{aligned} AA^* &= \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \begin{bmatrix} \bar{\alpha} & \bar{\beta} \\ \bar{\gamma} & \bar{\delta} \end{bmatrix} = \begin{bmatrix} |\alpha|^2 + |\gamma|^2 & \alpha\bar{\beta} + \gamma\bar{\delta} \\ \bar{\alpha}\beta + \bar{\gamma}\delta & |\beta|^2 + |\delta|^2 \end{bmatrix} \\ A^*A &= \begin{bmatrix} \bar{\alpha} & \bar{\beta} \\ \bar{\gamma} & \bar{\delta} \end{bmatrix} \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} = \begin{bmatrix} |\alpha|^2 + |\beta|^2 & \bar{\alpha}\gamma + \bar{\beta}\delta \\ \alpha\bar{\gamma} + \beta\bar{\delta} & |\gamma|^2 + |\delta|^2 \end{bmatrix} \end{aligned}$$

So the conditions for A to be normal are

$$\begin{aligned} |\beta|^2 &= |\gamma|^2, \\ \alpha\bar{\gamma} + \beta\bar{\delta} &= \bar{\alpha}\beta + \bar{\gamma}\delta \end{aligned}$$

The last equation is easier to remember if we note that it means that the columns of A must have the same inner product as the columns of A^*.

Observe that unitary, self- and skew-adjoint operators are normal. Another very simple normal operator that isn't necessarily of those three types is $\lambda 1_V$ for all $\lambda \in \mathbb{C}$.

PROPOSITION 27. (Characterization of Normal Operators) *Let $L : V \to V$ be an operator on an inner product space. Then the following conditions are equivalent.*

(1) $LL^* = L^*L$.
(2) $\|L(x)\| = \|L^*(x)\|$ *for all* $x \in V$.
(3) $BC = CB$, *where* $B = \frac{1}{2}(L + L^*)$ *and* $C = \frac{1}{2}(L - L^*)$.

PROOF. $1 \iff 2$: Note that for all $x \in V$ we have

$$\begin{array}{cc} & \|L(x)\| = \|L^*(x)\| \\ \iff & \|L(x)\|^2 = \|L^*(x)\|^2 \\ \iff & (L(x)|L(x)) = (L^*(x)|L^*(x)) \\ \iff & (x|L^*L(x)) = (x|LL^*(x)) \\ \iff & (x|(L^*L - LL^*)(x)) = 0 \\ \iff & L^*L - LL^* = 0 \end{array}$$

The last implication is a consequence of the fact that $L^*L - LL^*$ is self-adjoint.

$3 \iff 1$: We note that

$$\begin{aligned} BC &= \frac{1}{2}(L + L^*)\frac{1}{2}(L - L^*) \\ &= \frac{1}{4}(L + L^*)(L - L^*) \\ &= \frac{1}{4}\left(L^2 - (L^*)^2 + L^*L - LL^*\right), \\ CB &= \frac{1}{4}(L - L^*)(L + L^*) \\ &= \frac{1}{4}\left(L^2 - (L^*)^2 - L^*L + LL^*\right). \end{aligned}$$

So $BC = CB$ if and only if $L^*L - LL^* = -L^*L + LL^*$ which is the same as saying that $LL^* = L^*L$. □

We also need a general result about invariant subspaces.

LEMMA 21. *Let $L : V \to V$ be an operator on a finite dimensional inner product space. If $M \subset V$ is an L and L^* invariant subspace, then $M^\perp$ is also L and L^* invariant. In particular.*

$$(L|_{M^\perp})^* = L^*|_{M^\perp}.$$

PROOF. Let $x \in M$ and $y \in M^\perp$. We have to show that

$$\begin{aligned} (x|L(y)) &= 0, \\ (x|L^*(y)) &= 0. \end{aligned}$$

For the first identity use that

$$(x|L(y)) = (L^*(x)|y) = 0$$

since $L^*(x) \in M$. Similarly for the second that

$$(x|L^*(y)) = (L(x)|y) = 0$$

since $L(x) \in M$. □

We are now ready to prove the spectral theorem for normal operators.

THEOREM 35. (The Spectral Theorem for Normal Operators) *Let $L : V \to V$ be a normal operator on a complex inner product space, then there is an orthonormal basis e_1, ..., e_n of eigenvectors, i.e., $L(e_1) = \lambda_1 e_1$, ..., $L(e_n) = \lambda_n e_n$.*

PROOF. As with the spectral theorem the proof depends on showing that we can find an eigenvalue and that the orthogonal complement to an eigenvalue is invariant.

Rather than appealing to the fundamental theorem of algebra in order to find an eigenvalue for L we shall use what we know about self-adjoint operators. This has the advantage of also yielding a proof that works in the real case (see "Real Forms" below). First decompose $L = B + iC$, where B and C are self-adjoint and then use the spectral theorem to find $\alpha \in \mathbb{R}$ such that $\ker(B - \alpha 1_V) \neq \{0\}$. Next note that since $B \cdot iC = iC \cdot B$ it follows that $BC = CB$. Therefore, if $x \in \ker(B - \alpha 1_V)$, then

$$\begin{aligned}(B - \alpha 1_V)(C(x)) &= BC(x) - \alpha C(x) \\ &= CB(x) - C(\alpha x) \\ &= C((B - \alpha 1_V)(x)) \\ &= 0.\end{aligned}$$

Thus $C : \ker(B - \alpha 1_V) \to \ker(B - \alpha 1_V)$. Using that C and hence also its restriction to $\ker(B - \alpha 1_V)$ are self-adjoint we can find $x \in \ker(B - \alpha 1_V)$ so that $C(x) = \beta x$. This means that

$$\begin{aligned}L(x) &= B(x) + iC(x) \\ &= \alpha x + i\beta x \\ &= (\alpha + i\beta)x.\end{aligned}$$

Hence we have found an eigenvalue $\alpha + i\beta$ for L with a corresponding eigenvector x. We see in addition that

$$\begin{aligned}L^*(x) &= B(x) - iC(x) \\ &= (\alpha - i\beta)x.\end{aligned}$$

Thus $\operatorname{span}\{x\}$ is both L and L^* invariant. The previous lemma then shows that $M = (\operatorname{span}\{x\})^\perp$ is also L and L^* invariant. Hence $(L|_M)^* = L^*|_M$ showing that $L|_M : M \to M$ is also normal. We can then use induction as in the spectral theorem to finish the proof. □

As an immediate consequence we get a result for unitary operators.

THEOREM 36. (The Spectral Theorem for Unitary Operators) *Let $L : V \to V$ be unitary, then there is an orthonormal basis e_1, ..., e_n such that $L(e_1) = e^{i\theta_1} e_1$, ..., $L(e_n) = e^{i\theta_n} e_n$, where $\theta_1, ..., \theta_n \in \mathbb{R}$.*

We also have the more abstract form of the spectral theorem.

THEOREM 37. *Let $L : V \to V$ be a normal operator on a complex finite dimensional inner product space and $\lambda_1, ..., \lambda_k$ the distinct eigenvalues for L. Then*

$$1_V = \operatorname{proj}_{\ker(L - \lambda_1 1_V)} + \cdots + \operatorname{proj}_{\ker(L - \lambda_k 1_V)}$$

and

$$L = \lambda_1 \operatorname{proj}_{\ker(L - \lambda_1 1_V)} + \cdots + \lambda_k \operatorname{proj}_{\ker(L - \lambda_k 1_V)}.$$

Let us see what happens in some examples.

EXAMPLE 85. *Let*

$$L = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}, \alpha, \beta \in \mathbb{R}$$

then L is normal. When $\alpha = 0$ it is skew-adjoint, when $\beta = 0$ it is self-adjoint and when $\alpha^2 + \beta^2 = 1$ it is an orthogonal transformation. The decomposition $L = B + iC$ looks like

$$\begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix} + i \begin{bmatrix} 0 & -i\beta \\ i\beta & 0 \end{bmatrix}$$

Here

$$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$$

has α as an eigenvalue and

$$\begin{bmatrix} 0 & -i\beta \\ i\beta & 0 \end{bmatrix}$$

has $\pm\beta$ as eigenvalues. Thus L has eigenvalues $(\alpha \pm i\beta)$.

EXAMPLE 86.

$$\begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is normal and has 1 as an eigenvalue. We are then reduced to looking at

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

which has $\pm i$ as eigenvalues.

4.1. Exercises.

(1) Consider $L_A(X) = AX$ and $R_A(X) = XA$ as linear operators on $\text{Mat}_{n\times n}(\mathbb{C})$. What conditions do you need on A in order for these maps to be normal?
(2) Assume that $L : V \to V$ is normal and that $p \in \mathbb{F}[t]$. Show that $p(L)$ is also normal.
(3) Assume that $L : V \to V$ is normal. Without using the spectral theorem show
  (a) $\ker(L) = \ker(L^*)$.
  (b) $\ker(L - \lambda 1_V) = \ker\left(L^* - \bar{\lambda} 1_V\right)$.
  (c) $\text{im}(L) = \text{im}(L^*)$.
  (d) $(\ker(L))^{\perp} = \text{im}(L)$.
(4) Assume that $L : V \to V$ is normal. Without using the spectral theorem show
  (a) $\ker(L) = \ker\left(L^k\right)$ for any $k \geq 1$. Hint: Use the self-adjoint operator $K = L^* L$.
  (b) $\text{im}(L) = \text{im}\left(L^k\right)$ for any $k \geq 1$.
  (c) $\ker(L - \lambda 1_V) = \ker\left((L - \lambda 1_V)^k\right)$ for any $k \geq 1$.
  (d) Show that the minimal polynomial of L has no multiple roots.

(5) *(Characterization of Normal Operators)* Let $L : V \to V$ be a linear operator on a finite dimensional inner product space. Show that L is normal if and only if $(L \circ E | L \circ E) = (L^* \circ E | L^* \circ E)$ for all orthogonal projections $E : V \to V$. Hint: Use the formula

$$(L_1 | L_2) = \sum_{i=1}^{n} (L_1 (e_i) | L_2 (e_i))$$

for suitable choices of orthonormal bases $e_1, ..., e_n$ for V.

(6) Let $L : V \to V$ be an operator on a finite dimensional inner product space. Assume that $M \subset V$ is an L invariant subspace and let $E : V \to V$ be the orthogonal projection onto M.

(a) Justify all of the steps in the calculation:

$$\begin{aligned}(L^* \circ E | L^* \circ E) &= \left(E^{\perp} \circ L^* \circ E | E^{\perp} \circ L^* \circ E\right) + (E \circ L^* \circ E | E \circ L^* \circ E) \\ &= \left(E^{\perp} \circ L^* \circ E | E^{\perp} \circ L^* \circ E\right) + (E \circ L \circ E | E \circ L \circ E) \\ &= \left(E^{\perp} \circ L^* \circ E | E^{\perp} \circ L^* \circ E\right) + (L \circ E | L \circ E) .\end{aligned}$$

Hint: Use the result that $E^* = E$ from "Orthogonal Projections Redux" and that $L(M) \subset M$ implies $E \circ L \circ E = L \circ E$.

(b) If L is normal use the previous exercise to conclude that M is L^* invariant and $M^{\perp}$ is L invariant.

(7) *(Characterization of Normal Operators)* Let $L : V \to V$ be a linear map on a finite dimensional inner product space. Assume that L has the property that all L invariant subspaces are also L^* invariant.

(a) Show that L is completely reducible.

(b) Show that the matrix representation with respect to an orthonormal basis is diagonalizable when viewed as complex matrix.

(c) Show that L is normal.

(8) Assume that $L : V \to V$ satisfies $L^* L = \lambda 1_V$, for some $\lambda \in \mathbb{C}$. Show that L is normal.

(9) Show that if a projection is normal then it is an orthogonal projection.

(10) If $L : V \to V$ is normal and $p \in \mathbb{F}[t]$, then $p(L)$ is also normal and if $\mathbb{F} = \mathbb{C}$ then

$$p(L) = p(\lambda_1) \operatorname{proj}_{\ker(L - \lambda_1 1_V)} + \cdots + p(\lambda_k) \operatorname{proj}_{\ker(L - \lambda_k 1_V)} .$$

(11) Let $L, K : V \to V$ be normal. Show by example that neither $L + K$ nor LK need be normal.

(12) Let A be an upper triangular matrix. Show that A is normal if and only if it is diagonal. Hint: Compute and compare the diagonal entries in AA^* and $A^* A$.

(13) *(Characterization of Normal Operators)* Let $L : V \to V$ be an operator on a finite dimensional complex inner product space. Show that L is normal if and only if $L^* = p(L)$ for some polynomial p.

(14) *(Characterization of Normal Operators)* Let $L : V \to V$ be an operator on a finite dimensional complex inner product space. Show that L is normal if and only if $L^* = LU$ for some unitary operator $U : V \to V$.

(15) Let $L : V \to V$ be normal on a finite dimensional complex inner product space. Show that $L = K^2$ for some normal operator K.

(16) Give the canonical form for the linear maps that are both self-adjoint and unitary.
(17) Give the canonical form for the linear maps that are both skew-adjoint and unitary.

5. Unitary Equivalence

In the special case where $V = \mathbb{F}^n$ the spectral theorem can be rephrased in terms of change of basis. Recall from "Matrix Representations Redux" in chapter 1 that if we pick a different basis $x_1, ..., x_n$ for $\mathbb{F}^n$, then the matrix representations for a linear map represented by A in the standard basis and B in the new basis are related by

$$A = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} B \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^{-1}.$$

In case $x_1, ..., x_n$ is an orthonormal basis this reduces to

$$A = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} B \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^{*},$$

where $\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}$ is a unitary or orthogonal operator.

Two $n \times n$ matrices A and B are said to be *unitarily equivalent* if $A = UBU^*$, where $U \in U_n$, i.e., U is an $n \times n$ matrix such that $U^*U = UU^* = 1_{\mathbb{F}^n}$. In case $U \in O_n \subset U_n$ we also say that the matrices are *orthogonally equivalent*.

The results from the previous two sections can now be paraphrased in the following way.

Corollary 31. (1) *A normal $n \times n$ matrix is unitarily equivalent to a diagonal matrix.*
(2) *A self-adjoint $n \times n$ matrix is unitarily or orthogonally equivalent to a real diagonal matrix.*
(3) *A skew-adjoint $n \times n$ matrix is unitarily equivalent to a purely imaginary diagonal matrix.*
(4) *A unitary $n \times n$ matrix is unitarily equivalent to a diagonal matrix whose diagonal elements are unit scalars.*

Using the group properties of unitary matrices one can easily show the next two results.

Proposition 28. *If A and B are unitarily equivalent, then*
(1) *A is normal if and only if B is normal.*
(2) *A is self-adjoint if and only if B is self-adjoint.*
(3) *A is skew-adjoint if and only if B is skew-adjoint.*
(4) *A is unitary if and only if B is unitary.*

In addition to these results we see that the spectral theorem for normal operators implies:

Corollary 32. *Two normal operators are unitarily equivalent if and only if they have the same eigenvalues (counted with multiplicities).*

Example 87. *The Pauli matrices are defined by*

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}.$$

They are all self-adjoint and unitary. Moreover, all have eigenvalues ± 1 so they are all unitarily equivalent.

EXAMPLE 88. *If we multiply the Pauli matrices by i we get three skew-adjoint and unitary matrices with eigenvalues $\pm i$:*

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

that are also all unitarily equivalent. The 8 matrices

$$\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

form a group that corresponds to the quaternions $\pm 1, \pm i, \pm j, \pm k$.

EXAMPLE 89.

$$\begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$$

are not unitarily equivalent as the first is not normal while the second is normal. Note however that both are diagonalizable with the same eigenvalues.

5.1. Exercises.

(1) Decide which of the following matrices are unitarily equivalent

$$\begin{aligned} A &= \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \\ B &= \begin{bmatrix} 2 & 2 \\ 0 & 0 \end{bmatrix}, \\ C &= \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}, \\ D &= \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}. \end{aligned}$$

(2) Decide which of the following matrices are unitarily equivalent

$$\begin{aligned} A &= \begin{bmatrix} i & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\ B &= \begin{bmatrix} 1 & -1 & 0 \\ i & i & 1 \\ 0 & 1 & 1 \end{bmatrix}, \\ C &= \begin{bmatrix} 1 & 0 & 0 \\ 1 & i & 1 \\ 0 & 0 & 1 \end{bmatrix}, \\ D &= \begin{bmatrix} 1+i & -\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \end{aligned}$$

(3) Assume that $A, B \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ are unitarily equivalent. Show that if A has a square root, i.e., $A = C^2$ for some $C \in \mathrm{Mat}_{n\times n}(\mathbb{C})$, then also B has a square root.

(4) Assume that $A, B \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ are unitarily equivalent. Show that if A is positive, i.e., A is self-adjoint and has positive eigenvalues, then B is also positive.

(5) Assume that $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ is normal. Show that A is unitarily equivalent to A^* if and only if A is self-adjoint.

6. Real Forms

In this section we are going to explain the canonical forms for normal real linear operators that are not necessarily diagonalizable.

The idea is to follow the proof of the spectral theorem for complex normal operators. Thus we use induction on dimension to obtain the desired canonical forms. To get the induction going we decompose $L = B + C$, where $BC = CB$, B is self-adjoint and C is skew-adjoint. The spectral theorem can be applied to B and we observe that the eigenspaces for B are C-invariant, since $BC = CB$. Unless $B = \alpha 1_V$ we can therefore find a nontrivial orthogonal decomposition of V that reduces L. In case $B = \alpha 1_V$ all subspaces of V are B-invariant. Thus we use C to find invariant subspaces for L. To find such subspaces observe that C^2 is self-adjoint and select an eigenvector/value pair $C^2(x) = \lambda x$. Since C maps x to $C(x)$ and $C(x)$ to $C^2(x) = \lambda x$ the subspace $\mathrm{span}\{x, C(x)\}$ is invariant. If this subspace is 1-dimensional x is also an eigenvector for C, otherwise the subspace is 2-dimensional. All in all this shows that V can be decomposed into 1 and 2-dimensional subspaces that are invariant under B and C. As these subspaces are contained in the eigenspaces for B we only need to figure out how C acts on them. In the 1-dimensional case it is spanned by an eigenvector C. So the only case left to study is when $C : M \to M$ is skew-adjoint and M is 2-dimensional with no non-trivial invariant subspaces. In this case we just select a unit vector $x \in M$ and note that $C(x) \neq 0$ as x would otherwise span a 1-dimensional invariant subspace. In addition z and $C(z)$ are always perpendicular as

$$\begin{aligned}(C(z)|z) &= -(z|C(z)) \\ &= -(C(z)|z).\end{aligned}$$

In particular, x and $C(x)/\|C(x)\|$ form an orthonormal basis for M. In this basis the matrix representation for C is

$$\begin{bmatrix} C(x) & C\left(\frac{C(x)}{\|C(x)\|}\right) \end{bmatrix} = \begin{bmatrix} x & \frac{C(x)}{\|C(x)\|} \end{bmatrix} \begin{bmatrix} 0 & \gamma \\ \|C(x)\| & 0 \end{bmatrix}$$

as $C\left(\frac{C(x)}{\|C(x)\|}\right)$ is perpendicular to $C(x)$ and hence a multiple of x. Finally we get that $\gamma = -\|C(x)\|$ since the matrix has to be skew-symmetric.

This analysis shows what the canonical form for a normal real operator is.

THEOREM 38. (The Canonical Form for Real Normal Operators) *Let $L : V \to V$ be a normal operator, then we can find an orthonormal basis* $e_1, ..., e_k, x_1, y_1, ..., x_l, y_l$ *where* $k + 2l = n$ *and*

$$\begin{aligned}L(e_i) &= \lambda_i e_i, \\ L(x_j) &= \alpha_j x_j + \beta_j y_j, \\ L(y_j) &= -\beta_j x_j + \alpha_j y_j\end{aligned}$$

and $\lambda_i, \alpha_j, \beta_j \in \mathbb{R}$. *Thus* L *has the matrix representation*

$$\begin{bmatrix} \lambda_1 & \cdots & 0 & 0 & 0 & \cdots & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & & & \\ 0 & \cdots & \lambda_k & 0 & 0 & \cdots & & & \\ 0 & \cdots & 0 & \alpha_1 & -\beta_1 & 0 & \cdots & & \vdots \\ 0 & \cdots & 0 & \beta_1 & \alpha_1 & 0 & \cdots & & \\ & & & 0 & 0 & \ddots & & & \\ \vdots & & & & & & \ddots & 0 & 0 \\ & & & & & & 0 & \alpha_l & -\beta_l \\ 0 & & & \cdots & & & 0 & \beta_l & \alpha_l \end{bmatrix}$$

with respect to the basis $e_1, ..., e_k, x_1, y_1, ..., x_l, y_l$.

This yields two corollaries for skew-adjoint and orthogonal maps.

Corollary 33. (The Canonical Form for Real Skew-adjoint Operators) *Let* $L : V \to V$ *be a skew-adjoint operator, then we can find an orthonormal basis* $e_1, ..., e_k, x_1, y_1, ..., x_l, y_l$ *where* $k + 2l = n$ *and*

$$\begin{aligned} L(e_i) &= 0, \\ L(x_j) &= \beta_j y_j, \\ L(y_j) &= -\beta_j x_j \end{aligned}$$

and $\beta_j \in \mathbb{R}$. *Thus* L *has the matrix representation*

$$\begin{bmatrix} 0 & \cdots & 0 & 0 & 0 & \cdots & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & & & \\ 0 & \cdots & 0 & 0 & 0 & \cdots & & & \\ 0 & \cdots & 0 & 0 & -\beta_1 & 0 & \cdots & & \vdots \\ 0 & \cdots & 0 & \beta_1 & 0 & 0 & \cdots & & \\ & & & 0 & 0 & \ddots & & & \\ \vdots & & & & & & \ddots & 0 & 0 \\ & & & & & & 0 & 0 & -\beta_l \\ 0 & & & \cdots & & & 0 & \beta_l & 0 \end{bmatrix}$$

with respect to the basis $e_1, ..., e_k, x_1, y_1, ..., x_l, y_l$.

Corollary 34. (The Canonical Form for Orthogonal Operators) *Let* $O : V \to V$ *be an orthogonal operator, then we can find an orthonormal basis* $e_1, ..., e_k, x_1, y_1, ..., x_l, y_l$ *where* $k + 2l = n$ *and*

$$\begin{aligned} O(e_i) &= \pm e_i, \\ O(x_j) &= \cos(\theta_j) x_j + \sin(\theta_j) y_j, \\ O(y_j) &= -\sin(\theta_j) x_j + \cos(\theta_j) y_j \end{aligned}$$

and $\lambda_i, \alpha_j, \beta_j \in \mathbb{R}$. *Thus* L *has the matrix representation*

$$\begin{bmatrix} \pm 1 & \cdots & 0 & 0 & 0 & \cdots & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & & & \\ 0 & \cdots & \pm 1 & 0 & 0 & \cdots & & & \\ 0 & \cdots & 0 & \cos(\theta_1) & -\sin(\theta_1) & 0 & \cdots & & \vdots \\ 0 & \cdots & 0 & \sin(\theta_1) & \cos(\theta_1) & 0 & \cdots & & \\ & & & 0 & 0 & \ddots & & & \\ \vdots & & & & & & \ddots & 0 & 0 \\ & & & & & & 0 & \cos(\theta_l) & -\sin(\theta_l) \\ 0 & & & \cdots & & & 0 & \sin(\theta_l) & \cos(\theta_l) \end{bmatrix}$$

with respect to the basis $e_1, ..., e_k, x_1, y_1, ..., x_l, y_l$.

Proof. We just need to justify the specific form of the eigenvalues. We know that as a unitary operator all the eigenvalues look like $e^{i\theta}$. If they are real they must therefore be ± 1. Otherwise we use Euler's formula $e^{i\theta} = \cos\theta + i \sin\theta$ to get the desired form. □

Note that we can artificially group some of the matrices in the decomposition of the orthogonal operators by using

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix},$$

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} \cos\pi & -\sin\pi \\ \sin\pi & \cos\pi \end{bmatrix}$$

By paring off as many eigenvectors for ± 1 as possible we then obtain.

Corollary 35. *Let* $O : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ *be an orthogonal operator, then we can find an orthonormal basis where* L *has one of the following two types of the matrix representations*

Type I

$$\begin{bmatrix} \cos(\theta_1) & -\sin(\theta_1) & 0 & \cdots & 0 & 0 \\ \sin(\theta_1) & \cos(\theta_1) & 0 & \cdots & 0 & 0 \\ 0 & 0 & \ddots & & & \\ \vdots & \vdots & & \ddots & 0 & 0 \\ 0 & 0 & & 0 & \cos(\theta_n) & -\sin(\theta_n) \\ 0 & 0 & & 0 & \sin(\theta_n) & \cos(\theta_n) \end{bmatrix},$$

Type II

$$\begin{bmatrix} -1 & 0 & 0 & 0 & \cdots & & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & & 0 & 0 \\ 0 & 0 & \cos(\theta_1) & -\sin(\theta_1) & 0 & \cdots & & \vdots \\ 0 & 0 & \sin(\theta_1) & \cos(\theta_1) & 0 & \cdots & & \\ & & 0 & 0 & \ddots & & & \\ \vdots & \vdots & & & & \ddots & 0 & 0 \\ 0 & 0 & & & & 0 & \cos(\theta_{n-1}) & -\sin(\theta_{n-1}) \\ 0 & 0 & \cdots & & & 0 & \sin(\theta_{n-1}) & \cos(\theta_{n-1}) \end{bmatrix}.$$

Corollary 36. *Let $O : \mathbb{R}^{2n+1} \to \mathbb{R}^{2n+1}$ be an orthogonal operator, then we can find an orthonormal basis where L has one of the following two the matrix representations*

Type I

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \cos(\theta_1) & -\sin(\theta_1) & 0 & \cdots & & \vdots \\ 0 & \sin(\theta_1) & \cos(\theta_1) & 0 & \cdots & & \\ 0 & 0 & 0 & \ddots & & & \\ \vdots & & & & \ddots & 0 & 0 \\ 0 & & & & 0 & \cos(\theta_n) & -\sin(\theta_n) \\ 0 & \cdots & & & 0 & \sin(\theta_n) & \cos(\theta_n) \end{bmatrix}$$

Type II

$$\begin{bmatrix} -1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \cos(\theta_1) & -\sin(\theta_1) & 0 & \cdots & & \vdots \\ 0 & \sin(\theta_1) & \cos(\theta_1) & 0 & \cdots & & \\ 0 & 0 & 0 & \ddots & & & \\ \vdots & & & & \ddots & 0 & 0 \\ 0 & & & & 0 & \cos(\theta_n) & -\sin(\theta_n) \\ 0 & \cdots & & & 0 & \sin(\theta_n) & \cos(\theta_n) \end{bmatrix}.$$

Like with unitary equivalence we also have the concept of orthogonal equivalence. One can with the appropriate modifications prove similar results about when matrices are orthogonally equivalent. The above results apparently give us the simplest type of matrix that real normal, skew-adjoint, and orthogonal operators are orthogonally equivalent to.

Note that type I operators have the property that -1 has even multiplicity, while for type II -1 has odd multiplicity. In particular we note that type I is the same as saying that the determinant is 1 while type II means that the determinant is -1. The collection of orthogonal transformations of type I is denoted SO_n. This set is a *subgroup* of O_n, i.e., if $A, B \in SO_n$, then $AB \in SO_n$. This is not obvious given what we know now, but the proof is quite simple using determinants.

6.1. Exercises.

(1) Explain what the canonical form is for real linear maps that are both orthogonal and skew-adjoint.

(2) Let $L : V \to V$ be orthogonal on a real inner product space and assume that $\dim(\ker(L + 1_V))$ is even. Show that $L = K^2$ for some orthogonal K.

(3) Use the canonical forms to show
 (a) If $U \in U_n$, then $U = \exp(A)$ where A is skew-adjoint.
 (b) If $O \in O_n$ is of type I, then $O = \exp(A)$ where A is skew-symmetric.

(4) Let $L : V \to V$ be skew-adjoint on a real inner product space. Show that $L = K^2$ for some K. Can you do this with a skew-adjoint K?

(5) Let $A \in O_n$. Show that the following conditions are equivalent:
 (a) A has type I.
 (b) The product of the real eigenvalues is 1.
 (c) The product of all real and complex eigenvalues is 1.
 (d) $\dim(\ker(L + 1_{\mathbb{R}^n}))$ is even.
 (e) $\chi_A(t) = t^n + \cdots + a_1 t + (-1)^n$, i.e., the constant term is $(-1)^n$.

(6) Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ satisfy $AO = OA$ for all $O \in SO_n$.
 (a) If $n = 2$, then
$$A = \begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}.$$
 (b) If $n \geq 3$, then $A = \lambda 1_{\mathbb{R}^n}$.

(7) Let $L : \mathbb{R}^3 \to \mathbb{R}^3$ be skew-symmetric.
 (a) Show that there is a unique vector $w \in \mathbb{R}^3$ such that $L(x) = w \times x$. w is known as the Darboux vector for L.
 (b) Show that the assignment $L \to w$ gives a linear isomorphism from skew-symmetric 3×3 matrices to $\mathbb{R}^3$.
 (c) Show that if $L_1(x) = w_1 \times x$ and $L_2(x) = w_2 \times x$, then the commutator
$$[L_1, L_2] = L_1 \circ L_2 - L_2 \circ L_1$$
 satisfies
$$[L_1, L_2](x) = (w_1 \times w_2) \times x$$
 Hint: This corresponds to the Jacobi identity:
$$(x \times y) \times z + (z \times x) \times y + (y \times z) \times x = 0.$$
 (d) Show that
$$L(x) = w_2 (w_1|x) - w_1 (w_2|x)$$
 is skew-symmetric and that
$$(w_1 \times w_2) \times x = w_2 (w_1|x) - w_1 (w_2|x).$$
 (e) Conclude that all skew-symmetric $L : \mathbb{R}^3 \to \mathbb{R}^3$ are of the form
$$L(x) = w_2 (w_1|x) - w_1 (w_2|x).$$

(8) For $u_1, u_2 \in \mathbb{R}^n$.
 (a) Show that
$$L(x) = (u_1 \wedge u_2)(x) = (u_1|x) u_2 - (u_2|x) u_1$$
 defines a skew-symmetric operator.

(b) Show that:

$$\begin{aligned} u_1 \wedge u_2 &= -u_2 \wedge u_1 \\ (\alpha u_1 + \beta v_1) \wedge u_2 &= \alpha (u_1 \wedge u_2) + \beta (v_1 \wedge u_2) \end{aligned}$$

(c) Show Bianchi's identity: For all $x, y, z \in \mathbb{R}^n$ we have:

$$(x \wedge y)(z) + (z \wedge x)(y) + (y \wedge z)(x) = 0.$$

(d) When $n \geq 4$ show that not all skew-symmetric $L : \mathbb{R}^n \to \mathbb{R}^n$ are of the form $L(x) = u_1 \wedge u_2$. Hint: Let $u_1, ..., u_4$ be linearly independent and consider

$$L = u_1 \wedge u_2 + u_3 \wedge u_4.$$

(e) Show that the skew-symmetric operators $e_i \wedge e_j$, where $i < j$, form a basis for the skew-symmetric operators.

7. Orthogonal Transformations

In this section we are going to try to get a better grasp on orthogonal transformations.

We start by specializing the above canonical forms for orthogonal transformations to the two situations where things can be visualized, namely, in dimensions 2 and 3.

Corollary 37. *Any orthogonal operator $O : \mathbb{R}^2 \to \mathbb{R}^2$ has one of the following two forms in the standard basis:*
Either it is a rotation by θ and is of the form

$$\text{Type I: } \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix},$$

or it is a reflection in the line spanned by $(\cos\alpha, \sin\alpha)$ and has the form

$$\text{Type II: } \begin{bmatrix} \cos(2\alpha) & \sin(2\alpha) \\ \sin(2\alpha) & -\cos(2\alpha) \end{bmatrix}.$$

Moreover, O is a rotation if $\chi_O(t) = t^2 - (2\cos\theta)t + 1$ and θ is given by $\cos\theta = \frac{1}{2}\operatorname{tr} O$, while O is a reflection if $\operatorname{tr} O = 0$ and $\chi_O(t) = t^2 - 1$.

Proof. We know that there is an orthonormal basis x_1, x_2 that puts O into one of the two forms

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

We can write

$$x_1 = \begin{bmatrix} \cos(\alpha) \\ \sin(\alpha) \end{bmatrix}, x_2 = \pm \begin{bmatrix} -\sin(\alpha) \\ \cos(\alpha) \end{bmatrix}$$

The sign on x_2 can have an effect on the matrix representation as we shall see. In the case of the rotation it means a sign change in the angle, in the reflection case it doesn't change the form at all.

To find the form of the matrix in the usual basis we use the change of basis formula for matrix representations. Before doing this let us note that the law of exponents:

$$\exp(i(\theta + \alpha)) = \exp(i\theta)\exp(i\alpha)$$

tells us that the corresponding real 2×2 matrices satisfy:

$$\begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} = \begin{bmatrix} \cos(\alpha+\theta) & -\sin(\alpha+\theta) \\ \sin(\alpha+\theta) & \cos(\alpha+\theta) \end{bmatrix}$$

Thus

$$\begin{aligned} O &= \begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{bmatrix} \\ &= \begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{bmatrix} \\ &= \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \end{aligned}$$

as expected. If x_2 is changed to $-x_2$ we have

$$\begin{aligned} O &= \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix} \\ &= \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(-\theta) & \sin(-\theta) \\ -\sin(-\theta) & \cos(-\theta) \end{bmatrix} \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix} \\ &= \begin{bmatrix} \cos(\alpha-\theta) & \sin(\alpha-\theta) \\ \sin(\alpha-\theta) & -\cos(\alpha-\theta) \end{bmatrix} \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ -\sin(-\alpha) & -\cos(-\alpha) \end{bmatrix} \\ &= \begin{bmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{bmatrix} \end{aligned}$$

Finally the reflection has the form

$$\begin{aligned} O &= \begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{bmatrix} \\ &= \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{bmatrix} \\ &= \begin{bmatrix} \cos(2\alpha) & \sin(2\alpha) \\ \sin(2\alpha) & -\cos(2\alpha) \end{bmatrix}. \end{aligned}$$

□

Note that there is clearly an ambiguity in what it should mean to be a rotation by θ as either of the two matrices

$$\begin{bmatrix} \cos(\pm\theta) & -\sin(\pm\theta) \\ \sin(\pm\theta) & \cos(\pm\theta) \end{bmatrix}$$

describe such a rotation. What is more, the same orthogonal transformation can have different canonical forms depending on what basis we choose as we just saw in the proof of the above theorem. Unfortunately it isn't possible to sort this out without being very careful about the choice of basis, specifically one needs to additional concept of orientation which in turn uses determinants.

We now go to the three dimensional situation.

Corollary 38. *Any orthogonal operator $O : \mathbb{R}^3 \to \mathbb{R}^3$ is either*

Type I *a rotation in the plane that is perpendicular to the line representing the* $+1$ *eigenspace, or*

Type II *it is a rotation in the plane that is perpendicular to the* -1 *eigenspace followed by a reflection in that plane, corresponding to multiplying by* -1 *in the* -1 *eigenspace.*

As in the 2 dimensional situation we can also discover which case we are in by calculating the characteristic polynomial. For a rotation O in an axis we have

$$\begin{aligned}\chi_O(t) &= (t-1)\left(t^2-(2\cos\theta)\,t+1\right)\\ &= t^3-(1+2\cos\theta)\,t^2+(1+2\cos\theta)\,t-1\\ &= t^3-(\operatorname{tr}O)\,t^2+(\operatorname{tr}O)\,t-1,\end{aligned}$$

while the case involving a reflection

$$\begin{aligned}\chi_O(t) &= (t+1)\left(t^2-(2\cos\theta)\,t+1\right)\\ &= t^3-(-1+2\cos\theta)\,t^2-(-1+2\cos\theta)\,t+1\\ &= t^3-(\operatorname{tr}O)\,t^2-(\operatorname{tr}O)\,t+1.\end{aligned}$$

EXAMPLE 90. *Imagine a cube that is centered at the origin and so that the edges and sides are parallel to coordinate axes and planes. We note that all of the orthogonal transformations that either reflect in a coordinate plane or form* $90^\circ, 180^\circ, 270^\circ$ *rotations around the coordinate axes are symmetries of the cube. Thus the cube is mapped to itself via each of these isometries. In fact, the collection of all isometries that preserve the cube in this fashion is a (finite) group. It is evidently a subgroup of* O_3. *There are more symmetries than those already mentioned, namely, if we pick two antipodal vertices then we can rotate the cube into itself by* 120° *and* 240° *rotations around the line going through these two points. What is even more surprising is perhaps that these rotations can be obtained by composing the already mentioned* 90° *rotations. To see this let*

$$O_x=\begin{bmatrix}1&0&0\\0&0&-1\\0&1&0\end{bmatrix}, O_y=\begin{bmatrix}0&0&-1\\0&1&0\\1&0&0\end{bmatrix}$$

be 90° *rotations around the* x- *and* y-*axes respectively. Then*

$$\begin{aligned}O_xO_y &= \begin{bmatrix}1&0&0\\0&0&-1\\0&1&0\end{bmatrix}\begin{bmatrix}0&0&-1\\0&1&0\\1&0&0\end{bmatrix}=\begin{bmatrix}0&0&-1\\-1&0&0\\0&1&0\end{bmatrix}\\ O_yO_x &= \begin{bmatrix}0&0&-1\\0&1&0\\1&0&0\end{bmatrix}\begin{bmatrix}1&0&0\\0&0&-1\\0&1&0\end{bmatrix}=\begin{bmatrix}0&-1&0\\0&0&-1\\1&0&0\end{bmatrix}\end{aligned}$$

so we see that these two rotations do not commute. We now compute the (complex) eigenvalues via the characteristic polynomials in order to figure out what these new isometries look like. Since both matrices have zero trace they have characteristic polynomial

$$\chi(t)=t^3-1.$$

Thus they describe rotations where

$$\begin{aligned}\operatorname{tr}(O) &= 1+2\cos(\theta)=0, \text{ or}\\ \theta &= \pm\frac{2\pi}{3}.\end{aligned}$$

around the axis that corresponds to the 1 eigenvector. For O_xO_y we have that $(1,-1,-1)$ is an eigenvector for 1, while for O_yO_x we have $(-1,1,-1)$. These two eigenvectors describe the directions for two different diagonals in the cube. Completing, say, $(1,-1,-1)$ to an orthonormal basis for $\mathbb{R}^3$, then tells us that

$$
\begin{aligned}
O_xO_y &= \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{-1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} \\ \frac{-1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\left(\pm\frac{2\pi}{3}\right) & -\sin\left(\pm\frac{2\pi}{3}\right) \\ 0 & \sin\left(\pm\frac{2\pi}{3}\right) & \cos\left(\pm\frac{2\pi}{3}\right) \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{-1}{\sqrt{3}} & \frac{-1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{6}} & \frac{-1}{\sqrt{6}} & \frac{2}{\sqrt{6}} \end{bmatrix} \\
&= \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{-1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} \\ \frac{-1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \mp\frac{\sqrt{3}}{2} \\ 0 & \pm\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{-1}{\sqrt{3}} & \frac{-1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{6}} & \frac{-1}{\sqrt{6}} & \frac{2}{\sqrt{6}} \end{bmatrix} \\
&= \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{-1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} \\ \frac{-1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{-1}{\sqrt{3}} & \frac{-1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{6}} & \frac{-1}{\sqrt{6}} & \frac{2}{\sqrt{6}} \end{bmatrix}
\end{aligned}
$$

The fact that we pick $+$ rather than $-$ depends on our orthonormal basis as we can see by changing the basis by a sign in the last column:

$$
O_xO_y = \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} \\ \frac{-1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{-1}{\sqrt{3}} & 0 & \frac{-2}{\sqrt{6}} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{-1}{\sqrt{3}} & \frac{-1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{-1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{-2}{\sqrt{6}} \end{bmatrix}
$$

We are now ready to discuss how the two types of orthogonal transformations interact with each other when multiplied. Let us start with the 2 dimensional situation. One can directly verify that

$$
\begin{bmatrix} \cos\theta_1 & -\sin\theta_1 \\ \sin\theta_1 & \cos\theta_1 \end{bmatrix} \begin{bmatrix} \cos\theta_2 & -\sin\theta_2 \\ \sin\theta_2 & \cos\theta_2 \end{bmatrix} = \begin{bmatrix} \cos(\theta_1+\theta_2) & -\sin(\theta_1+\theta_2) \\ \sin(\theta_1+\theta_2) & \cos(\theta_1+\theta_2) \end{bmatrix},
$$

$$
\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{bmatrix} = \begin{bmatrix} \cos(\theta+\alpha) & \sin(\theta+\alpha) \\ \sin(\theta+\alpha) & -\cos(\theta+\alpha) \end{bmatrix},
$$

$$
\begin{bmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} \cos(\alpha-\theta) & \sin(\alpha-\theta) \\ \sin(\alpha-\theta) & -\cos(\alpha-\theta) \end{bmatrix},
$$

$$
\begin{bmatrix} \cos\alpha_1 & \sin\alpha_1 \\ \sin\alpha_1 & -\cos\alpha_1 \end{bmatrix} \begin{bmatrix} \cos\alpha_2 & \sin\alpha_2 \\ \sin\alpha_2 & -\cos\alpha_2 \end{bmatrix} = \begin{bmatrix} \cos(\alpha_1-\alpha_2) & -\sin(\alpha_1-\alpha_2) \\ \sin(\alpha_1-\alpha_2) & \cos(\alpha_1-\alpha_2) \end{bmatrix}.
$$

Thus we see that if the transformations are of the same type their product has type I, while if they have different type their product has type II. This is analogous to multiplying positive and negative numbers. This result actually holds in all dimensions and has a very simple proof using determinants. Euler proved this result in the 3-dimensional case without using determinants. What we are going to look into here is the observation that any rotation (type I) in O_2 is a product of two reflections. More specifically if $\theta = \alpha_1 - \alpha_2$, then the above calculation shows that

$$
\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} \cos\alpha_1 & \sin\alpha_1 \\ \sin\alpha_1 & -\cos\alpha_1 \end{bmatrix} \begin{bmatrix} \cos\alpha_2 & \sin\alpha_2 \\ \sin\alpha_2 & -\cos\alpha_2 \end{bmatrix}.
$$

To pave the way for a higher dimensional analogue of this we define $A \in O_n$ to be a *reflection* if it has the canonical form

$$A = O \begin{bmatrix} -1 & 0 & & 0 \\ 0 & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix} O^*.$$

This implies that BAB^* is also a reflection for all $B \in O_n$. To get a better picture of what A does we note that the -1 eigenvector gives the reflection in the hyperplane spanned by the $n-1$ dimensional $+1$ eigenspace. If z is a unit eigenvector for -1, then we can write A in the following way

$$A(x) = R_z(x) = x - 2(x|z)\,z.$$

To see why this is true first note that if x is an eigenvector for $+1$, then it is perpendicular to z and hence

$$x - 2(x|z)\,z = x$$

In case $x = z$ we have

$$\begin{aligned} z - 2(z|z)\,z &= z - 2z \\ &= -z \end{aligned}$$

as desired. We can now prove an interesting and important lemma.

Lemma 22. (E. Cartan) *Let $A \in O_n$. If A has type I, then A is a product of an even number of reflections, while if A has type II, then it is a product of an odd number of reflections.*

Proof. The canonical form for A can be expressed as follows:

$$A = OI_{\pm}R_1 \cdots R_l O^*,$$

where O is the orthogonal change of basis matrix, each R_i corresponds to a rotation on a two dimensional subspace M_i and

$$I_{\pm} = \begin{bmatrix} \pm 1 & 0 & & 0 \\ 0 & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}$$

where $+$ is used for type I and $-$ is used for type II. The above two dimensional construction shows that each rotation is a product of two reflections on M_i. If we extend these two dimensional reflections to be the identity on $M_i^{\perp}$, then they become reflections on the whole space. Thus we have

$$A = OI_{\pm}(A_1B_1)\cdots(A_lB_l)\,O^*,$$

where $I_{\pm}$ is either the identity or a reflection and $A_1, B_1, ..., A_l, B_l$ are all reflections. Finally

$$\begin{aligned} A &= OI_{\pm}(A_1B_1)\cdots(A_lB_l)\,O^* \\ &= (OI_{\pm}O^*)(OA_1O^*)(OB_1O^*)\cdots(OA_lO^*)(OB_lO^*). \end{aligned}$$

This proves the claim. □

The converse to this lemma is also true, namely, that any even number of reflection compose to a type I orthogonal transformation, while an odd numbers yields one of type II. This proof of this fact is very simple if one uses determinents.

7.1. Exercises.

(1) Decide the type and what the rotation and/or line of reflection is for each the matrices
$$\begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix},$$
$$\begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}.$$

(2) Decide on the type, ± 1 eigenvector and possible rotation angles on the orthogonal complement for the ± 1 eigenvector for the matrices:
$$\begin{bmatrix} -\frac{1}{3} & -\frac{2}{3} & -\frac{2}{3} \\ -\frac{2}{3} & -\frac{1}{3} & \frac{2}{3} \\ -\frac{2}{3} & \frac{2}{3} & -\frac{1}{3} \end{bmatrix},$$
$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$
$$\begin{bmatrix} \frac{2}{3} & -\frac{2}{3} & \frac{1}{3} \\ -\frac{2}{3} & -\frac{1}{3} & \frac{2}{3} \\ \frac{1}{3} & \frac{2}{3} & \frac{2}{3} \end{bmatrix},$$
$$\begin{bmatrix} \frac{1}{3} & \frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & -\frac{2}{3} & \frac{1}{3} \\ \frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \end{bmatrix}.$$

(3) Write the matrices from 1 and 2 as products of reflections.

(4) Let $O \in O_3$ and assume we have $u \in \mathbb{R}^3$ such that for all $x \in \mathbb{R}^3$
$$\frac{1}{2}\left(O - O^t\right)(x) = u \times x.$$
 (a) Show that u determines the axis of rotation by showing that: $O(u) = \pm u$.
 (b) Show that the rotation is determined by $|\sin\theta| = |u|$.
 (c) Show that for any $O \in O_3$ we can find $u \in \mathbb{R}^3$ such that the above formula holds.

(5) *(Euler)* Define the rotations around the three coordinate axes in $\mathbb{R}^3$ by
$$\begin{aligned} O_x(\alpha) &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{bmatrix}, \\ O_y(\beta) &= \begin{bmatrix} \cos\beta & 0 & -\sin\beta \\ 0 & 1 & 0 \\ \sin\beta & 0 & \cos\beta \end{bmatrix}, \\ O_z(\gamma) &= \begin{bmatrix} \cos\gamma & -\sin\gamma & 0 \\ \sin\gamma & \cos\gamma & 0 \\ 0 & 0 & 1 \end{bmatrix}. \end{aligned}$$

(a) Show that any $O \in SO(3)$ is of the form $O = O_x(\alpha) O_y(\beta) O_z(\gamma)$. The angles α, β, γ are called the *Euler angles* for O. Hint:

$$O_x(\alpha) O_y(\beta) O_z(\gamma) = \begin{bmatrix} \cos\beta\cos\gamma & -\cos\beta\sin\gamma & -\sin\beta \\ & & -\sin\alpha\cos\beta \\ & & \cos\alpha\sin\beta \end{bmatrix}$$

(b) Show that $O_x(\alpha) O_y(\beta) O_z(\gamma) \in SO(3)$ for all α, β, γ.
(c) Show that if $O_1, O_2 \in SO(3)$ then also $O_1 O_2 \in SO(3)$.

(6) Find the matrix representations with respect to the canonical basis for $\mathbb{R}^3$ for all of the orthogonal matrices that describe a rotation by θ in $\text{span}\{(1,1,0),(1,2,1)\}$.

(7) Let $z \in \mathbb{R}^n$ be a unit vector and

$$R_z(x) = x - 2(x|z)z$$

the reflection in the hyperplane perpendicular to z.
(a) Show that

$$\begin{aligned} R_z &= R_{-z}, \\ (R_z)^{-1} &= R_z. \end{aligned}$$

(b) If $y, z \in \mathbb{R}^n$ are linearly independent unit vectors, then show that $R_y R_z \in O_n$ is a rotation on $M = \text{span}\{y, z\}$ and the identity on $M^\perp$.
(c) Show that the angle θ of rotation is given by the relationship

$$\begin{aligned} \cos\theta &= -1 + 2\left|(y|z)\right|^2 \\ &= \cos(2\psi), \end{aligned}$$

where $(y|z) = \cos(\psi)$.

(8) Let Σ_n denote the group of permutations. These are the bijective maps from $\{1, 2, ..., n\}$ to itself. The group product is composition and inverses are the inverse maps. Show that the map defined by sending $\sigma \in \Sigma_n$ to the permutation matrix O_σ defined by $O_\sigma(e_i) = e_{\sigma(i)}$ is a group homomorphism

$$\Sigma_n \to O_n,$$

i.e., show $O_\sigma \in O_n$ and $O_{\sigma\circ\tau} = O_\sigma \circ O_\tau$. (See also the last example in "Linear Maps as Matrices").

(9) Let $A \in O_4$.
(a) Show that we can find a 2 dimensional subspace $M \subset \mathbb{R}^4$ such that M and $M^\perp$ are both invariant under A.
(b) Show that we can choose M so that $A|_{M^\perp}$ is rotation and $A|_M$ is a rotation precisely when A is type I while $A|_M$ is a reflection when A has type II.
(c) Show that if A has type I then

$$\begin{aligned} \chi_A(t) &= t^4 - 2(\cos(\theta_1) + \cos(\theta_2))t^3 \\ &\quad + (2 + 4\cos(\theta_1)\cos(\theta_2))t^2 - 2(\cos(\theta_1) + \cos(\theta_2))t + 1 \\ &= t^4 - (\text{tr}(A))t^3 + (2 + \text{tr}(A|_M)\,\text{tr}(A|_{M^\perp}))t^2 - (\text{tr}(A))t + 1, \end{aligned}$$

where $\text{tr}(A) = \text{tr}(A|_M) + \text{tr}(A|_{M^\perp})$.

(d) Show that if A has type II then

$$\begin{aligned}\chi_A(t) &= t^4 - (2\cos(\theta))\,t^3 + (2\cos\theta)\,t - 1\\ &= t^4 - (\operatorname{tr}(A))\,t^3 + (\operatorname{tr}(A))\,t - 1\\ &= t^4 - (\operatorname{tr}(A|_{M^\perp}))\,t^3 + (\operatorname{tr}(A|_{M^\perp}))\,t - 1.\end{aligned}$$

8. Triangulability

There is a result that gives a simple form for general complex linear maps in an orthonormal basis. The result is a sort of consolation prize for operators without any special properties relating to the inner product structure. This triagulability theorem gives a different proof of the Jordan-Chevalley decomposition for "The Jordan Canonical form" to the effect that a complex linear operator is the sum of two commuting operators, one which is diagonalizable and one which is nilpotent. In the subsequent sections on "The Singular Value Decomposition" and "The Polar Composition" we shall see some other simplified forms for general linear maps between inner product spaces.

Theorem 39. (Schur's Theorem) *Let $L : V \to V$ be a linear operator on a finite dimensional complex inner product space. It is possible to find an orthonormal basis $e_1, ..., e_n$ such that the matrix representation $[L]$ is upper triangular in this basis, i.e.,*

$$\begin{aligned}L &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} [L] \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^*\\ &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{nn} \end{bmatrix} \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}^*.\end{aligned}$$

Before discussing how to prove this result let us consider a few examples.

Example 91. *Note that*

$$\begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

are both in the desired form. The former matrix is diagonalizable but not with respect to an orthonormal basis. So within that framework we can't improve its canonical form. The latter matrix is not diagonalizable so there is nothing else to discuss.

Example 92. *Any 2×2 matrix A can be put into upper triangular form by finding an eigenvector e_1 and then selecting e_2 to be orthogonal to e_1. This is because we must have*

$$\begin{bmatrix} Ae_1 & Ae_2 \end{bmatrix} = \begin{bmatrix} e_1 & e_2 \end{bmatrix} \begin{bmatrix} \lambda & \beta \\ 0 & \gamma \end{bmatrix}.$$

Proof. *(of Schur's theorem)* Note that if we have the desired form

$$\begin{bmatrix} L(e_1) & \cdots & L(e_n) \end{bmatrix} = \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{nn} \end{bmatrix}$$

then we can construct a *flag* of invariant subspaces

$$\{0\} \subset V_1 \subset V_2 \subset \cdots \subset V_{n-1} \subset V,$$

where $\dim V_k = k$ and $L(V_k) \subset V_k$, defined by $V_k = \operatorname{span}\{e_1, ..., e_k\}$. Conversely given such a flag of subspaces we can find the orthonormal basis by selecting unit vectors $e_k \in V_k \cap V_{k-1}^{\perp}$.

In order to exhibit such a flag we use an induction argument along the lines of what we did when proving the spectral theorems for self-adjoint and normal operators. In this case the proof of Schur's theorem is reduced to showing that any complex linear map has an invariant subspace of dimension $\dim V - 1$. To see why this is true consider the adjoint $L^* : V \to V$ and select an eigenvalue/vector pair $L^*(y) = \mu y$. Then define $V_{n-1} = y^{\perp} = \{x \in V : (x|y) = 0\}$ and note that for $x \in V_{n-1}$ we have

$$\begin{aligned} (L(x)|y) &= (x|L^*(y)) \\ &= (x|\mu y) \\ &= \mu (x|y) \\ &= 0. \end{aligned}$$

Thus V_{n-1} is L invariant. □

Example 93. *Let*

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

To find the basis that puts A into upper triangular form we can always use an eigenvalue e_1 for A as the first vector. To use the induction we need one for A^* as well. Note however that if $Ax = \lambda x$ and $A^* y = \mu y$ then

$$\begin{aligned} \lambda (x|y) &= (\lambda x|y) \\ &= (Ax|y) \\ &= (x|A^* y) \\ &= (x|\mu y) \\ &= \bar{\mu} (x|y). \end{aligned}$$

So x and y are perpendicular as long as $\lambda \neq \bar{\mu}$. Having selected e_1 we should then select e_3 as an eigenvector for A^* where the eigenvalue is not conjugate to the one for e_1. Next we note that $e_3^{\perp}$ is invariant and contains e_1. Thus we can easily find $e_2 \in e_3^{\perp}$ as a vector perpendicular to e_1. This then gives the desired basis for A.

Now let us implement this on the original matrix. First note that 0 is not an eigenvalue for either matrix as $\ker(A) = \{0\} = \ker(A^*)$. *This is a little unlucky of course. Thus we must find λ such that $(A - \lambda 1_{\mathbb{C}^3})\, x = 0$ has a nontrivial solution.*

This means that we should study the augmented system

$$\begin{bmatrix} -\lambda & 0 & 1 & 0 \\ 1 & -\lambda & 0 & 0 \\ 1 & 1 & -\lambda & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & -\lambda & 0 \\ 1 & -\lambda & 0 & 0 \\ -\lambda & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & -\lambda & 0 \\ 0 & -\lambda-1 & \lambda & 0 \\ 0 & \lambda & 1-\lambda^2 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & -\lambda & 0 \\ 0 & \lambda & 1-\lambda^2 & 0 \\ 0 & \lambda+1 & -\lambda & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & -\lambda & 0 \\ 0 & \lambda & 1-\lambda^2 & 0 \\ 0 & 0 & -\lambda-\frac{\lambda+1}{\lambda}\left(1-\lambda^2\right) & 0 \end{bmatrix}$$

In order to find a nontrivial solution to the last equation the characteristic equation

$$\lambda\left(-\lambda-\frac{\lambda+1}{\lambda}\left(1-\lambda^2\right)\right)=\lambda^3-\lambda-1$$

must vanish. This is not a pretty equation to solve but we do know that it has a solution which is real. We run into the same equation when considering A^* and we know that we can find yet another solution that is either complex or a different real number. Thus we can conclude that we can put this matrix into upper triangular form. Despite the simple nature of the matrix the upper triangular form is not very pretty.

The theorem on triangulability evidently does not depend on our earlier theorems such as the spectral theorem. In fact all of those results can be re-proved using the theorem on triangulability. The spectral theorem itself can, for instance, be proved by simply observing that the matrix representation for a normal operator must be normal if the basis is orthonormal. But an upper triangular matrix can only be normal if it is diagonal.

One of the nice uses of Schur's theorem is to linear differential equations. Assume that we have a system $L(x)=\dot{x}-Ax=b$, where $A\in\mathrm{Mat}_{n\times n}(\mathbb{C}), b\in\mathbb{C}^n$. Then find a basis arranged as a matrix U so that U^*AU is upper triangular. If we let $x=Uy$, then the system can be rewritten as $U\dot{y}-AUy=b$, which is equivalent to solving

$$K(y)=\dot{y}-U^*AUy=U^*b.$$

Since U^*AU is upper triangular it will look like

$$\begin{bmatrix} \dot{y}_1 \\ \vdots \\ \dot{y}_{n-1} \\ \dot{y}_n \end{bmatrix} - \begin{bmatrix} \beta_{11} & \cdots & \beta_{1,n-1} & \beta_{1,n} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \beta_{n-1,n-1} & \beta_{n-1,n} \\ 0 & \cdots & 0 & \beta_{nn} \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_{n-1} \\ y_n \end{bmatrix} = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_{n-1} \\ \gamma_n \end{bmatrix}.$$

Now start by solving the last equation $\dot{y}_n-\beta_{nn}y_n=\gamma_n$ and then successively solve backwards using that we know how to solve linear equations of the form

$\dot{z} - \alpha z = f(t)$. Finally translate back to $x = U^* y$ to find x. Note that this also solves any particular initial value problem $x(t_0) = x_0$ as we know how to solve each of the systems with a fixed initial value at t_0. Specifically $\dot{z} - \alpha z = f(t)$, $z(t_0) = z_0$ has the unique solution

$$\begin{aligned} z(t) &= z_0 \exp(\alpha(t - t_0)) \int_{t_0}^{t} \exp(-\alpha(s - t_0)) f(s)\, ds \\ &= z_0 \exp(\alpha t) \int_{t_0}^{t} \exp(-\alpha s) f(s)\, ds. \end{aligned}$$

Note that the procedure only uses that A is a matrix whose entries are complex numbers. The constant b can in fact be allowed to have smooth functions as entries without changing a single step in the construction.

We could, of course, have used the Jordan canonical form as an upper triangular representative for A as well. The advantage of Schur's theorem is that the transition matrix is unitary and therefore easy to invert.

8.1. Exercises.

(1) Show that for any linear map $L : V \to V$ on an n-dimensional vector space, where the field of scalars $\mathbb{F} \subset \mathbb{C}$, we have $\operatorname{tr} L = \lambda_1 + \cdots + \lambda_n$, where $\lambda_1, ..., \lambda_n$ are the complex roots of $\chi_L(t)$ counted with multiplicities. Hint: First go to a matrix representation $[L]$, then consider this as a linear map on $\mathbb{C}^n$ and triangularize it.

(2) Let $L : V \to V$, where V is a real finite dimensional inner product space, and assume that $\chi_L(t)$ splits, i.e., all roots are real. Show that there is an orthonormal basis in which the matrix representation for L is upper triangular.

(3) Use Schur's theorem to prove that if $A \in \operatorname{Mat}_{n \times n}(\mathbb{C})$ and $\varepsilon > 0$, then we can find $A_\varepsilon \in \operatorname{Mat}_{n \times n}(\mathbb{C})$ such that $\|A - A_\varepsilon\| \leq \varepsilon$ and the n eigenvalues for A_ε are distinct. Conclude that any complex linear operator on a finite dimensional inner product space can be approximated by diagonalizable operators.

(4) Let $L : V \to V$ be a linear operator on a complex inner product space and let $p \in \mathbb{C}[t]$. Show that μ is an eigenvalue for $p(L)$ if and only if $\mu = p(\lambda)$ where λ is an eigenvalue for L.

(5) Show that a linear operator $L : V \to V$ on an n-dimensional inner product space is normal if and only if

$$\operatorname{tr}(L^* L) = |\lambda_1|^2 + \cdots + |\lambda_n|^2,$$

where $\lambda_1, ..., \lambda_n$ are the complex roots of the characteristic polynomial $\chi_L(t)$.

(6) Let $L : V \to V$ be an invertible linear operator on an n-dimensional complex inner product space. If $\lambda_1, ..., \lambda_n$ are the eigenvalues for L counted with multiplicities, then

$$\left\|L^{-1}\right\| \leq C_n \frac{\|L\|^{n-1}}{|\lambda_1| \cdots |\lambda_n|}$$

for some constant C_n that depends only on n. Hint: If $Ax = b$ and A is upper triangular show that there are constants

$$1 = C_{n,n} \leq C_{n,n-1} \leq \cdots \leq C_{n,1}$$

such that

$$\begin{aligned} |\xi_k| &\leq C_{n,k}\frac{\|b\|\,\|A\|^{n-k}}{|\alpha_{nn}\cdots\alpha_{kk}|}, \\ A &= \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{nn} \end{bmatrix}, \\ x &= \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix}. \end{aligned}$$

Then bound $L^{-1}(e_i)$ using that $L\left(L^{-1}(e_i)\right) = e_i$.

(7) Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ and $\lambda \in \mathbb{C}$ be given and assume that there is a unit vector x such that

$$\|Ax - \lambda x\| < \frac{\varepsilon^n}{C_n\,\|A - \lambda 1_V\|^{n-1}}.$$

Show that there is an eigenvalue λ' for A such that

$$\left|\lambda - \lambda'\right| < \varepsilon.$$

Hint: Use the above exercise to conclude that if

$$\begin{aligned} (A - \lambda 1_V)(x) &= b, \\ \|b\| &< \frac{\varepsilon^n}{C_n\,\|A - \lambda 1_V\|^{n-1}}. \end{aligned}$$

and all eigenvalues for $A - \lambda 1_V$ have absolute value $\geq \varepsilon$, then $\|x\| < 1$.

(8) Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ be given and assume that $\|A - B\| < \delta$ for some small δ.

(a) Show that all eigenvalues for A and B lie in the compact set $K = \{z : |z| \leq \|A\| + 1\}$.

(b) Show that if $\lambda \in K$ is no closer than ε to any eigenvalue for A, then

$$\left\|(\lambda 1_V - A)^{-1}\right\| < C_n\frac{(2\,\|A\| + 2)^{n-1}}{\varepsilon^n}.$$

(c) Using

$$\delta = \frac{\varepsilon^n}{C_n\,(2\,\|A\| + 2)^{n-1}}$$

show that any eigenvalue for B is within ε of some eigenvalue for A.

(d) Show that

$$\left\|(\lambda 1_V - B)^{-1}\right\| \leq C_n\frac{(2\,\|A\| + 2)^{n-1}}{\varepsilon^n}$$

and that any eigenvalue for A is within ε of an eigenvalue for B.

(9) Show directly that the solution to $\dot{z} - \alpha z = f(t)$, $z(t_0) = z_0$ is unique. Conclude that the initial value problems for systems of differential equations with constant coefficients have unique solutions.

(10) Find the general solution to the system $\dot{x} - Ax = b$, where

(a) $A = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$.

(b) $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$.

(c) $A = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}$.

9. The Singular Value Decomposition*

Using the results we have developed so far it is possible to obtain some very nice decompositions for general linear maps as well. First we treat the so called singular value decomposition. Note that general linear maps $L : V \to W$ do not have eigenvalues. The singular values of L that we define below are a good substitute for eigenvalues.

THEOREM 40. (The Singular Value Decomposition) *Let $L : V \to W$ be a linear map between finite dimensional inner product spaces. There is an orthonormal basis $e_1, ..., e_m$ for V such that $(L(e_i) | L(e_j)) = 0$ if $i \neq j$. Moreover, we can find orthonormal bases $e_1, ..., e_m$ for V and $f_1, ..., f_n$ for W so that*

$$\begin{aligned} L(e_1) &= \sigma_1 f_1, ..., L(e_k) = \sigma_k f_k, \\ L(e_{k+1}) &= \cdots = L(e_m) = 0 \end{aligned}$$

for some $k \leq m$. In particular,

$$\begin{aligned} L &= \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} [L] \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix}^* \\ &= \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} \begin{bmatrix} \sigma_1 & 0 & \cdots & & & \\ 0 & \ddots & 0 & & & \\ \vdots & 0 & \sigma_k & 0 & & \\ & & 0 & 0 & & \\ & & & & \ddots & \end{bmatrix} \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix}^* \end{aligned}$$

PROOF. Use the spectral theorem on $L^*L : V \to V$ to find an orthonormal basis $e_1, ..., e_m$ for V such that $L^*L(e_i) = \lambda_i e_i$. Then

$$(L(e_i) | L(e_j)) = (L^*L(e_i) | e_j) = (\lambda_i e_i | e_j) = \lambda_i \delta_{ij}.$$

Next reorder if necessary so that $\lambda_1, ..., \lambda_k \neq 0$ and define

$$f_i = \frac{L(e_i)}{\|L(e_i)\|}, i = 1, ..., k.$$

Finally select $f_{k+1}, ..., f_n$ so that we get an orthonormal basis for W.

In this way we see that $\sigma_i = \|L(e_i)\|$. Finally we must check that

$$L(e_{k+1}) = \cdots = L(e_m) = 0.$$

This is because $\|L(e_i)\|^2 = \lambda_i$ for all i. □

The values $\sigma = \sqrt{\lambda}$ where λ is an eigenvalue for L^*L are called the *singular values* of L. We often write the decomposition of L as follows

$$\begin{aligned}
L &= U\Sigma\tilde{U}^*, \\
U &= \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix}, \\
\tilde{U} &= \begin{bmatrix} e_1 & \cdots & e_m \end{bmatrix}, \\
\Sigma &= \begin{bmatrix} \sigma_1 & 0 & \cdots & & & \\ 0 & \ddots & 0 & & & \\ \vdots & 0 & \sigma_k & 0 & & \\ & & 0 & 0 & & \\ & & & & \ddots & \end{bmatrix}.
\end{aligned}$$

and we generally oder the singular values $\sigma_1 \geq \cdots \geq \sigma_k$.

The singular value decomposition gives us a nice way of studying systems $Lx = b$, when L isn't necessarily invertible. In this case L has a partial or generalized inverse called the *Moore-Penrose inverse*. The construction is quite simple. Take a linear map $L : V \to W$, then observe that $L|_{(\ker(L))^\perp} : (\ker(L))^\perp \to \operatorname{im}(L)$ is an isomorphism. Thus we can define the generalized inverse $L^\dagger : W \to V$ in such a way that

$$\begin{aligned}
\ker\left(L^\dagger\right) &= (\operatorname{im}(L))^\perp, \\
\operatorname{im}\left(L^\dagger\right) &= (\ker(L))^\perp, \\
L^\dagger|_{\operatorname{im}(L)} &= \left(L|_{(\ker(L))^\perp} : (\ker(L))^\perp \to \operatorname{im}(L)\right)^{-1}.
\end{aligned}$$

If we have picked orthonormal bases that yield the singular value decomposition, then

$$\begin{aligned}
L^\dagger(f_1) &= \sigma_1^{-1} f_1, ..., L^\dagger(f_k) = \sigma_k^{-1} f_k, \\
L^\dagger(f_{k+1}) &= \cdots = L^\dagger(f_n) = 0.
\end{aligned}$$

Using the singular value decomposition $L = U\Sigma\tilde{U}^*$ we can also define

$$L^\dagger = \tilde{U}\Sigma^\dagger U^*,$$

where

$$\Sigma^\dagger = \begin{bmatrix} \sigma_1^{-1} & 0 & \cdots & & & \\ 0 & \ddots & 0 & & & \\ \vdots & 0 & \sigma_k^{-1} & 0 & & \\ & & 0 & 0 & & \\ & & & & \ddots & \end{bmatrix}$$

This generalized inverse can now be used to try to solve $Lx = b$ for given $b \in W$. Before explaining how that works we list some of the important properties of the generalized inverse.

PROPOSITION 29. *Let $L : V \to W$ be a linear map between finite dimensional inner product spaces and $L^\dagger$ the Moore-Penrose inverse. Then*

(1) $(\lambda L)^\dagger = \lambda^{-1} L^\dagger$ *if* $\lambda \neq 0$.

(2) $\left(L^{\dagger}\right)^{\dagger} = L$.
(3) $(L^*)^{\dagger} = \left(L^{\dagger}\right)^*$.
(4) $LL^{\dagger}$ *is an orthogonal projection with* $\mathrm{im}\left(LL^{\dagger}\right) = \mathrm{im}(L)$ *and* $\ker\left(LL^{\dagger}\right) = \ker(L^*) = \ker\left(L^{\dagger}\right)$.
(5) $L^{\dagger}L$ *is an orthogonal projection with* $\mathrm{im}\left(L^{\dagger}L\right) = \mathrm{im}(L^*) = \mathrm{im}\left(L^{\dagger}\right)$ *and* $\ker\left(L^{\dagger}L\right) = \ker(L)$.
(6) $L^{\dagger}LL^{\dagger} = L^{\dagger}$.
(7) $LL^{\dagger}L = L$.

PROOF. All of these properties can be proven using the abstract definition. Instead we shall see how the matrix representation coming from the singular value decomposition can also be used to prove the results. Conditions 1-3 are straightforward to prove using that the singular value decomposition of L yields singular value decompositions of both $L^{\dagger}$ and L^*.

To prove 4 and 5 we use the matrix representation to see that

$$\begin{aligned} L^{\dagger}L &= \tilde{U}\Sigma^{\dagger}U^*U\Sigma\tilde{U}^* \\ &= \tilde{U}\begin{bmatrix} 1 & 0 & \cdots & & & \\ 0 & \ddots & 0 & & & \\ \vdots & 0 & 1 & 0 & & \\ & & 0 & 0 & & \\ & & & & \ddots & \end{bmatrix}\tilde{U}^* \end{aligned}$$

and similarly

$$LL^{\dagger} = U\begin{bmatrix} 1 & 0 & \cdots & & & \\ 0 & \ddots & 0 & & & \\ \vdots & 0 & 1 & 0 & & \\ & & 0 & 0 & & \\ & & & & \ddots & \end{bmatrix}U^*$$

This proves that these maps are orthogonal projections as the bases are orthonormal. It also yields the desired properties for kernels and images.

Finally 6,7 now follow via a similar calculation using the matrix representations. □

To solve $Lx = b$ for given $b \in W$ we can now use.

COROLLARY 39. *$Lx = b$ has a solution if and only if $b = LL^{\dagger}b$ and all solutions are given by*

$$x = L^{\dagger}b + \left(1_V - L^{\dagger}L\right)z,$$

where $z \in V$. Moreover the smallest solution is given by

$$x_0 = L^{\dagger}b.$$

In case $b \neq LL^{\dagger}b$, the best approximate solutions are given by

$$x = L^{\dagger}b + \left(1_V - L^{\dagger}L\right)z, z \in V$$

again with

$$x_0 = L^{\dagger}b$$

being the smallest.

PROOF. Since $LL^\dagger$ is the orthogonal projection onto $\operatorname{im}(L)$ we see that $b \in \operatorname{im}(L)$ if and only if $b = LL^\dagger b$. This means that $b = L\left(L^\dagger b\right)$ so that $x_0 = L^\dagger b$ is a solution to the system. Next we note that $\left(1_V - L^\dagger L\right)$ is the orthogonal projection onto $\left(\operatorname{im}(L^*)\right)^\perp = \ker(L)$. Thus all solutions are of the desired form. Finally as $L^\dagger b \in \operatorname{im}(L^*)$ the Pythagorean Theorem implies that

$$\left\|L^\dagger b + \left(1_V - L^\dagger L\right) z\right\|^2 = \left\|L^\dagger b\right\|^2 + \left\|\left(1_V - L^\dagger L\right) z\right\|^2$$

showing that

$$\left\|L^\dagger b\right\|^2 \leq \left\|L^\dagger b + \left(1_V - L^\dagger L\right) z\right\|^2$$

for all z.

The last statement is a consequence of the fact that $LL^\dagger b$ is the element in $\operatorname{im}(L)$ that is closest to b since $LL^\dagger$ is an orthogonal projection. □

9.1. Exercises.

(1) Show that the singular decomposition of a self-adjoint operator L with nonnegative eigenvalues looks like $U\Sigma U^*$ where the diagonal entries of Σ are the eigenvalues of L.

(2) Find the singular value decompositions of

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

(3) Find the generalized inverses to

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

(4) Let $L : V \to W$ be a linear operator between finite dimensional inner product spaces and $\sigma_1 \geq \cdots \geq \sigma_k$ the singular values of L. Show that the results of the section can be rephrased as follows: There exist orthonormal bases $e_1, ..., e_m$ for V and $f_1, ..., f_n$ for W such that

$$\begin{aligned} L(x) &= \sigma_1 (x|e_1) f_1 + \cdots + \sigma_k (x|e_k) f_k, \\ L^*(y) &= \sigma_1 (y|f_1) e_1 + \cdots + \sigma_k (y|f_k) e_k, \\ L^\dagger(y) &= \sigma_1^{-1} (y|f_1) e_1 + \cdots + \sigma_k^{-1} (y|f_k) e_k. \end{aligned}$$

(5) Let $L : V \to W$ be a linear operator on an n-dimensional inner product space. Show that L is an isometry if and only if $\ker(L) = \{0\}$ and all singular values are 1.

(6) Let $L : V \to W$ be a linear operator between finite dimensional inner product spaces. Show that

$$\|L\| = \sigma_1,$$

where σ_1 is the largest singular value of L.

(7) Let $L : V \to W$ be a linear operator between finite dimensional inner product spaces. If there are orthonormal bases $e_1, ..., e_m$ for V and $f_1, ..., f_n$ for W such that $L(e_i) = \tau_i f_i$, $i \leq k$ and $L(e_i) = 0$, $i > k$, then the τ_is are the singular values of L.

(8) Let $L : V \to W$ be a nontrivial linear operator between finite dimensional inner product spaces.

(a) If $e_1, ..., e_m$ is an orthonormal basis for V show that
$$\operatorname{tr}(L^*L) = \|L(e_1)\|^2 + \cdots + \|L(e_m)\|^2.$$
(b) If $\sigma_1 \geq \cdots \geq \sigma_k$ are the singular values for L show that
$$\operatorname{tr}(L^*L) = \sigma_1^2 + \cdots + \sigma_k^2.$$

10. The Polar Decomposition*

In this section we are going to study general linear operators $L : V \to V$. These can be decomposed in a manner similar to the polar coordinate decomposition of complex numbers: $z = e^{i\theta}|z|$.

THEOREM 41. (The Polar Decomposition) *Let $L : V \to V$ be a linear operator on an inner product space, then $L = WS$, where W is unitary (or orthogonal) and S is self-adjoint with nonnegative eigenvalues. Moreover, if L is invertible then W and S are uniquely determined by L.*

PROOF. The proof is similar to the construction of the singular value decomposition. In fact we can use the singular value decomposition to prove the polar decomposition:
$$\begin{aligned} L &= U\Sigma\tilde{U}^* \\ &= U\tilde{U}^*\tilde{U}\Sigma\tilde{U}^* \\ &= \left(U\tilde{U}^*\right)\left(\tilde{U}\Sigma\tilde{U}^*\right) \end{aligned}$$
Thus we let
$$\begin{aligned} W &= U\tilde{U}^*, \\ S &= \tilde{U}\Sigma\tilde{U}^* \end{aligned}$$
Clearly W is unitary as it is a composition of two isometries. And S is certainly self-adjoint with nonnegative eigenvalues as we have diagonalized it with an orthonormal basis and Σ has nonnegative diagonal entries.

Finally assume that L is invertible and
$$L = WS = \tilde{W}T$$
where $W, \tilde{W}$ are unitary and S, T are self-adjoint with positive eigenvalues. Then S and T must also be invertible and
$$\begin{aligned} ST^{-1} &= \tilde{W}W^{-1} \\ &= \tilde{W}W^*. \end{aligned}$$
This implies that ST^{-1} is unitary. Thus
$$\begin{aligned} \left(ST^{-1}\right)^{-1} &= \left(ST^{-1}\right)^* \\ &= (T^*)^{-1}S^* \\ &= T^{-1}S, \end{aligned}$$
and therefore
$$\begin{aligned} 1_V &= T^{-1}SST^{-1} \\ &= T^{-1}S^2T^{-1}. \end{aligned}$$
This means that $S^2 = T^2$. Since both operators are self-adjoint and have nonnegative eigenvalues this implies that $S = T$ and hence $\tilde{W} = W$ as desired. □

There is also an $L = SW$ decomposition, where $S = U\Sigma U^*$ and $W = U\tilde{U}^*$. From this it is clear that S and W need not be the same in the two decomposition unless $U = \tilde{U}$ in the singular value decomposition. This is equivalent to L being normal (see also exercises).

Recall from chapter 1 that we have the *general linear group* $Gl_n(\mathbb{F}) \subset \mathrm{Mat}_{n\times n}(\mathbb{F})$ of invertible $n \times n$ matrices. Further define $PS_n(\mathbb{F}) \subset \mathrm{Mat}_{n\times n}(\mathbb{F})$ as being the self-adjoint positive matrices, i.e., the eigenvalues are positive. The polar decomposition says that we have bijective (nonlinear) maps (i.e., one-to-one and onto maps)

$$\begin{aligned} Gl_n(\mathbb{C}) &\approx U_n \times PS_n(\mathbb{C}), \\ Gl_n(\mathbb{R}) &\approx O_n \times PS_n(\mathbb{R}), \end{aligned}$$

given by $A = WS \longleftrightarrow (W, S)$. These maps are in fact *homeomorphisms*, i.e., both $(W, S) \mapsto WS$ and $A = WS \mapsto (W, S)$ are continuous. The first map only involves matrix multiplication so it is obviously continuous. That $A = WS \to (W, S)$ is continuous takes a little more work. Assume that $A_k = W_k S_k$ and that $A_k \to A = WS \in Gl_n$. Then we need to show that $W_k \to W$ and $S_k \to S$. The space of unitary or orthogonal operators is compact. So any subsequence of W_k has a convergent subsequence. Now assume that $W_{k_l} \to \bar{W}$, then also $S_{k_l} = \left(W_{k_l}^*\right) A_{k_l} \to \bar{W}^* A$. Thus $A = \bar{W}\left(\bar{W}^* A\right)$, which implies by the uniqueness of the polar decomposition that $\bar{W} = W$ and $S_{k_l} \to S$. This means that convergent subsequences of W_k always converge to W, this in turn implies that $W_k \to W$. We then conclude that also $S_k \to S$ as desired.

Next we note that PS_n is a *convex cone*. This means that if $A, B \in PS_n$, then also $sA + tB \in PS_n$ for all $t, s > 0$. It is obvious that $sA + tB$ is self-adjoint. To see that all eigenvalues are positive we use that $(Ax|x), (Bx|x) > 0$ for all $x \neq 0$ to see that

$$((sA + tB)(x)|x) = s(Ax|x) + t(Bx|x) > 0.$$

The importance of this last observation is that we can deform any matrix $A = WS$ via

$$A_t = W(tI + (1-t)A) \in Gl_n$$

into a unitary or orthogonal matrix. This means that many *topological* properties of Gl_n can be investigated by studying the compact groups U_n and O_n.

An interesting example of this is that $Gl_n(\mathbb{C})$ is path connected, i.e., for any two matrices $A, B \in Gl_n(\mathbb{C})$ there is a continuous path $C : [0, \alpha] \to Gl_n(\mathbb{C})$ such that $C(0) = A$ and $C(\alpha) = B$. By way of contrast $Gl_n(\mathbb{R})$ has two path connected components. We can see these two facts for $n = 1$ as $Gl_1(\mathbb{C}) = \{\alpha \in \mathbb{C} : \alpha \neq 0\}$ is connected, while $Gl_1(\mathbb{R}) = \{\alpha \in \mathbb{R} : \alpha \neq 0\}$ consists of the two components corresponding the positive and negative numbers. For general n we can prove this by using the canonical form for unitary and orthogonal matrices. In the unitary situation we have that any $U \in U_n$ looks like

$$\begin{aligned} U &= BDB^* \\ &= B \begin{bmatrix} \exp(i\theta_1) & & 0 \\ & \ddots & \\ 0 & & \exp(i\theta_n) \end{bmatrix} B^*, \end{aligned}$$

where $B \in U_n$. Then define

$$D(t) = \begin{bmatrix} \exp(it\theta_1) & & 0 \\ & \ddots & \\ 0 & & \exp(it\theta_n) \end{bmatrix}.$$

Hence $D(t) \in U_n$ and $U(t) = BD(t)B^* \in U_n$ defines a path that at $t = 0$ is I and at $t = 1$ is U. Thus any unitary transformation can be joined to the identity matrix inside U_n.

In the orthogonal case we see using the real canonical form that a similar deformation using

$$\begin{bmatrix} \cos(t\theta_i) & -\sin(t\theta_i) \\ \sin(t\theta_i) & \cos(t\theta_i) \end{bmatrix}$$

will deform any orthogonal transformation to one of the following two matrices

$$\begin{bmatrix} 1 & 0 & & 0 \\ 0 & 1 & & 0 \\ & & \ddots & \\ 0 & 0 & & 1 \end{bmatrix} \text{ or } O \begin{bmatrix} -1 & 0 & & 0 \\ 0 & 1 & & 0 \\ & & \ddots & \\ 0 & 0 & & 1 \end{bmatrix} O^t.$$

Here

$$O \begin{bmatrix} -1 & 0 & & 0 \\ 0 & 1 & & 0 \\ & & \ddots & \\ 0 & 0 & & 1 \end{bmatrix} O^t$$

is the same as the reflection R_x where x is the first column vector in O (-1 eigenvector). We then have to show that $1_{\mathbb{R}^n}$ and R_x cannot be joined to each other inside O_n. This is done by contradiction. Thus assume that $A(t)$ is a continuous path with

$$\begin{aligned} A(0) &= \begin{bmatrix} 1 & 0 & & 0 \\ 0 & 1 & & 0 \\ & & \ddots & \\ 0 & 0 & & 1 \end{bmatrix}, \\ A(1) &= O \begin{bmatrix} -1 & 0 & & 0 \\ 0 & 1 & & 0 \\ & & \ddots & \\ 0 & 0 & & 1 \end{bmatrix} O^t, \\ A(t) &\in O_n, \text{ for all } t \in [0,1]. \end{aligned}$$

The characteristic polynomial

$$\chi_{A(t)}(\lambda) = t^n + \cdots + a_0(t)$$

has coefficients that vary continuously with t (the proof of this uses determinants). However, $a_0(0) = (-1)^n$, while $a_0(1) = (-1)^{n-1}$. Thus the Intermediate Value Theorem tells us that $a_0(t_0) = 0$ for some $t_0 \in (0,1)$. But this implies that $\lambda = 0$ is a root of $A(t_0)$, thus contradicting that $A(t_0) \in O_n \subset Gl_n$.

10.1. Exercises.

(1) Find the polar decomposition for

$$\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}, \text{ and } \begin{bmatrix} \alpha & 1 \\ 0 & \alpha \end{bmatrix}$$

(2) Find the polar decomposition for

$$\begin{bmatrix} 0 & \beta & 0 \\ \alpha & 0 & 0 \\ 0 & 0 & \gamma \end{bmatrix} \text{ and } \begin{bmatrix} 1 & -1 & 0 \\ 0 & 0 & 2 \\ 1 & 1 & 0 \end{bmatrix}.$$

(3) If $L : V \to V$ is a linear operator on an inner product space. Define the *Cayley transform* of L as $(L + 1_V)(L - 1_V)^{-1}$.
   (a) If L is skew-adjoint show that $(L + 1)(L - 1)^{-1}$ is an isometry that does not have -1 as an eigenvalue.
   (b) Show that $U \to (U - 1_V)(U + 1_V)^{-1}$ takes isometries that do not have -1 as an eigenvalue to skew-adjoint operators and is an inverse to the Cayley transform.

(4) Let $L : V \to V$ be a linear operator on an inner product space. Show that $L = SW$, where W is unitary (or orthogonal) and S is self-adjoint with nonnegative eigenvalues. Moreover, if L is invertible then W and S are unique. Show by example that the operators in this polar decomposition do not have to be the same as in the $L = WS$ decomposition.

(5) Let $L = WS$ be the unique polar decomposition of an invertible operator $L : V \to V$ on a finite dimensional inner product space V. Show that L is normal if and only if $WS = SW$.

(6) The purpose of this exercise is to check some properties of the exponential map $\exp : \text{Mat}_{n\times n}(\mathbb{F}) \to Gl_n(\mathbb{F})$. You may want to consult "Matrix Exponentials" in Chapter 3 for the definition and various elementary properties.
   (a) Show that exp maps normal operators to normal operators.
   (b) Show that exp maps self-adjoint operators to positive self-adjoint operators and that it is a homeomorphism, i.e., it is one-to-one, onto, continuous and the inverse is also continuous.
   (c) Show that exp maps skew-adjoint operators to isometries, but is not one-to-one. In the complex case show that it is onto.

(7) Let $L : V \to V$ be normal and $L = S + A$, where S is self-adjoint and A skew-adjoint. Recall that since L is normal S and A commute.
   (a) Show that $\exp(S)\exp(A) = \exp(A)\exp(S)$ is the polar decomposition of $\exp(L)$.
   (b) Show that any invertible normal transformation can be written as $\exp(L)$ for some normal L.

11. Quadratic Forms*

Conic sections are those figures we obtain by intersecting a cone with a plane. Analytically this is the problem of determining all of the intersections of a cone given by $z = x^2 + y^2$ with a plane $z = ax + by + c$.

We can picture what these intersections look like by shining a flash light on a wall. The light emanating from the flash light describes a cone which is then intersected by the wall. The figures we get are circles, ellipses, parabolae and hyperbolae, depending on how we hold the flash light.

These questions naturally lead to the more general question of determining the figures described by the equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

We shall see below that it is possible to make a linear change of coordinates, that depends only on the quadratic quantities, such that the equation is transformed into an equation of the simpler form

$$a'(x')^2 + c'(y')^2 + d'x' + e'y' + f' = 0.$$

It is now easy to see that the solutions to such an equation consist of a circle, ellipse, parabola, hyperbola, or the degenerate cases of two lines, a point or nothing. Moreover a, b, c together determine the type of the figure as long as it isn't degenerate.

Aside from the esthetical virtues of this problem, it also comes up naturally when solving the two-body problem from physics. A rather remarkable coincidence between beauty and the real world. Another application is to the problem of deciding when a function in two variables has a maximum, minimum, or neither at a critical point.

The goal here is to study this problem in the more general case with n variables and show how the Spectral Theorem can be brought in to help our investigations. We shall also explain the use in multivariable calculus.

A *quadratic form* Q in n real variables $x = (x_1, ..., x_n)$ is a function of the form

$$Q(x) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j.$$

The term $x_i x_j$ only appears once in this sum. We can artificially have it appear twice so that the sum is more symmetric

$$Q(x) = \sum_{i,j=1}^{n} a'_{ij} x_i x_j,$$

where $a'_{ii} = a_{ii}$ and $a'_{ij} = a'_{ji} = a_{ij}/2$. If we define A as the matrix whose entries are a'_{ij} and use the inner product on $\mathbb{R}^n$, then the quadratic form can be written in the more abstract and condensed form

$$Q(x) = (Ax|x).$$

The important observation is that A is a symmetric real matrix and hence self-adjoint. This means that we can find a new orthonormal basis for $\mathbb{R}^n$ that diagonalizes A. If this basis is given by the matrix B, then

$$\begin{aligned} A &= BDB^{-1} \\ &= B \begin{bmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_n \end{bmatrix} B^{-1} \\ &= B \begin{bmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_n \end{bmatrix} B^t \end{aligned}$$

If we define new coordinates by

$$\begin{aligned}\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} &= B^{-1}\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \text{ or} \\ x &= By,\end{aligned}$$

then

$$\begin{aligned} Q(x) &= (Ax|x) \\ &= (ABy|By) \\ &= \left(B^tABy|y\right) \\ &= Q'(y). \end{aligned}$$

Since B is an orthogonal matrix we have that $B^{-1} = B^t$ and hence $B^tAB = B^{-1}AB = D$. Thus

$$Q'(y) = \sigma_1 y_1^2 + \cdots + \sigma_n y_n^2$$

in the new coordinates.

The general classification of the types of quadratic forms is given by

(1) If all of $\sigma_1, ..., \sigma_n$ are positive or negative, then it is said to be *elliptic*.
(2) If all of $\sigma_1, ..., \sigma_n$ are nonzero and there are both negative and positive values, then it said to be *hyperbolic*.
(3) If at least one of $\sigma_1, ..., \sigma_n$ is zero, then it is called *parabolic*.

In the case of two variables this makes perfect sense as $x^2 + y^2 = r^2$ is a circle (special ellipse), $x^2 - y^2 = f$ two branches of a hyperbola, and $x^2 = f$ a parabola. The first two cases occur when $\sigma_1 \cdots \sigma_n \neq 0$. In this case the quadratic form is said to be *nondegenerate*. In the parabolic case $\sigma_1 \cdots \sigma_n = 0$ and we say that the quadratic form is degenerate.

Having obtained this simple classification it would be nice to find a way of characterizing these types directly from the characteristic polynomial of A without having to find the roots. This is actually not too hard to accomplish.

Lemma 23. (Descartes' Rule of Signs) *Let*

$$p(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 = (t - \lambda_1)\cdots(t - \lambda_n),$$

where $a_0, ..., a_{n-1}, \lambda_1, ..., \lambda_n \in \mathbb{R}$.

(1) 0 *is a root of* $p(t)$ *if and only if* $a_0 = 0$.
(2) *All roots of* $p(t)$ *are negative if and only if* $a_{n-1}, ..., a_0 > 0$.
(3) *If* n *is odd, then all roots of* $p(t)$ *are positive if and only if* $a_{n-1} < 0$, $a_{n-2} > 0, ..., a_1 > 0$, $a_0 < 0$.
(4) *If* n *is even, then all roots of* $p(t)$ *are positive if and only if* $a_{n-1} < 0$, $a_{n-2} > 0, ..., a_1 < 0$, $a_0 > 0$.

Proof. Descartes rule is actually more general as it relates the number of positive roots to the number of times the coefficients change sign. The simpler version, however, suffices for our purposes.

Part 1 is obvious as $p(0) = a_0$.

The relationship

$$t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 = (t - \lambda_1)\cdots(t - \lambda_n)$$

clearly shows that $a_{n-1}, ..., a_0 > 0$ if $\lambda_1, ..., \lambda_n < 0$. Conversely if $a_{n-1}, ..., a_0 > 0$, then it is obvious that $p(t) > 0$ for all $t \geq 0$.

For the other two properties consider $q(t) = p(-t)$ and use 2. □

This lemma gives us a very quick way of deciding whether a given quadratic form is parabolic or elliptic. If it is not one of these two types, then we know it has to be hyperbolic.

We can now begin to apply this to multivariable calculus. First let us consider a function of the form $f(x) = a + Q(x)$, where Q is a quadratic form. We note that $f(0) = a$ and that $\frac{\partial f}{\partial x_i}(0) = 0$ for $i = 1, ..., n$. Thus the origin is a critical point for f. The type of the quadratic form will now tell us whether 0 is a maximum, minimum, or neither. Let us assume that Q is nondegenerate. If $0 > \sigma_1 \geq \cdots \geq \sigma_n$, then $f(x) \leq a + \sigma_1 ||x||^2 \leq a$ and 0 is a maximum for f. On the other hand if $\sigma_1 \geq \cdots \geq \sigma_n > 0$, then $f(x) \geq a + \sigma_n ||x||^2 \geq a$ and 0 is a minimum for f. In case $\sigma_1, ..., \sigma_n$ have both signs 0 is neither a minimum or a maximum. Clearly f will increase in directions where $\sigma_i > 0$ and decrease where $\sigma_i < 0$. In such a situation we say that f has a *saddle point*. In the parabolic case we can do a similar analysis, but as we shall see it won't do us any good for more general functions.

In general we can study a smooth function $f : \mathbb{R}^n \to \mathbb{R}$ at a critical point x_0, i.e., $df_{x_0} = 0$. The Taylor expansion up to order 2 tells us that

$$f(x_0 + h) = f(x_0) + \sum_{i,j=1}^{n} \frac{\partial^2 f}{\partial x_i \partial x_j}(x_0) h_i h_j + o\left(\|h\|^2\right),$$

where $o\left(||h||^2\right)$ is a function of x_0 and h with the property that

$$\lim_{h \to 0} \frac{o\left(\|h\|^2\right)}{\|h\|^2} = 0.$$

Using $A = \left[\frac{\partial^2 f}{\partial x_i \partial x_j}(x_0)\right]$ the second derivative term therefore looks like a quadratic form in h. We can now prove

THEOREM 42. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a smooth function that has a critical point at x_0 with $\sigma_1 \geq \cdots \geq \sigma_n$ the eigenvalues for the symmetric matrix $\left[\frac{\partial^2 f}{\partial x_i \partial x_j}(x_0)\right]$.*

(1) *If $\sigma_n > 0$, then x_0 is a local minimum for f.*
(2) *If $\sigma_1 < 0$, then x_0 is a local maximum for f.*
(3) *If $\sigma_1 > 0$ and $\sigma_n < 0$, then f has a saddle point at x_0.*
(4) *Otherwise there is no conclusion about f at x_0.*

PROOF. Case 1 and 2 have similar proofs so we emphasize 1 only. Choose a neighborhood around x_0 where

$$\left|\frac{o\left(\|h\|^2\right)}{\|h\|^2}\right| \leq \sigma_n.$$

In this neighborhood we have

$$\begin{aligned} f(x_0+h) &= f(x_0)+\sum_{i,j=1}^{n}\frac{\partial^2 f}{\partial x_i\partial x_j}(x_0)\,h_ih_j+o\left(\|h\|^2\right)\\ &\geq f(x_0)+\sigma_n\,\|h\|^2+\frac{o\left(\|h\|^2\right)}{\|h\|^2}\|h\|^2\\ &= f(x_0)+\left(\sigma_n+\frac{o\left(\|h\|^2\right)}{\|h\|^2}\right)\|h\|^2\\ &\geq f(x_0)\end{aligned}$$

as desired.

In case 3 select unit eigenvectors v_1 and v_n corresponding to σ_1 and σ_n. Then

$$f(x_0+tv_i)=f(x_0)+t^2\sigma_i+o\left(t^2\right).$$

As we have

$$\lim_{t\to 0}\frac{o\left(t^2\right)}{t^2}=0,$$

this formula implies that $f(x_0+tv_1)>f(x_0)$ for small t while $f(x_0+tv_n)<f(x_0)$ for small t. This means that f does not have a local maximum or minimum at x_0. □

Example 94. *Let $f(x,y,z)=x^2-y^2+3xy-z^2+4yz$. The derivative is given by $(2x+3y,-2y+3x+4z,-2z+4y)$. To see when this is zero we have to solve*

$$\begin{bmatrix}2&3&0\\3&-2&4\\0&4&-2\end{bmatrix}\begin{bmatrix}x\\y\\z\end{bmatrix}=\begin{bmatrix}0\\0\\0\end{bmatrix}$$

One quickly sees that $(0,0,0)$ is the only solution. We now wish to check what type of critical point this is. Thus we compute the second derivative matrix

$$\begin{bmatrix}2&3&0\\3&-2&4\\0&4&-2\end{bmatrix}$$

The characteristic polynomial is $t^3+2t^2-29t+6$. The coefficients do not conform to the patterns that guarantee that the roots are all positive or negative so we conclude that the origin is a saddle point.

Example 95. *The function $f(x,y)=x^2\pm y^4$ has a critical point at $(0,0)$. The second derivative matrix is*

$$\begin{bmatrix}2&0\\0&\pm 12y^2\end{bmatrix}.$$

When $y=0$, this is of parabolic type so we can't conclude what type of critical point it is. In reality it is a minimum when $+$ is used and a saddle point when $-$ is used in the definition for f.

EXAMPLE 96. *Let Q be a quadratic form corresponding to the matrix*

$$A = \begin{bmatrix} 6 & 1 & 2 & 3 \\ 1 & 5 & 0 & 4 \\ 2 & 0 & 2 & 0 \\ 3 & 4 & 0 & 7 \end{bmatrix}$$

The characteristic polynomial is given by $t^4 - 20t^3 + 113t^2 - 200t + 96$. Here we see that the coefficients tells us that the roots must be positive.

11.1. Exercises.

(1) A bilinear form on a vector space V is a function $B : V \times V \to \mathbb{F}$ such that $x \to B(x,y)$ and $y \to B(x,y)$ are both linear. Show that a quadratic form Q always looks like $Q(x) = B(x,x)$, where B is a bilinear form.

(2) A bilinear form is said to be symmetric, respectively skew-symmetric, if $B(x,y) = B(y,x)$, respectively $B(x,y) = -B(y,x)$ for all x, y.
   (a) Show that a quadratic form looks like $Q(x) = B(x,x)$ where B is symmetric.
   (b) Show that $B(x,x) = 0$ for all $x \in V$ if and only if B is skew-symmetric.

(3) Let B be a bilinear form on $\mathbb{R}^n$ or $\mathbb{C}^n$.
   (a) Show that $B(x,y) = (Ax|y)$ for some matrix A.
   (b) Show that B is symmetric if and only if A is symmetric.
   (c) Show that B is skew-symmetric if and only if A is skew-symmetric.
   (d) If $x = Cx'$ is a change of basis show that if B corresponds to A in the standard basis, then it corresponds to $C^t AC$ in the new basis.

(4) Let $Q(x)$ be a quadratic form on $\mathbb{R}^n$. Show that there is an orthogonal basis where

$$Q(z) = -z_1^2 - \cdots - z_k^2 + z_{k+1}^2 + \cdots + z_l^2,$$

where $0 \leq k \leq l \leq n$. Hint: Use the orthonormal basis that diagonalized Q and adjust the lengths of the basis vectors.

(5) Let $B(x,y)$ be a skew-symmetric form on $\mathbb{R}^n$.
   (a) If $B(x,y) = (Ax|y)$ where $A = \begin{bmatrix} 0 & -\beta \\ \beta & 0 \end{bmatrix}$, $\beta \in \mathbb{R}$, then show that there is a basis for $\mathbb{R}^2$ where $B(x', y')$ corresponds to $A' = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.
   (b) If $B(x,y)$ is a skew-symmetric bilinear form on $\mathbb{R}^n$, then there is a basis where $B(x', y')$ corresponds to a matrix of the type

$$A' = \begin{bmatrix} 0 & -1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & \vdots & 0 \\ \vdots & \vdots & \ddots & 0 & 0 & 0 & \vdots & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

(6) Show that for a quadratic form $Q(z)$ on $\mathbb{C}^n$ we can always change coordinates to make it look like

$$Q'(z') = (z'_1)^2 + \cdots + (z'_n)^2.$$

(7) Show that $Q(x, y) = ax^2 + 2bxy + cy^2$ is elliptic when $ac - b^2 > 0$, hyperbolic when $ac - b^2 < 0$, and parabolic when $ac - b^2 = 0$.

(8) If A is a symmetric real matrix, then show that $tI + A$ defines an elliptic quadratic form when $|t|$ is sufficiently large.

(9) Decide for each of the following matrices whether or not the corresponding quadratic form is elliptic, hyperbolic, or parabolic.

(a) $$\begin{bmatrix} -7 & -2 & -3 & 0 \\ -2 & -6 & -4 & 0 \\ -3 & -4 & -5 & 2 \\ 0 & 0 & 2 & -3 \end{bmatrix}.$$

(b) $$\begin{bmatrix} 7 & 3 & -3 & 4 \\ 3 & 2 & -1 & 0 \\ -3 & -1 & 5 & -2 \\ 4 & 0 & -2 & 10 \end{bmatrix}.$$

(c) $$\begin{bmatrix} -8 & -3 & 0 & -2 \\ -3 & -1 & -1 & 0 \\ 0 & -1 & 1 & 3 \\ -2 & 0 & 3 & -3 \end{bmatrix}.$$

(d) $$\begin{bmatrix} 15 & 2 & 3 & 4 \\ 2 & 4 & 2 & 0 \\ 3 & 2 & 3 & -2 \\ 4 & 0 & -2 & 5 \end{bmatrix}.$$

CHAPTER 5

Determinants

1. Geometric Approach

Before plunging in to the theory of determinants we are going to make an attempt at defining them in a more geometric fashion. This works well in low dimensions and will serve to motivate our more algebraic constructions in subsequent sections.

From a geometric point of view the determinant of a linear operator $L : V \to V$ is a scalar $\det(L)$ that measures how L changes the volume of solids in V. To understand how this works we obviously need to figure out how volumes are computed in V. In this section we will study this problem in dimensions 1 and 2. In subsequent sections we take a more axiomatic and algebraic approach, but the ideas come from what we have presented here.

Let V be 1-dimensional and assume that the scalar field is $\mathbb{R}$ so as to keep things as geometric as possible. We already know that $L : V \to V$ must be of the form $L(x) = \lambda x$ for some $\lambda \in \mathbb{R}$. This λ clearly describes how L changes the length of vectors as $||L(x)|| = |\lambda| \, ||x||$. The important and surprising thing to note is that while we need an inner product to compute the length of vectors it is not necessary to know the norm in order to compute how L changes the length of vectors.

Let now V be 2-dimensional. If we have a real inner product, then we can talk about areas of simple geometric configurations. We shall work with parallelograms as they are easy to define, one can easily find their area, and linear operators map parallelograms to parallelograms. Given $x, y \in V$ the parallelogram $\pi(x, y)$ with sides x and y is defined by

$$\pi(x, y) = \{sx + ty : s, t \in [0, 1]\}.$$

The area of $\pi(x, y)$ can be computed by the usual formula where one multiplies the base length with the height. If we take x to be the base, then the height is the projection of y onto to orthogonal complement of x. Thus we get the formula

$$\begin{aligned} \operatorname{area}(\pi(x, y)) &= \|x\| \, \|y - \operatorname{proj}_x(y)\| \\ &= \|x\| \left\| y - \frac{(y|x)\, x}{||x||^2} \right\|. \end{aligned}$$

This expression does not appear to be symmetric in x and y, but if we square it we get

$$\begin{aligned}
(\text{area}\,(\pi\,(x,y)))^2 &= (x|x)\,(y-\text{proj}_x\,(y)\,|y-\text{proj}_x\,(y)) \\
&= (x|x)\,((y|y)-2\,(y|\,\text{proj}_x\,(y))+(\text{proj}_x\,(y)\,|\,\text{proj}_x\,(y))) \\
&= (x|x)\left((y|y)-2\left(y\left|\frac{(y|x)\,x}{\|x\|^2}\right.\right)+\left(\frac{(y|x)\,x}{\|x\|^2}\left|\frac{(y|x)\,x}{\|x\|^2}\right.\right)\right) \\
&= (x|x)\,(y|y)-(x|y)^2\,,
\end{aligned}$$

which is symmetric in x and y. Now assume that

$$\begin{aligned}
x' &= \alpha x+\beta y \\
y' &= \gamma x+\delta y
\end{aligned}$$

or

$$\begin{bmatrix} x' & y' \end{bmatrix} = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}$$

then we see that

$$\begin{aligned}
&(\text{area}\,(\pi\,(x',y')))^2 \\
=\;& (x'|x')\,(y'|y')-(x'|y')^2 \\
=\;& (\alpha x+\beta y|\alpha x+\beta y)\,(\gamma x+\delta y|\gamma x+\delta y)-(\alpha x+\beta y|\gamma x+\delta y)^2 \\
=\;& \left(\alpha^2\,(x|x)+2\alpha\beta\,(x|y)+\beta^2\,(y|y)\right)\left(\gamma^2\,(x|x)+2\gamma\delta\,(x|y)+\delta^2\,(y|y)\right) \\
&-(\alpha\gamma\,(x|x)+(\alpha\delta+\beta\gamma)\,(x|y)+\beta\delta\,(y|y))^2 \\
=\;& \left(\alpha^2\delta^2+\beta^2\gamma^2-2\alpha\beta\gamma\delta\right)\left((x|x)\,(y|y)-(x|y)^2\right) \\
=\;& (\alpha\delta-\beta\gamma)^2\,(\text{area}\,(\pi\,(x,y)))^2\,.
\end{aligned}$$

This tells us several things. First, if we know how to compute the area of just one parallelogram, then we can use linear algebra to compute the area of any other parallelogram by simply expanding the base vectors for the new parallelogram in terms of the base vectors of the given parallelogram. This has the surprising consequence that the ratio of the areas of two parallelograms does not depend upon the inner product! With this in mind we can then define the determinant of a linear operator $L : V \to V$ so that

$$(\det\,(L))^2 = \frac{(\text{area}\,(\pi\,(L\,(x)\,,L\,(y))))^2}{(\text{area}\,(\pi\,(x,y)))^2}.$$

To see that this doesn't depend on x and y we chose x' and y' as above and note that

$$\begin{bmatrix} L\,(x') & L\,(y') \end{bmatrix} = \begin{bmatrix} L\,(x) & L\,(y) \end{bmatrix} \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}$$

and

$$\begin{aligned}
\frac{(\text{area}\,(\pi\,(L\,(x')\,,L\,(y'))))^2}{(\text{area}\,(\pi\,(x',y')))^2} &= \frac{(\alpha\delta-\beta\gamma)^2\,(\text{area}\,(\pi\,(L\,(x)\,,L\,(y))))^2}{(\alpha\delta-\beta\gamma)^2\,(\text{area}\,(\pi\,(x,y)))^2} \\
&= \frac{(\text{area}\,(\pi\,(L\,(x)\,,L\,(y))))^2}{(\text{area}\,(\pi\,(x,y)))^2}.
\end{aligned}$$

Thus $(\det(L))^2$ depends neither on the inner product that is used to compute the area nor on the vectors x and y. Finally we can refine the definition so that

$$\begin{aligned} \det(L) &= \begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc, \text{ where} \\ \begin{bmatrix} L(x) & L(y) \end{bmatrix} &= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix}. \end{aligned}$$

This introduces a sign in the definition which one can also easily check doesn't depend on the choice of x and y.

This approach generalizes to higher dimensions, but it also runs into a little trouble. The keen observer might have noticed that the formula for the area is in fact a determinant

$$\begin{aligned} (\text{area}(\pi(x,y)))^2 &= (x|x)(y|y) - (x|y)^2 \\ &= \begin{vmatrix} (x|x) & (x|y) \\ (x|y) & (y|y) \end{vmatrix}. \end{aligned}$$

When passing to higher dimensions it will become increasingly harder to justify how the volume of a parallelepiped depends on the base vectors without using a determinant. Thus we encounter a bit of a vicious circle when trying to define determinants in this fashion.

The other problem is that we used only real scalars. One can modify the approach to also work for complex numbers, but beyond that there isn't much hope. The approach we take below is mirrored on the constructions here, but they work for general scalar fields.

2. Algebraic Approach

As was done in the previous section we are going to separate the idea of volumes and determinants, the latter being exclusively for linear operators and a quantity which is independent of others structures on the vector space. Since what we are going to call volume forms are used to define determinants we start by defining these. Unlike the more motivational approach we took in the previous section we are here going to take a more axiomatic approach.

Let V be an n-dimensional vector space over $\mathbb{F}$. A *volume form*

$$\text{vol} : \overbrace{V \times \cdots \times V}^{\text{n times}} \to \mathbb{F}$$

is simply a multi-linear map, i.e., it is linear in each variable if the others are fixed, that is also alternating. More precisely if $x_1, ..., x_{i-1}, x_{i+1}, ...x_n \in V$ then

$$x \to \text{vol}(x_1, ..., x_{i-1}, x, x_{i+1}, ..., x_n)$$

is linear, and for $i < j$ we have the *alternating property* when x_i and x_j are transposed:

$$\text{vol}(..., x_i, ..., x_j, ...) = -\text{vol}(..., x_j, ..., x_i, ...).$$

In "Existence of the Volume Form" below we shall show that such volume forms always exist. In this section we are going to establish some important properties and also give some methods for computing volumes.

PROPOSITION 30. *Let* vol : $V \times \cdots \times V \to \mathbb{F}$ *be a volume form on an n-dimensional vector space over* $\mathbb{F}$. *Then*

(1) $\operatorname{vol}(\ldots,x,\ldots,x,\ldots)=0.$
(2) $\operatorname{vol}(x_1,\ldots,x_{i-1},x_i+y,x_{i+1},\ldots,x_n)=\operatorname{vol}(x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n)$ *if* $y=\sum_{k\neq i}\alpha_k x_k$ *is a linear combination of* $x_1,\ldots,x_{i-1},x_{i+1},\ldots x_n$.
(3) $\operatorname{vol}(x_1,\ldots,x_n)=0$ *if* $x_1,\ldots,x_n$ *are linearly dependent.*
(4) *If* $\operatorname{vol}(x_1,\ldots,x_n)\neq 0$, *then* $x_1,\ldots,x_n$ *form a basis for* V.

Proof. 1. The alternating property tells us that

$$\operatorname{vol}(\ldots,x,\ldots,x,\ldots)=-\operatorname{vol}(\ldots,x,\ldots,x,\ldots)$$

if we switch x and x. Thus $\operatorname{vol}(\ldots,x,\ldots,x,\ldots)=0$.

2. Let $y=\sum_{k\neq i}\alpha_k x_k$ and use linearity to conclude

$$\begin{aligned}\operatorname{vol}(x_1,\ldots,x_{i-1},x_i+y,x_{i+1},\ldots,x_n) &= \operatorname{vol}(x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n)\\ &\quad+\sum_{k\neq i}\alpha_k\operatorname{vol}(x_1,\ldots,x_{i-1},x_k,x_{i+1},\ldots,x_n).\end{aligned}$$

Since x_k is always equal to one of $x_1,\ldots,x_{i-1},x_{i+1},\ldots x_n$ we see that

$$\alpha_k\operatorname{vol}(x_1,\ldots,x_{i-1},x_k,x_{i+1},\ldots,x_n)=0.$$

This implies the claim.

3. If $x_1=0$ we are finished. Otherwise we have that some $x_k=\sum_{i=1}^{k-1}\alpha_i x_i$, then 2. implies that

$$\begin{aligned}\operatorname{vol}(x_1,\ldots,0+x_k,\ldots,x_n) &= \operatorname{vol}(x_1,\ldots,0,\ldots,x_n)\\ &= 0.\end{aligned}$$

4. From 3. we have that $x_1,\ldots,x_n$ are linearly independent. Since V has dimension n they must also form a basis. □

Note that in the above proof we had to use that $1\neq -1$ in the scalar field. This is certainly true for the fields we work with. When working with more general fields like $\mathbb{F}=\{0,1\}$ we need to modify the alternating property. Instead we can assume that the volume form $\operatorname{vol}(x_1,\ldots,x_n)$ satisfies: $\operatorname{vol}(x_1,\ldots,x_n)=0$ whenever $x_i=x_j$. This in turn implies the alternating property. To prove this note that if $x=x_i+x_j$, then

$$\begin{aligned}0 &= \operatorname{vol}\Big(\ldots,\overset{\text{i}^{\text{th}}\text{ place}}{x},\ldots,\overset{\text{j}^{\text{th}}\text{ place}}{x},\ldots\Big)\\ &= \operatorname{vol}\Big(\ldots,\overset{\text{i}^{\text{th}}\text{ place}}{x_i+x_j},\ldots,\overset{\text{j}^{\text{th}}\text{ place}}{x_i+x_j},\ldots\Big)\\ &= \operatorname{vol}\Big(\ldots,\overset{\text{i}^{\text{th}}\text{ place}}{x_i},\ldots,\overset{\text{j}^{\text{th}}\text{ place}}{x_i},\ldots\Big)+\operatorname{vol}\Big(\ldots,\overset{\text{i}^{\text{th}}\text{ place}}{x_j},\ldots,\overset{\text{j}^{\text{th}}\text{ place}}{x_i},\ldots\Big)\\ &\quad+\operatorname{vol}\Big(\ldots,\overset{\text{i}^{\text{th}}\text{ place}}{x_i},\ldots,\overset{\text{j}^{\text{th}}\text{ place}}{x_j},\ldots\Big)+\operatorname{vol}\Big(\ldots,\overset{\text{i}^{\text{th}}\text{ place}}{x_j},\ldots,\overset{\text{j}^{\text{th}}\text{ place}}{x_j},\ldots\Big)\\ &= \operatorname{vol}\Big(\ldots,\overset{\text{i}^{\text{th}}\text{ place}}{x_j},\ldots,\overset{\text{j}^{\text{th}}\text{ place}}{x_i},\ldots\Big)+\operatorname{vol}\Big(\ldots,\overset{\text{i}^{\text{th}}\text{ place}}{x_i},\ldots,\overset{\text{j}^{\text{th}}\text{ place}}{x_j},\ldots\Big),\end{aligned}$$

which shows that the form is alternating.

Theorem 43. (Uniqueness of Volume Forms) *Let* $\operatorname{vol}_1,\operatorname{vol}_2:V\times\cdots\times V\to\mathbb{F}$ *be two volume forms on an* n*-dimensional vector space over* $\mathbb{F}$. *If* vol_2 *is nontrivial then* $\operatorname{vol}_1=\lambda\operatorname{vol}_2$ *for some* $\lambda\in\mathbb{F}$.

PROOF. If we assume that vol_2 is nontrivial, then we can find $x_1, ..., x_n \in V$ so that $\mathrm{vol}_2(x_1, ..., x_n) \neq 0$. Then define λ so that

$$\mathrm{vol}_1(x_1, ..., x_n) = \lambda \, \mathrm{vol}_2(x_1, ..., x_n).$$

If $z_1, ..., z_n \in V$, then we can write

$$\begin{aligned}
\begin{bmatrix} z_1 & \cdots & z_n \end{bmatrix} &= \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} A \\
&= \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{bmatrix}
\end{aligned}$$

For any volume form vol we then have

$$\begin{aligned}
\mathrm{vol}(z_1, ..., z_n) &= \mathrm{vol}\left(\sum_{i_1=1}^{n} x_{i_1}\alpha_{i_1 1}, ..., \sum_{i_n=1}^{n} x_{i_n}\alpha_{i_n n}\right) \\
&= \sum_{i_1=1}^{n} \alpha_{i_1 1} \, \mathrm{vol}\left(x_{i_1}, ..., \sum_{i_n=1}^{n} \alpha_{i_n n} x_{i_n}\right) \\
&\ \ \vdots \\
&= \sum_{i_1, ..., i_n=1}^{n} \alpha_{i_1 1} \cdots \alpha_{i_n n} \, \mathrm{vol}(x_{i_1}, ..., x_{i_n}).
\end{aligned}$$

The first thing we should note is that $\mathrm{vol}(x_{i_1}, ..., x_{i_n}) = 0$ if any two of the indices $i_1, ..., i_n$ are equal. When doing the sum

$$\sum_{i_1, ..., i_n=1}^{n} \alpha_{i_1 1} \cdots \alpha_{i_n n} \, \mathrm{vol}(x_{i_1}, ..., x_{i_n})$$

we can therefore assume that all of the indices $i_1, ..., i_n$ are different. This means that by switching indices around we have

$$\mathrm{vol}(x_{i_1}, ..., x_{i_n}) = \pm \, \mathrm{vol}(x_1, ..., x_n)$$

where the sign $\pm$ depends on the number of switches we have to make in order to rearrange $i_1, ..., i_n$ to get back to the standard ordering $1, ..., n$. Since this number of switches does not depend on vol but only on the indices we obtain the desired result:

$$\begin{aligned}
\mathrm{vol}_1(z_1, ..., z_n) &= \sum_{i_1, ..., i_n=1}^{n} \pm \alpha_{i_1 1} \cdots \alpha_{i_n n} \, \mathrm{vol}_1(x_1, ..., x_n) \\
&= \sum_{i_1, ..., i_n=1}^{n} \pm \alpha_{i_1 1} \cdots \alpha_{i_n n} \lambda \, \mathrm{vol}_2(x_1, ..., x_n) \\
&= \lambda \sum_{i_1, ..., i_n=1}^{n} \pm \alpha_{i_1 1} \cdots \alpha_{i_n n} \, \mathrm{vol}_2(x_1, ..., x_n) \\
&= \lambda \, \mathrm{vol}_2(z_1, ..., z_n).
\end{aligned}$$

□

From the proof of this theorem we also obtain one of the crucial results about volumes that we mentioned in the previous section.

COROLLARY 40. *If $x_1, ..., x_n \in V$ is a basis for V then any volume form* vol *is completely determined by its value* $\text{vol}(x_1, ..., x_n)$.

This corollary could be used to create volume forms by simply defining

$$\text{vol}(z_1, ..., z_n) = \sum_{i_1,...,i_n} \pm\alpha_{i_1 1} \cdots \alpha_{i_n n} \text{vol}(x_1, ..., x_n),$$

where $\{i_1, ..., i_n\} = \{1, ..., n\}$. For that to work we would have to show that the sign $\pm$ is well-defined in the sense that it doesn't depend on the particular way in which we reorder $i_1, ..., i_n$ to get $1, ..., n$. While this is certainly true we shall not prove this combinatorial fact here. Instead we observe that if we have a volume form that is nonzero on $x_1, ..., x_n$ then the fact that $\text{vol}(x_{i_1}, ..., x_{i_n})$ is a multiple of $\text{vol}(x_1, ..., x_n)$ tells us that this sign is well-defined and so doesn't depend on the way in which $1, ..., n$ was rearranged to get $i_1, ..., i_n$. We use the notation $\text{sign}(i_1, ..., i_n)$ for the sign we get from

$$\text{vol}(x_{i_1}, ..., x_{i_n}) = \text{sign}(i_1, ..., i_n) \text{vol}(x_1, ..., x_n).$$

Our last property for volume forms is to see what happens when we restrict it to subspaces. To this end, let vol be a nontrivial volume form on V and $M \subset V$ a k-dimensional subspace of V. If we fix vectors $y_1, ..., y_{n-k} \in V$, then we can define a form on M by

$$\text{vol}_M(x_1, ..., x_k) = \text{vol}(x_1, ..., x_k, y_1, ..., y_{n-k})$$

where $x_1, ..., x_k \in M$. It is clear that vol_M is linear in each variable and also alternating as vol has those properties. Moreover, if $y_1, ..., y_{n-k}$ form a basis for a complement to M in V, then $x_1, ..., x_k, y_1, ..., y_{n-k}$ will be a basis for V as long as $x_1, ..., x_k$ is a basis for M. In this case vol_M becomes a nontrivial volume form as well. If, however, some linear combination of $y_1, ..., y_{n-k}$ lies in M then it follows that $\text{vol}_M = 0$.

2.1. Exercises.

(1) Let V be a 3-dimensional real inner product space and vol a volume form so that $\text{vol}(e_1, e_2, e_3) = 1$ for some orthonormal basis. For $x, y \in V$ define $x \times y$ as the unique vector such that

$$\text{vol}(x, y, z) = \text{vol}(z, x, y) = (z|x \times y).$$

(a) Show that $x \times y = -y \times x$ and that $x \to x \times y$ is linear.

(b) Show that

$$(x_1 \times y_1|x_2 \times y_2) = (x_1|x_2)(y_1|y_2) - (x_1|y_2)(x_2|y_1).$$

(c) Show that

$$\|x \times y\| = \|x\| \|y\| |\sin\theta|,$$

where

$$\cos\theta = \frac{(x, y)}{\|x\| \|y\|}.$$

(d) Show that

$$x \times (y \times z) = (x|z) y - (x|y) z.$$

(e) Show that the Jacobi identity holds

$$x \times (y \times z) + z \times (x \times y) + y \times (z \times x) = 0.$$

(2) Let $x_1, ..., x_n \in \mathbb{R}^n$ and do a Gram-Schmidt procedure so as to obtain a QR decomposition

$$\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} = \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} \begin{bmatrix} r_{11} & \cdots & r_{1n} \\ & \ddots & \vdots \\ 0 & & r_{nn} \end{bmatrix},$$

Show that

$$\mathrm{vol}\,(x_1, ..., x_n) = r_{11} \cdots r_{nn}\,\mathrm{vol}\,(e_1, ..., e_n)$$

and explain why $r_{11} \cdots r_{nn}$ gives the geometrically defined volume that comes from the formula where one multiplies height and base "area" and in turn uses that same principle to compute the base "area" etc. In other words

$$\begin{aligned} r_{11} &= \|x_1\|, \\ r_{22} &= \left\|x_2 - \mathrm{proj}_{x_1}(x_2)\right\|, \\ &\vdots \\ r_{nn} &= \left\|x_n - \mathrm{proj}_{M_{n-1}}(x_n)\right\|. \end{aligned}$$

(3) Show that

$$\mathrm{vol}\left(\begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \begin{bmatrix} \gamma \\ \delta \end{bmatrix}\right) = \alpha\delta - \gamma\beta$$

defines a volume form on $\mathbb{F}^2$ such that $\mathrm{vol}\,(e_1, e_2) = 1$.

(4) Show that we can define a volume form on $\mathbb{F}^3$ by

$$\begin{aligned} \mathrm{vol}\left(\begin{bmatrix} a_{11} \\ a_{21} \\ a_{31} \end{bmatrix}, \begin{bmatrix} a_{12} \\ a_{22} \\ a_{32} \end{bmatrix}, \begin{bmatrix} a_{13} \\ a_{23} \\ a_{33} \end{bmatrix}\right) &= a_{11}\,\mathrm{vol}\left(\begin{bmatrix} a_{22} \\ a_{32} \end{bmatrix}, \begin{bmatrix} a_{23} \\ a_{33} \end{bmatrix}\right) \\ &\quad -a_{12}\,\mathrm{vol}\left(\begin{bmatrix} a_{21} \\ a_{31} \end{bmatrix}, \begin{bmatrix} a_{23} \\ a_{33} \end{bmatrix}\right) \\ &\quad +a_{13}\,\mathrm{vol}\left(\begin{bmatrix} a_{21} \\ a_{31} \end{bmatrix}, \begin{bmatrix} a_{22} \\ a_{32} \end{bmatrix}\right) \\ &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{32}a_{21} \\ &\quad -a_{11}a_{23}a_{32} - a_{33}a_{12}a_{21} - a_{22}a_{13}a_{31}. \end{aligned}$$

(5) Assume that $\mathrm{vol}\,(e_1, ..., e_4) = 1$ for the standard basis in $\mathbb{R}^4$. Using the permutation formula for the volume form determine with a minimum of calculations the sign for the volume of the columns in each of the matrices.

(a) $$\begin{bmatrix} 1000 & -1 & 2 & -1 \\ 1 & 1000 & 1 & 2 \\ 3 & -2 & 1 & 1000 \\ 2 & -1 & 1000 & 2 \end{bmatrix}$$

(b) $$\begin{bmatrix} 2 & 1000 & 2 & -1 \\ 1 & -1 & 1000 & 2 \\ 3 & -2 & 1 & 1000 \\ 1000 & -1 & 1 & 2 \end{bmatrix}$$

(c) $\begin{bmatrix} 2 & -2 & 2 & 1000 \\ 1 & -1 & 1000 & 2 \\ 3 & 1000 & 1 & -1 \\ 1000 & -1 & 1 & 2 \end{bmatrix}$

(d) $\begin{bmatrix} 2 & -2 & 1000 & -1 \\ 1 & 1000 & 2 & 2 \\ 3 & -1 & 1 & 1000 \\ 1000 & -1 & 1 & 2 \end{bmatrix}$

3. How to Calculate Volumes

Before establishing the existence of the volume form we shall try to use what we learned in the previous section in a more concrete fashion to calculate $\mathrm{vol}(z_1,...,z_n)$. Assume that $\mathrm{vol}(z_1,...,z_n)$ is a volume form on V and that there is a basis $x_1,...,x_n$ for V where $\mathrm{vol}(x_1,...,x_n)$ is known. First observe that when

$$\begin{bmatrix} z_1 & \cdots & z_n \end{bmatrix} = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} A$$

and $A = [\alpha_{ij}]$ is an upper triangular matrix then $\alpha_{i_1 1}\cdots\alpha_{i_n n} = 0$ unless $i_1 \leq 1,...,i_n \leq n$. Since we also need all the indices $i_1,...,i_n$ to be distinct, this implies that $i_1 = 1,....,i_n = n$. Thus we have the simple relationship

$$\mathrm{vol}(z_1,...,z_n) = \alpha_{11}\cdots\alpha_{nn}\,\mathrm{vol}(x_1,...,x_n).$$

While we can't expect this to happen too often it is possible to change $z_1,...,z_n$ to vectors $y_1,...,y_n$ in such a way that

$$\mathrm{vol}(z_1,...,z_n) = \pm\,\mathrm{vol}(y_1,...,y_n)$$

and

$$\begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} A$$

where A is upper triangular.

To construct the y_is we simply use *elementary column operations*. This works in almost the same way as Gauss elimination but with the twist that we are multiplying by matrices on the right (see also "Row Reduction" in chapter 1). The allowable operations are

(1) Interchanging vectors z_k and z_l.
(2) Multiplying z_l by $\alpha \in \mathbb{F}$ and adding it to z_k.

The second operation does change volume, hwile the first changes it by a sign. So if $\begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix}$ is obtained from $\begin{bmatrix} z_1 & \cdots & z_n \end{bmatrix}$ through these operations we have

$$\mathrm{vol}(z_1,...,z_n) = \pm\,\mathrm{vol}(y_1,...,y_n).$$

The minus sign occurs exactly when we have done an odd number of interchanges. We now need to explain why we can obtain $\begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix}$ such that

$$\begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & & \alpha_{2n} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{nn} \end{bmatrix}.$$

The only thing to note is that the process might break down if $z_1,....,z_n$ are linearly dependent. In that case we have $\mathrm{vol} = 0$.

Instead of describing the procedure abstractly let us see how it works in practice. In the case of $\mathbb{F}^n$ we assume that we are using a volume form such that $\operatorname{vol}(e_1,...,e_n) = 1$ for the canonical basis. Since that uniquely defines the volume form we introduce some special notation for it

$$|A| = \begin{vmatrix} x_1 & \cdots & x_n \end{vmatrix} = \operatorname{vol}(x_1,...,x_n)$$

where $A \in \operatorname{Mat}_{n\times n}(\mathbb{F})$ is the matrix such that

$$\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} = \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} A$$

EXAMPLE 97. *Let*

$$\begin{bmatrix} z_1 & z_2 & z_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 3 \\ -2 & 0 & 0 \end{bmatrix}.$$

We can rearrange this into

$$\begin{bmatrix} z_2 & z_3 & z_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -2 \end{bmatrix}$$

This takes two transpositions. Thus

$$\begin{aligned} \operatorname{vol}(z_1,z_2,z_3) &= \operatorname{vol}(z_2,z_3,z_1) \\ &= 1\cdot 3\cdot(-2)\operatorname{vol}(e_1,e_2,e_3) \\ &= -6\operatorname{vol}(e_1,e_2,e_3). \end{aligned}$$

EXAMPLE 98. *Let*

$$\begin{bmatrix} z_1 & z_2 & z_3 & z_4 \end{bmatrix} = \begin{bmatrix} 3 & 0 & 1 & 3 \\ 1 & -1 & 2 & 0 \\ -1 & 1 & 0 & -2 \\ -3 & 1 & 1 & -3 \end{bmatrix}.$$

$$\begin{aligned} & \begin{vmatrix} 3 & 0 & 1 & 3 \\ 1 & -1 & 2 & 0 \\ -1 & 1 & 0 & -2 \\ -3 & 1 & 1 & -3 \end{vmatrix} \\ = & \begin{vmatrix} 0 & 1 & 2 & 3 \\ 1 & -1 & 2 & 0 \\ 1 & \frac{1}{3} & -\frac{2}{3} & -2 \\ 0 & 0 & 0 & -3 \end{vmatrix} \text{ after eliminating entries in row 4,} \\ = & \begin{vmatrix} 3 & 2 & 2 & 3 \\ 4 & 0 & 2 & 0 \\ 0 & 0 & -\frac{2}{3} & -2 \\ 0 & 0 & 0 & -3 \end{vmatrix} \text{ after eliminating entries in row 3,} \\ = & \begin{vmatrix} 2 & 3 & 2 & 3 \\ 0 & 4 & 2 & 0 \\ 0 & 0 & -\frac{2}{3} & -2 \\ 0 & 0 & 0 & -3 \end{vmatrix} \text{ after switching column one and two.} \end{aligned}$$

Thus we get

$$\begin{aligned} \operatorname{vol}(z_1, ..., z_4) &= -2 \cdot 4 \cdot \left(-\frac{2}{3}\right) \cdot (-3) \operatorname{vol}(e_1, ..., e_4) \\ &= -16 \operatorname{vol}(e_1, ..., e_4). \end{aligned}$$

EXAMPLE 99. *Let us try to find*

$$\left| \begin{matrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2 & \cdots & 2 \\ 1 & 2 & 3 & \cdots & 3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & 3 & \cdots & n \end{matrix} \right|$$

Instead of starting with the last column vector we are going to start with the first. This will lead us to a lower triangular matrix, but otherwise we are using the same principles.

$$\begin{aligned} \left| \begin{matrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2 & \cdots & 2 \\ 1 & 2 & 3 & \cdots & 3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & 3 & \cdots & n \end{matrix} \right| &= \left| \begin{matrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 2 & \cdots & 2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 2 & \cdots & n-1 \end{matrix} \right| \\ &= \left| \begin{matrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & n-2 \end{matrix} \right| \\ &\vdots \\ &= \left| \begin{matrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 1 \end{matrix} \right| \\ &= 1 \end{aligned}$$

3.1. Exercises.

(1) The following problem was first considered by Leibniz and appears to be the first use of determinants. Let $A \in \operatorname{Mat}_{(n+1)\times n}(\mathbb{F})$ and $b \in \mathbb{F}^{n+1}$.
  (a) If there is a solution to the over determined system $Ax = b$, $x \in \mathbb{F}^n$, then the augmented matrix satisfies $|A|\, b| = 0$.
  (b) Conversely, if A has $\operatorname{rank}(A) = n$ and $|A|\, b| = 0$, then there is a solution to $Ax = b$, $x \in \mathbb{F}^n$.

(2) Find

$$\left|\begin{array}{ccccc} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cdots & 1 & 0 & 1 \end{array}\right|$$

(3) Let $x_1, ..., x_k \in \mathbb{R}^n$ and assume that $\operatorname{vol}(e_1, ..., e_n) = 1$. Show that

$$|G(x_1, ..., x_k)| \leq \|x_1\|^2 \cdots \|x_k\|^2,$$

where $G(x_1, ..., x_k)$ is the Gram matrix whose ij entries are the inner products $(x_j|x_i)$.

(4) Think of $\mathbb{R}^n$ as an inner product space where $\operatorname{vol}(e_1, ..., e_n) = 1$.

(a) If $x_1, ..., x_n \in \mathbb{R}^n$, show that

$$G(x_1, ..., x_n) = \left[\begin{array}{ccc} x_1 & \cdots & x_n \end{array}\right]^* \left[\begin{array}{ccc} x_1 & \cdots & x_n \end{array}\right].$$

(b) Show that

$$|G(x_1, ..., x_n)| = |\operatorname{vol}(x_1, ..., x_n)|^2.$$

(c) Using the previous exercise conclude that Hadamard's inequality holds

$$|\operatorname{vol}(x_1, ..., x_n)|^2 \leq \|x_1\|^2 \cdots \|x_n\|^2.$$

(d) When is

$$|\operatorname{vol}(x_1, ..., x_n)|^2 = \|x_1\|^2 \cdots \|x_n\|^2?$$

(5) Assume that $\operatorname{vol}(e_1, ..., e_4) = 1$ for the standard basis in $\mathbb{R}^4$. Find the volumes

(a) $\left|\begin{array}{cccc} 0 & -1 & 2 & -1 \\ 1 & 0 & 1 & 2 \\ 3 & -2 & 1 & 0 \\ 2 & -1 & 0 & 2 \end{array}\right|$

(b) $\left|\begin{array}{cccc} 2 & 0 & 2 & -1 \\ 1 & -1 & 0 & 2 \\ 3 & -2 & 1 & 1 \\ 0 & -1 & 1 & 2 \end{array}\right|$

(c) $\left|\begin{array}{cccc} 2 & -2 & 2 & 0 \\ 1 & -1 & 1 & 2 \\ 3 & 0 & 1 & -1 \\ 1 & -1 & 1 & 2 \end{array}\right|$

(d) $\left|\begin{array}{cccc} 2 & -2 & 0 & -1 \\ 1 & 1 & 2 & 2 \\ 3 & -1 & 1 & 1 \\ 1 & -1 & 1 & 2 \end{array}\right|$

4. Existence of the Volume Form

The construction of $\mathrm{vol}(x_1,...,x_n)$ proceeds by induction on the dimension of V. Thus fix a basis $e_1,...,e_n \in V$ that we assume is going to have unit volume. Next we assume, by induction, that there is a volume form vol^{n-1} on $\mathrm{span}\{e_2,...,e_n\}$ such that $e_2,...,e_n$ has unit volume. Finally let $E : V \to V$ be the projection onto $\mathrm{span}\{e_2,...,e_n\}$ whose kernel is $\mathrm{span}\{e_1\}$. For a collection $x_1,...,x_n \in V$ we decompose $x_i = \alpha_i e_1 + E(x_i)$. The volume form vol^n on V is now defined by

$$\mathrm{vol}^n(x_1,...,x_n) = \sum_{k=1}^{n} (-1)^{k-1} \alpha_k \mathrm{vol}^{n-1}\left(E(x_1),...,\widehat{E(x_k)},...,E(x_n)\right).$$

This is essentially like defining the volume via a Laplace expansion along the first row. As α_k, E, and vol^{n-1} are linear it is obvious that the new vol^n form is linear in each variable. The alternating property follows if we can show that the form vanishes when $x_i = x_j$. This is done as follows

$$\begin{aligned} & \mathrm{vol}^n(...,x_i,...x_j,...) \\ = & \sum_{k\neq i,j} (-1)^{k-1} \alpha_k \mathrm{vol}^{n-1}\left(...,E(x_i),...,\widehat{E(x_k)},...,E(x_j),...\right) \\ & + (-1)^{i-1} \alpha_i \mathrm{vol}^{n-1}\left(...,\widehat{E(x_i)},...,E(x_j),...\right) \\ & + (-1)^{j-1} \alpha_j \mathrm{vol}^{n-1}\left(...,E(x_i),...,\widehat{E(x_j)},...\right) \end{aligned}$$

Using that $E(x_i) = E(x_j)$ and vol^{n-1} is alternating on $\mathrm{span}\{e_2,...,e_n\}$ shows

$$\mathrm{vol}^{n-1}\left(...,E(x_i),...,\widehat{E(x_k)},...,E(x_j),...\right) = 0$$

Hence

$$\begin{aligned} & \mathrm{vol}^n(...,x_i,...x_j,...) \\ = & (-1)^{i-1} \alpha_i \mathrm{vol}^{n-1}\left(...,\widehat{E(x_i)},...,E(x_j),...\right) \\ & + (-1)^{j-1} \alpha_j \mathrm{vol}^{n-1}\left(...,E(x_i),...,\widehat{E(x_j)},...\right) \\ = & (-1)^{i-1}(-1)^{j-1-i} \alpha_i \mathrm{vol}^{n-1}\left(...,E(x_{i-1}),\overset{i^{\mathrm{th}}\text{ place}}{E(x_j)},E(x_{i+1})...\right) \\ & + (-1)^{j-1} \alpha_j \mathrm{vol}^{n-1}\left(...,E(x_i),...,\widehat{E(x_j)},...\right), \end{aligned}$$

where moving $E(x_j)$ to the i^{th}-place in the expression

$$\mathrm{vol}^{n-1}\left(...,\widehat{E(x_i)},...,E(x_j),...\right)$$

requires $j-1-i$ moves since $E(x_j)$ is in the $(j-1)$-place. Using that $\alpha_i = \alpha_j$ and $E(x_i) = E(x_j)$, this shows

$$\begin{aligned} \mathrm{vol}^n(...,x_i,...x_j,...) &= (-1)^{j-2} \alpha_i \mathrm{vol}^{n-1}\left(...,\overset{i^{th}\text{ place}}{E(x_j)},...,,...\right) \\ & \quad + (-1)^{j-1} \alpha_j \mathrm{vol}^{n-1}\left(...,E(x_i),...,\widehat{E(x_j)},...\right) \\ &= 0. \end{aligned}$$

Aside from defining the volume form we also get a method for calculating volumes using induction on dimension. In $\mathbb{F}$ we just define $\operatorname{vol}(x) = x$. For $\mathbb{F}^2$ we have

$$\operatorname{vol}\left(\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right) = ad - cb.$$

In $\mathbb{F}^3$ we get

$$\begin{aligned}
\operatorname{vol}\left(\begin{bmatrix} a_{11} \\ a_{21} \\ a_{31} \end{bmatrix}, \begin{bmatrix} a_{12} \\ a_{22} \\ a_{32} \end{bmatrix}, \begin{bmatrix} a_{13} \\ a_{23} \\ a_{33} \end{bmatrix}\right) &= a_{11} \operatorname{vol}\left(\begin{bmatrix} a_{22} \\ a_{32} \end{bmatrix}, \begin{bmatrix} a_{23} \\ a_{33} \end{bmatrix}\right) \\
&\quad -a_{12} \operatorname{vol}\left(\begin{bmatrix} a_{21} \\ a_{31} \end{bmatrix}, \begin{bmatrix} a_{23} \\ a_{33} \end{bmatrix}\right) \\
&\quad +a_{13} \operatorname{vol}\left(\begin{bmatrix} a_{21} \\ a_{31} \end{bmatrix}, \begin{bmatrix} a_{22} \\ a_{32} \end{bmatrix}\right) \\
&= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\
&\quad -a_{11}a_{32}a_{23} - a_{12}a_{21}a_{33} - a_{13}a_{31}a_{22} \\
&= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{32}a_{21} \\
&\quad -a_{11}a_{23}a_{32} - a_{33}a_{12}a_{21} - a_{22}a_{13}a_{31}.
\end{aligned}$$

In the above definition there is, of course, nothing special about the choice of basis $e_1, ..., e_n$ or the ordering of the basis. Let us refer to the specific choice of volume form as vol_1 as we are expanding along the first row. If we switch e_1 and e_k then we are apparently expanding along the k^{th} row instead. This defines a volume form vol_k. By construction we have

$$\begin{aligned}
\operatorname{vol}_1(e_1, ..., e_n) &= 1, \\
\operatorname{vol}_k\left(e_k, e_2, ..., \overset{k^{\text{th}}\text{ place}}{e_1}, ..., e_n\right) &= 1.
\end{aligned}$$

Thus

$$\begin{aligned}
\operatorname{vol}_1 &= (-1)^{k-1} \operatorname{vol}_k \\
&= (-1)^{k+1} \operatorname{vol}_k.
\end{aligned}$$

So if we wish to calculate vol_1 by an expansion along the k^{th} row we need to remember the extra sign $(-1)^{k+1}$. In the case of $\mathbb{F}^n$ we define the volume form vol to be vol_1 as constructed above. In this case we shall often just write

$$\left| \begin{array}{ccc} x_1 & \cdots & x_n \end{array} \right| = \operatorname{vol}(x_1, ..., x_n)$$

as in the previous section.

Example 100. *Let us try this with the example from the previous section*

$$\begin{bmatrix} z_1 & z_2 & z_3 & z_4 \end{bmatrix} = \begin{bmatrix} 3 & 0 & 1 & 3 \\ 1 & -1 & 2 & 0 \\ -1 & 1 & 0 & -2 \\ -3 & 1 & 1 & -3 \end{bmatrix}.$$

Expansion along the first row gives

$$\begin{aligned}
\begin{vmatrix} z_1 & z_2 & z_3 & z_4 \end{vmatrix} &= 3\begin{vmatrix} -1 & 2 & 0 \\ 1 & 0 & -2 \\ 1 & 1 & -3 \end{vmatrix} - 0\begin{vmatrix} 1 & 2 & 0 \\ -1 & 0 & -2 \\ -3 & 1 & -3 \end{vmatrix} \\
&\quad +1\begin{vmatrix} 1 & -1 & 0 \\ -1 & 1 & -2 \\ -3 & 1 & -3 \end{vmatrix} - 3\begin{vmatrix} 1 & -1 & 2 \\ -1 & 1 & 0 \\ -3 & 1 & 1 \end{vmatrix} \\
&= 3\cdot 0 - 0 + 1\cdot(-4) - 3\cdot 4 \\
&= -16
\end{aligned}$$

Expansion along the second row gives

$$\begin{aligned}
\begin{vmatrix} z_1 & z_2 & z_3 & z_4 \end{vmatrix} &= -1\begin{vmatrix} 0 & 1 & 3 \\ 1 & 0 & -2 \\ 1 & 1 & -3 \end{vmatrix} + (-1)\begin{vmatrix} 3 & 1 & 3 \\ -1 & 0 & -2 \\ -3 & 1 & -3 \end{vmatrix} \\
&\quad -2\begin{vmatrix} 3 & 0 & 3 \\ -1 & 1 & -2 \\ -3 & 1 & -3 \end{vmatrix} + 0\begin{vmatrix} 3 & 0 & 1 \\ -1 & 1 & 0 \\ -3 & 1 & 1 \end{vmatrix} \\
&= -1\cdot 4 - 1\cdot 6 - 2\cdot 3 + 0 \\
&= -16
\end{aligned}$$

The general formula in $\mathbb{F}^n$ for expanding along the k^{th} row in an $n \times n$ matrix $A = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}$ is called the *Laplace expansion* along the k^{th} row and looks like

$$\begin{aligned}
|A| &= (-1)^{k+1}\alpha_{k1}|A_{k1}| + (-1)^{k+2}\alpha_{k2}|A_{k2}| + \cdots + (-1)^{k+n}\alpha_{kn}|A_{kn}| \\
&= \sum_{i=1}^{n}(-1)^{k+i}\alpha_{ki}|A_{ki}|.
\end{aligned}$$

Here α_{ij} is the ij entry in A, i.e., the i^{th} coordinate for x_j, and A_{ij} is the *companion* $(n-1)\times(n-1)$ matrix for α_{ij}. The matrix A_{ij} is constructed from A by eliminating the i^{th} row and j^{th} column. Note that the exponent for -1 is $i+j$ when we are at the ij entry α_{ij}.

This expansion gives us a very intriguing formula for the determinant that looks like we have used the chain rule for differentiation in several variables. To explain this let us think of $|A|$ as a function in the entries x_{ij}. The expansion along the k^{th} row then looks like

$$|A| = (-1)^{k+1}x_{k1}|A_{k1}| + (-1)^{k+2}x_{k2}|A_{k2}| + \cdots + (-1)^{k+n}x_{kn}|A_{kn}|.$$

From the definition of $|A_{kj}|$ it follows that it does depend on the variables x_{ki}. Thus

$$\begin{aligned}
\frac{\partial |A|}{\partial x_{ki}} &= (-1)^{k+1}\frac{\partial x_{k1}}{\partial x_{ki}}|A_{k1}| + (-1)^{k+2}\frac{\partial x_{k2}}{\partial x_{ki}}|A_{k2}| + \cdots + (-1)^{k+n}\frac{\partial x_{kn}}{\partial x_{ki}}|A_{kn}| \\
&= (-1)^{k+i}|A_{ki}|.
\end{aligned}$$

Replacing $(-1)^{k+i}|A_{ki}|$ by the partial derivative then gives us the formula

$$\begin{aligned}|A| &= x_{k1}\frac{\partial|A|}{\partial x_{k1}}+x_{k2}\frac{\partial|A|}{\partial x_{k2}}+\cdots+x_{kn}\frac{\partial|A|}{\partial x_{kn}}\\ &= \sum_{i=1}^{n}x_{ki}\frac{\partial|A|}{\partial x_{ki}}.\end{aligned}$$

Since we get the same answer for each k this implies

$$n|A| = \sum_{i,j=1}^{n}x_{ij}\frac{\partial|A|}{\partial x_{ij}}.$$

4.1. Exercises.

(1) Find the determinant of the following $n\times n$ matrix where all entries are 1 except the entries just below the diagonal which are 0.

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1\\ 0 & 1 & 1 & \cdots & 1\\ 1 & 0 & 1 & \cdots & \vdots\\ \vdots & 1 & \ddots & \ddots & 1\\ 1 & \cdots & 1 & 0 & 1\end{vmatrix}$$

(2) Find the determinant of the following $n\times n$ matrix

$$\begin{vmatrix} 1 & \cdots & 1 & 1 & 1\\ 2 & \cdots & 2 & 2 & 1\\ 3 & \cdots & 3 & 1 & \vdots\\ \vdots & & 1 & \cdots & 1\\ n & 1 & \cdots & 1 & 1\end{vmatrix}$$

(3) (The Vandermonde Determinant)

(a) Show that

$$\begin{vmatrix} 1 & \cdots & 1\\ \lambda_1 & \cdots & \lambda_n\\ \vdots & & \vdots\\ \lambda_1^{n-1} & \cdots & \lambda_n^{n-1}\end{vmatrix} = \prod_{i<j}(\lambda_i-\lambda_j).$$

(b) When $\lambda_1,\ldots,\lambda_n$ are the complex roots of a polynomial $p(t)=t^n+a_{n-1}t^{n-1}+\cdots+a_1t+a_0$, we define the discriminant of p as

$$\Delta = D = \left(\prod_{i<j}(\lambda_i-\lambda_j)\right)^2.$$

When $n=2$ show that this conforms with the usual definition. In general one can compute Δ from the coefficients of p. Show that Δ is real if p is real.

(4) Consider the polynomial in n variables

$$p(x_1,\ldots,x_n)=\prod_{i<j}(x_i-x_j)$$

(a) If $\sigma \in S_n$ is a permutation, then

$$\operatorname{sign}(\sigma)\, p(x_1, ..., x_n) = p\left(x_{\sigma(1)}, ..., x_{\sigma(n)}\right).$$

(b) Using this show that the sign function $S_n \to \{\pm 1\}$ is a homomorphism, i.e., $\operatorname{sign}(\sigma\tau) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau)$.

(c) Using the above characterization show that $\operatorname{sign}(\sigma)$ can be determined by the number of inversions in the permutation. An inversion in σ is a pair of consecutive integers whose order is reversed, i.e., $\sigma(i) > \sigma(i+1)$.

(5) Let $A_n = [\alpha_{ij}]$ be a real skew-symmetric $n \times n$ matrix, i.e., $\alpha_{ij} = -\alpha_{ji}$.
  (a) Show that $|A_2| = \alpha_{12}^2$.
  (b) Show that $|A_4| = (\alpha_{12}\alpha_{34} + \alpha_{14}\alpha_{23} - \alpha_{13}\alpha_{24})^2$.
  (c) Show that $|A_{2n}| \geq 0$.
  (d) Show that $|A_{2n+1}| = 0$.

(6) Show that the $n \times n$ matrix satisfies

$$\begin{vmatrix} \alpha & \beta & \beta & \cdots & \beta \\ \beta & \alpha & \beta & \cdots & \beta \\ \beta & \beta & \alpha & \cdots & \beta \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta & \beta & \beta & \cdots & \alpha \end{vmatrix} = (\alpha + (n-1)\beta)(\alpha - \beta)^{n-1}.$$

(7) Show that the $n \times n$ matrix

$$A_n = \begin{bmatrix} \alpha_1 & 1 & 0 & \cdots & 0 \\ -1 & \alpha_2 & 1 & \cdots & 0 \\ 0 & -1 & \alpha_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_n \end{bmatrix}$$

satisfies

$$\begin{aligned} |A_1| &= \alpha_1 \\ |A_2| &= 1 + \alpha_1\alpha_2, \\ |A_n| &= \alpha_n |A_{n-1}| + |A_{n-2}|. \end{aligned}$$

(8) Show that an $n \times m$ matrix has (column) rank $\geq k$ if and only there is a submatrix of size $k \times k$ with nonzero determinant. Use this to prove that row and column ranks are equal.

(9) (a) Show that the area of the triangle whose vertices are

$$\begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}, \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix}, \begin{bmatrix} \alpha_3 \\ \beta_3 \end{bmatrix} \in \mathbb{R}^2$$

is given by

$$\frac{1}{2}\begin{vmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{vmatrix}.$$

(b) Show that 3 vectors

$$\begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}, \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix}, \begin{bmatrix} \alpha_3 \\ \beta_3 \end{bmatrix} \in \mathbb{R}^2$$

satisfy

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{vmatrix} = 0$$

if and only if they are collinear, i.e., lie on a line $l = \{at + b : t \in \mathbb{R}\}$, where $a, b \in \mathbb{R}^2$.

(c) Show that 4 vectors

$$\begin{bmatrix} \alpha_1 \\ \beta_1 \\ \gamma_1 \end{bmatrix}, \begin{bmatrix} \alpha_2 \\ \beta_2 \\ \gamma_2 \end{bmatrix}, \begin{bmatrix} \alpha_3 \\ \beta_3 \\ \gamma_3 \end{bmatrix}, \begin{bmatrix} \alpha_4 \\ \beta_4 \\ \gamma_4 \end{bmatrix} \in \mathbb{R}^3$$

satisfy

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \end{vmatrix} = 0$$

if and only if they are coplanar, i.e., lie in the same plane $\pi = \left\{ x \in \mathbb{R}^3 : (a, x) = \alpha \right\}$.

(10) Let

$$\begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}, \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix}, \begin{bmatrix} \alpha_3 \\ \beta_3 \end{bmatrix} \in \mathbb{R}^2$$

be three points in the plane.

(a) If $\alpha_1, \alpha_2, \alpha_3$ are distinct, then the equation for the parabola $y = ax^2 + bx + c$ passing through the three given points is given by

$$\frac{\begin{vmatrix} 1 & 1 & 1 & 1 \\ x & \alpha_1 & \alpha_2 & \alpha_3 \\ x^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \\ y & \beta_1 & \beta_2 & \beta_3 \end{vmatrix}}{\begin{vmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{vmatrix}} = 0.$$

(b) If the points are not collinear, then the equation for the circle $x^2 + y^2 + ax + by + c = 0$ passing through the three given points is given by

$$\frac{\begin{vmatrix} 1 & 1 & 1 & 1 \\ x & \alpha_1 & \alpha_2 & \alpha_3 \\ y & \beta_1 & \beta_2 & \beta_3 \\ x^2 + y^2 & \alpha_1^2 + \beta_1^2 & \alpha_2^2 + \beta_2^2 & \alpha_3^2 + \beta_3^2 \end{vmatrix}}{\begin{vmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{vmatrix}} = 0.$$

5. Determinants of Linear Operators

To define the determinant of a linear operator $L : V \to V$ we simply note that $\operatorname{vol}(L(x_1), ..., L(x_n))$ defines an alternating n-form that is linear in each variable. Thus

$$\operatorname{vol}(L(x_1), ..., L(x_n)) = \det(L) \operatorname{vol}(x_1, ..., x_n)$$

for some scalar $\det(L) \in \mathbb{F}$. This is the determinant of L. We note that a different volume form $\mathrm{vol}_1(x_1, ..., x_n)$ gives the same definition of the determinant. To see this we first use that $\mathrm{vol}_1 = \lambda\,\mathrm{vol}$ and then observe that

$$\begin{aligned}\mathrm{vol}_1(L(x_1), ..., L(x_n)) &= \lambda\,\mathrm{vol}(L(x_1), ..., L(x_n)) \\ &= \det(L)\,\lambda\,\mathrm{vol}(x_1, ..., x_n) \\ &= \det(L)\,\mathrm{vol}_1(x_1, ..., x_n).\end{aligned}$$

If $e_1, ..., e_n$ is chosen so that $\mathrm{vol}(e_1, ..., e_n) = 1$, then we get the simpler formula

$$\mathrm{vol}(L(e_1), ..., L(e_n)) = \det(L).$$

This leads us to one of the standard formulas for the determinant of a matrix. From the properties of volume forms we see that

$$\begin{aligned}\det(L) &= \mathrm{vol}(L(e_1), ..., L(e_n)) \\ &= \sum \alpha_{i_1 1} \cdots \alpha_{i_n n}\,\mathrm{vol}(e_{i_1}, ..., e_{i_n}) \\ &= \sum \pm\alpha_{i_1 1} \cdots \alpha_{i_n n} \\ &= \sum \mathrm{sign}(i_1, ..., i_n)\,\alpha_{i_1 1} \cdots \alpha_{i_n n},\end{aligned}$$

where $[\alpha_{ij}] = [L]$ is the matrix representation for L with respect to $e_1, ..., e_n$. This formula is often used as the definition of determinants. Note that it also shows that $\det(L) = \det([L])$ since

$$\begin{aligned}\begin{bmatrix} L(e_1) & \cdots & L(e_n) \end{bmatrix} &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}[L] \\ &= \begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix}\begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{bmatrix}\end{aligned}$$

The next proposition contains the fundamental properties for determinants.

Proposition 31. (Determinant Characterization of Invertibility)

(1) *If $L, K : V \to V$ are linear operators, then*

$$\det(L \circ K) = \det(L)\det(K)$$

(2) $\det(\alpha 1_V) = \alpha^n$.

(3) *If L is invertible then*

$$\det L^{-1} = \frac{1}{\det L}.$$

(4) *If $\det(L) \neq 0$, then L is invertible.*

Proof. For any $x_1, ..., x_n$ we have

$$\begin{aligned}\det(L \circ K)\,\mathrm{vol}(x_1, ..., x_n) &= \mathrm{vol}(L \circ K(x_1), ..., L \circ K(x_n)) \\ &= \det(L)\,\mathrm{vol}(K(x_1), ..., L(x_n)) \\ &= \det(L)\det(K)\,\mathrm{vol}(x_1, ..., x_n).\end{aligned}$$

The second property follows from

$$\mathrm{vol}(\alpha x_1, ..., \alpha x_n) = \alpha^n\,\mathrm{vol}(x_1, ..., x_n).$$

For the third we simply use that $1_V = L \circ L^{-1}$ so

$$1 = \det(L)\det\left(L^{-1}\right).$$

For the last property select a basis $x_1, ..., x_n$ for V. Then

$$\begin{aligned} \operatorname{vol}(L(x_1), ..., L(x_n)) &= \det(L) \operatorname{vol}(x_1, ..., x_n) \\ &\neq 0. \end{aligned}$$

Thus $L(x_1), ..., L(x_n)$ is also a basis for V. This implies that L is invertible. □

One can in fact show that any map $\Delta : \hom(V, V) \to \mathbb{F}$ such that

$$\begin{aligned} \Delta(K \circ L) &= \Delta(K) \Delta(L) \\ \Delta(1_V) &= 1 \end{aligned}$$

depends only on the determinant of the operator (see also exercises).

We have some further useful and interesting results for determinants of matrices.

PROPOSITION 32. *If* $A \in \operatorname{Mat}_{n\times n}(\mathbb{F})$ *can be written in block form*

$$A = \begin{bmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{bmatrix},$$

where $A_{11} \in \operatorname{Mat}_{n_1\times n_1}(\mathbb{F})$, $A_{12} \in \operatorname{Mat}_{n_1\times n_2}(\mathbb{F})$, *and* $A_{22} \in \operatorname{Mat}_{n_2\times n_2}(\mathbb{F})$, $n_1 + n_2 = n$, *then*

$$\det A = \det A_{11} \det A_{22}.$$

PROOF. Write the canonical basis for $\mathbb{F}^n$ as $e_1, ..., e_{n_1}, f_1, ..., f_{n_2}$ according to the block decomposition. Next observe that A can be written as a composition in the following way

$$\begin{aligned} A &= \begin{bmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{bmatrix} \\ &= \begin{bmatrix} 1 & A_{12} \\ 0 & A_{22} \end{bmatrix} \begin{bmatrix} A_{11} & 0 \\ 0 & 1 \end{bmatrix} \\ &= BC \end{aligned}$$

Thus it suffices to show that

$$\begin{aligned} \det \begin{bmatrix} 1 & A_{12} \\ 0 & A_{22} \end{bmatrix} &= \det B \\ &= \det(A_{22}) \end{aligned}$$

and

$$\begin{aligned} \det \begin{bmatrix} A_{11} & 0 \\ 0 & 1 \end{bmatrix} &= \det C \\ &= \det(A_{11}). \end{aligned}$$

To prove the last formula note that for fixed $f_1, ..., f_{n_2}$ and

$$x_1, ..., x_{n_1} \in \operatorname{span}\{e_1, ..., e_{n_1}\}$$

the volume form

$$\operatorname{vol}(x_1, ..., x_{n_1}, f_1, ..., f_{n_2})$$

defines the usual volume form on $\operatorname{span}\{e_1, ..., e_{n_1}\} = \mathbb{F}^{n_1}$. Thus

$$\begin{aligned} \det C &= \operatorname{vol}(C(e_1), ..., C(e_{n_1}), C(f_1), ..., C(f_{n_2})) \\ &= \operatorname{vol}(A_{11}(e_1), ..., A_{11}(e_{n_1}), f_1, ..., f_{n_2}) \\ &= \det A_{11}. \end{aligned}$$

For the first equation we observe

$$\begin{aligned}\det B &= \operatorname{vol}\left(B\left(e_1\right),...,B\left(e_{n_1}\right),B\left(f_1\right),...,B\left(f_{n_2}\right)\right)\\ &= \operatorname{vol}\left(e_1,...,e_{n_1},A_{12}\left(f_1\right)+A_{22}\left(f_1\right),...,A_{12}\left(f_{n_2}\right)+A_{22}\left(f_{n_2}\right)\right)\\ &= \operatorname{vol}\left(e_1,...,e_{n_1},A_{22}\left(f_1\right),...,A_{22}\left(f_{n_2}\right)\right)\end{aligned}$$

since $A_{12}\left(f_j\right)\in\operatorname{span}\left\{e_1,...,e_{n_1}\right\}$. Then we get $\det B=\det A_{22}$ as before. □

PROPOSITION 33. *If* $A\in\operatorname{Mat}_{n\times n}\left(\mathbb{F}\right)$, *then* $\det A=\det A^t$.

PROOF. First note that the result is obvious if A is upper triangular. Using row operations we can always find an invertible P such that PA is upper triangular. Here P is a product of the elementary matrices of the types I_{ij} and $R_{ij}\left(\alpha\right)$. The row interchange matrices I_{ij} are symmetric, i.e., $I_{ij}^t=I_{ij}$ and have $\det I_{ij}=-1$. While $R_{ji}\left(\alpha\right)$ is upper or lower triangular with 1s on the diagonal. Hence $\left(R_{ij}\left(\alpha\right)\right)^t=R_{ji}\left(\alpha\right)$ and $\det R_{ij}\left(\alpha\right)=1$. In particular, it follows that $\det P=\det P^t=\pm1$. Thus

$$\begin{aligned}\det A &= \frac{\det\left(PA\right)}{\det P}\\ &= \frac{\det\left(\left(PA\right)^t\right)}{\det\left(P\right)^t}\\ &= \frac{\det\left(A^tP^t\right)}{\det\left(P\right)^t}\\ &= \det\left(A^t\right)\end{aligned}$$

□

This last proposition tells us that the determinant map $A\to|A|$ defined on $\operatorname{Mat}_{n\times n}\left(\mathbb{F}\right)$ is linear and alternating in both columns and rows. This can be extremely useful when calculating determinants. It also tells us that one can do Laplace expansions along columns as well as rows.

5.1. Exercises.

(1) Find the determinant of

$$\begin{aligned}L &: \operatorname{Mat}_{n\times n}\left(\mathbb{F}\right)\to\operatorname{Mat}_{n\times n}\left(\mathbb{F}\right)\\ L\left(X\right) &= X^t.\end{aligned}$$

(2) Find the determinant of $L:P_n\to P_n$ where
  (a) $L\left(p\left(t\right)\right)=p\left(-t\right)$
  (b) $L\left(p\left(t\right)\right)=p\left(t\right)+p\left(-t\right)$
  (c) $L\left(p\right)=Dp=p'$.

(3) Find the determinant of $L=p\left(D\right)$, for $p\in\mathbb{C}\left[t\right]$ when restricted to the spaces
  (a) $V=P_n$.
  (b) $V=\operatorname{span}\left\{\exp\left(\lambda_1t\right),...,\exp\left(\lambda_nt\right)\right\}$.

(4) Let $L:V\to V$ be an operator on a finite dimensional inner product space. Show that

$$\overline{\det\left(L\right)}=\det\left(L^*\right).$$

(5) Let V be an n-dimensional inner product space and vol a volume form so that $\operatorname{vol}\left(e_1,...,e_n\right)=1$ for some orthonormal basis $e_1,...,e_n$.

(a) If $L : V \to V$ is an isometry, then $|\det L| = 1$.
(b) Show that the set of isometries L with $\det L = 1$ forms a group.

(6) Show that $O \in O_n$ has type I if and only if $\det(O) = 1$. Conclude that SO_n is a group.

(7) Given $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ consider the two linear operators $L_A(X) = AX$ and $R_A(X) = XA$ on $\mathrm{Mat}_{n\times n}(\mathbb{F})$. Compute the determinant for these operators in terms of the determinant for A.

(8) If $L : V \to V$ is a linear operator and vol a volume form on V, then

$$\begin{aligned}\operatorname{tr}(A)\operatorname{vol}(x_1,\dots,x_n) &= \operatorname{vol}(L(x_1),\dots,x_n)\\ &\quad+\operatorname{vol}(x_1,L(x_2),\dots,x_n)\\ &\quad\vdots\\ &\quad+\operatorname{vol}(x_1,\dots,L(x_n)).\end{aligned}$$

(9) Show that

$$p(t) = \det\begin{bmatrix} 1 & \cdots & 1 & 1\\ \lambda_1 & \cdots & \lambda_n & t\\ \vdots & & \vdots & \vdots\\ \lambda_1^n & \cdots & \lambda_n^n & t^n\end{bmatrix}$$

defines a polynomial of degree n whose roots are $\lambda_1,\dots,\lambda_n$. Compute k where

$$p(t) = k(t-\lambda_1)\cdots(t-\lambda_n)$$

by doing a Laplace expansion along the last column.

(10) Assume that the $n \times n$ matrix A has a block decomposition

$$A = \begin{bmatrix} A_{11} & A_{12}\\ A_{21} & A_{22}\end{bmatrix},$$

where A_{11} is an invertible matrix. Show that

$$\det(A) = \det(A_{11})\det\left(A_{22} - A_{21}A_{11}^{-1}A_{12}\right).$$

Hint: Select a suitable product decomposition of the form

$$\begin{bmatrix} A_{11} & A_{12}\\ A_{21} & A_{22}\end{bmatrix} = \begin{bmatrix} B_{11} & 0\\ B_{21} & B_{22}\end{bmatrix}\begin{bmatrix} C_{11} & C_{12}\\ 0 & C_{22}\end{bmatrix}.$$

(11) *(Jacobi's Theorem)* Let A be an invertible $n \times n$ matrix. Assume that A and A^{-1} have block decompositions

$$\begin{aligned} A &= \begin{bmatrix} A_{11} & A_{12}\\ A_{21} & A_{22}\end{bmatrix},\\ A^{-1} &= \begin{bmatrix} A'_{11} & A'_{12}\\ A'_{21} & A'_{22}\end{bmatrix}.\end{aligned}$$

Show

$$\det(A)\det(A'_{22}) = \det(A_{11}).$$

Hint: Compute the matrix product

$$\begin{bmatrix} A_{11} & A_{12}\\ A_{21} & A_{22}\end{bmatrix}\begin{bmatrix} 1 & A'_{12}\\ 0 & A'_{22}\end{bmatrix}.$$

(12) Let $A = \mathrm{Mat}_{n\times n}(\mathbb{F})$. We say that A has an LU decomposition if $A = LU$, where L is lower triangular with 1s on the diagonal and U is upper triangular. Show that A has an LU decomposition if all the *leading principal minors* have nonzero determinant. The leading principal $k\times k$ minor is the $k\times k$ submatrix gotten from A by eliminating the last $n-k$ rows and columns.

(13) *(Sylvester's Criterion)* Let A be a real and symmetric $n\times n$ matrix. Show that A has positive eigenvalues if and only if all leading principal minors have positive determinant. Hint: As with the $A = LU$ decomposition in the previous exercise show by induction on n that $A = U^*U$, where U is upper triangular. Such a decomposition is also called a *Choleski factorization*.

(14) *(Characterization of Determinant Functions)* Let $\Delta : \mathrm{Mat}_{n\times n}(\mathbb{F}) \to \mathbb{F}$ be a function such that

$$\begin{aligned}\Delta(AB) &= \Delta(A)\,\Delta(B),\\ \Delta(1_{\mathbb{F}^n}) &= 1.\end{aligned}$$

(a) Show that there is a function $f : \mathbb{F} \to \mathbb{F}$ satisfying

$$f(\alpha\beta) = f(\alpha)\,f(\beta)$$

such that $\Delta(A) = f(\det(A))$. Hint: Use the relationships between the elementary matrices established in the exercises to "Row Reduction" to show that

$$\begin{aligned}\Delta(I_{ij}) &= \pm 1,\\ \Delta(M_i(\alpha)) &= \Delta(M_1(\alpha)),\\ \Delta(R_{kl}(\alpha)) &= \Delta(R_{kl}(1)) = \Delta(R_{12}(1)),\end{aligned}$$

and define $f(\alpha) = \Delta(M_1(\alpha))$.

(b) If $\mathbb{F} = \mathbb{R}$ and n is even show that $\Delta(A) = |\det(A)|$ defines a function such that

$$\begin{aligned}\Delta(AB) &= \Delta(A)\,\Delta(B),\\ \Delta(\lambda 1_{\mathbb{R}^n}) &= \lambda^n.\end{aligned}$$

(c) If $\mathbb{F} = \mathbb{C}$ and in addition $\Delta(\lambda 1_{\mathbb{C}^n}) = \lambda^n$, then show that $\Delta(A) = \det(A)$.

(d) If $\mathbb{F} = \mathbb{R}$ and in addition $\Delta(\lambda 1_{\mathbb{R}^n}) = \lambda^n$, where n is odd, then show that $\Delta(A) = \det(A)$.

6. Linear Equations

Cramer's rule is a formula for the solution to n linear equations in n variables when we know that only one solution exists. We will generalize this construction a bit so as to see that it can be interpreted as an inverse to the isomorphism

$$\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} : \mathbb{F}^n \to V$$

when $x_1, ..., x_n$ is a basis.

THEOREM 44. *Let V be an n dimensional vector space and* vol *a volume form. If $x_1, ..., x_n$ is a basis for V and $x = x_1\alpha_1 + \cdots x_n\alpha_n$ is the expansion of $x \in V$ with respect to that basis, then*

$$\begin{aligned}
\alpha_1 &= \frac{\operatorname{vol}(x, x_2, ..., x_n)}{\operatorname{vol}(x_1, ..., x_n)}, \\
&\vdots \\
\alpha_i &= \frac{\operatorname{vol}(x_1, ..., x_{i-1}, x, x_{i+1}, ..., x_n)}{\operatorname{vol}(x_1, ..., x_n)}, \\
&\vdots \\
\alpha_n &= \frac{\operatorname{vol}(x_1, ..., x_{n-1}, x)}{\operatorname{vol}(x_1, ..., x_n)}.
\end{aligned}$$

PROOF. First note that each α_i depends linearly on x. Thus we have defined a linear map $V \to \mathbb{F}^n$. This means that we only need to check what happens when x is one of the vectors in the basis. If $x = x_i$, then

$$\begin{aligned}
\alpha_1 &= \frac{\operatorname{vol}(x_i, x_2, ..., x_n)}{\operatorname{vol}(x_1, ..., x_n)} = 0, \\
&\vdots \\
\alpha_i &= \frac{\operatorname{vol}(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n)}{\operatorname{vol}(x_1, ..., x_n)} = 1, \\
&\vdots \\
\alpha_n &= \frac{\operatorname{vol}(x_1, ..., x_{n-1}, x_i)}{\operatorname{vol}(x_1, ..., x_n)} = 0.
\end{aligned}$$

Showing that x_i is mapped to e_i. This means that it is the inverse to

$$\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} : \mathbb{F}^n \to V.$$

□

Cramer's rule isn't necessarily very practical when solving equations, but it is often a useful abstract tool. It also comes in handy, as we shall see below in "Differential Equations" when solving inhomogeneous linear differential equations.

Cramer's rule can also be used to solve linear equations $L(x) = b$, as long as $L : V \to V$ is an isomorphism. In particular, it can be used to compute the inverse of L as is done in one of the exercises. To see how we can solve $L(x) = b$, we first select a basis $x_1, ..., x_n$ for V and then consider the problem of solving

$$\begin{bmatrix} L(x_1) & \cdots & L(x_n) \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = b.$$

Since $L(x_1), ..., L(x_n)$ is also a basis we know that this forces

$$\begin{aligned}
\alpha_1 &= \frac{\operatorname{vol}(b, L(x_2), ..., L(x_n))}{\operatorname{vol}(L(x_1), ..., L(x_n))}, \\
&\vdots \\
\alpha_i &= \frac{\operatorname{vol}(L(x_1), ..., L(x_{i-1}), b, L(x_{i+1}), ..., L(x_n))}{\operatorname{vol}(L(x_1), ..., L(x_n))}, \\
&\vdots \\
\alpha_n &= \frac{\operatorname{vol}(L(x_1), ..., L(x_{n-1}), b)}{\operatorname{vol}(L(x_1), ..., L(x_n))}
\end{aligned}$$

with $x = x_1\alpha_1 + \cdots x_n\alpha_n$ being the solution. If we use $b = x_1, ..., x_n$, then we get the matrix representation for L^{-1} by finding the coordinates to the solutions of $L(x) = x_i$.

As an example let us see how we can solve

$$\begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ 1 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}.$$

First we see directly that

$$\begin{aligned}
\xi_2 &= \beta_1, \\
\xi_3 &= \beta_2, \\
&\vdots \\
\xi_1 &= \beta_n.
\end{aligned}$$

From Cramer's rule we get that

$$\xi_1 = \frac{\begin{vmatrix} \beta_1 & 1 & \cdots & 0 \\ \beta_2 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ \beta_n & 0 & \cdots & 0 \end{vmatrix}}{\begin{vmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ 1 & 0 & \cdots & 0 \end{vmatrix}}$$

A Laplace expansion along the first column tells us that

$$\begin{vmatrix} \beta_1 & 1 & \cdots & 0 \\ \beta_2 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ \beta_n & 0 & \cdots & 0 \end{vmatrix} = \beta_1 \begin{vmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ 0 & 0 & \cdots & 0 \end{vmatrix} - \beta_2 \begin{vmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ 0 & 0 & \cdots & 0 \end{vmatrix}$$

$$\cdots + (-1)^{n+1} \beta_n \begin{vmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 1 \end{vmatrix}$$

here all of the determinants are upper triangular and all but the last has zeros on the diagonal. Thus

$$\begin{vmatrix} \beta_1 & 1 & \cdots & 0 \\ \beta_2 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ \beta_n & 0 & \cdots & 0 \end{vmatrix} = (-1)^{n+1} \beta_n$$

Similarly

$$\begin{vmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ 1 & 0 & \cdots & 0 \end{vmatrix} = (-1)^{n+1}$$

so

$$\xi_1 = \beta_n.$$

Similar calculations will confirm our answers for $\xi_2, ..., \xi_n$. By using $b = e_1, ..., e_n$ we can also find the inverse

$$\begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ 1 & 0 & \cdots & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & 0 & \cdots & 1 \\ 1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 1 & 0 \end{bmatrix}.$$

6.1. Exercises.

(1) Let

$$A_n = \begin{bmatrix} 2 & -1 & 0 & \cdots & 0 \\ -1 & 2 & -1 & \cdots & 0 \\ 0 & -1 & 2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & -1 \\ 0 & 0 & \cdots & -1 & 2 \end{bmatrix}.$$

(a) Compute $\det A_n$ for $n = 1, 2, 3, 4$.
(b) Compute A_n^{-1} for $n = 1, 2, 3, 4$.
(c) Find $\det A_n$ and A_n^{-1} for general n.

(2) Given a nontrivial volume form vol on an n-dimensional vector space V, a linear operator $L : V \to V$ and a basis $x_1, ..., x_n$ for V define the *classical adjoint* $\text{adj}(L) : V \to V$ by

$$\begin{aligned}\text{adj}(L)(x) &= \text{vol}(x, L(x_2), ..., L(x_n))\, x_1 \\ &\quad + \text{vol}(L(x_1), x, L(x_3), ..., L(x_n))\, x_2 \\ &\quad \vdots \\ &\quad + \text{vol}(L(x_1), ..., L(x_{n-1}), x)\, x_n.\end{aligned}$$

(a) Show that $L \circ \text{adj}(L) = \text{adj}(L) \circ L = \det(L)\, 1_V$.

(b) Show that if L is an $n \times n$ matrix, then $\text{adj}(L) = (\text{cof} A)^t$, where $\text{cof} A$ is the cofactor matrix whose ij entry is $(-1)^{i+j} \det A_{ij}$, where A_{ij} is the $(n-1) \times (n-1)$ matrix obtained from A by deleting the i^{th} row and j^{th} column.

(c) Show that $\text{adj}(L)$ does not depend on the choice of basis $x_1, ..., x_n$ or volume form vol.

(3) *(Lagrange Interpolation)* Use Cramer's rule and

$$p(t) = \det \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \lambda_1 & \cdots & \lambda_n & t \\ \vdots & & \vdots & \vdots \\ \lambda_1^n & \cdots & \lambda_n^n & t^n \end{bmatrix}$$

to find $p \in P_n$ such that $p(t_0) = b_0, ..., p(t_n) = b_n$ where $t_0, ..., t_n \in \mathbb{C}$ are distinct.

(4) Let $A \in \text{Mat}_{n\times n}(\mathbb{F})$, where $\mathbb{F}$ is $\mathbb{R}$ or $\mathbb{C}$. Show that there is a constant C_n depending only on n such that if A is invertible, then

$$\left\| A^{-1} \right\| \leq C_n \frac{\|A\|^{n-1}}{|\det(A)|}.$$

(5) Let A be an $n \times n$ matrix whose entries are integers. If A is invertible show that A^{-1} has integer entries if and only if $\det(A) = \pm 1$.

(6) Decide when the system

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix}$$

can be solved for all β_1, β_2. Write down a formula for the solution.

(7) For which α is the matrix invertible

$$\begin{bmatrix} \alpha & \alpha & 1 \\ \alpha & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}?$$

(8) In this exercise we will see how Cramer used his rule to study Leibniz's problem of when $Ax = b$ can be solved assuming that $A \in \text{Mat}_{(n+1)\times n}(\mathbb{F})$ and $b \in \mathbb{F}^{n+1}$. Assume in addition that $\text{rank}(A) = n$. Then delete one row from $[A|b]$ so that the resulting system $[A'|b']$ has a unique solution. Use Cramer's rule to solve $A'x = b'$ and then insert this solution in the equation that was deleted. Show that this equation is satisfied if and only if $\det[A|b] = 0$. Hint: The last equation is equivalent to a Laplace expansion of $\det[A|b] = 0$ along the deleted row.

(9) For $a, b, c \in \mathbb{C}$ consider the real equation $a\xi + bv = c$, where $\xi, v \in \mathbb{R}$.
  (a) Write this as a system of the real equations.
  (b) Show that this system has a unique solution when $\operatorname{Im}(\bar{a}b) \neq 0$.
  (c) Use Cramer's rule to find a formula for ξ and v that depends $\operatorname{Im}(\bar{a}b)$, $\operatorname{Im}(\bar{a}c)$, $\operatorname{Im}(\bar{b}c)$.

7. The Characteristic Polynomial

Now that we know that the determinant of a linear operator characterizes whether or not it is invertible it would seem perfectly natural to define the characteristic polynomial of $L : V \to V$ by

$$\chi_L(t) = \det(t1_V - L).$$

Clearly a zero for the function $\chi_L(t)$ corresponds a value of t where $t1_V - L$ is not invertible and therefore $\ker(t1_V - L) \neq \{0\}$, but this means that such a t is an eigenvalue. We now need to justify why this definition yields the same function we constructed using Gauss elimination.

THEOREM 45. *Let $A \in \operatorname{Mat}_{n\times n}(\mathbb{F})$, then $\chi_A(t) = \det(t1_{\mathbb{F}^n} - A)$ is a monic polynomial of degree n whose roots in $\mathbb{F}$ are the eigenvalues for $A : \mathbb{F}^n \to \mathbb{F}^n$. Moreover, this definition for the characteristic polynomial agrees with the one given using Gauss elimination.*

PROOF. First we show that if $L : V \to V$ is a linear operator on an n-dimensional vector space, then $\chi_L(t) = \det(t1_V - L)$ defines a monic polynomial of degree n. To see this consider

$$= \operatorname{vol}((t1_V - L)e_1, ..., (t1_V - L)e_n)$$

and use linearity of vol to separate each of the terms $(t1_V - L)e_k = te_k - L(e_k)$. When doing this we get to factor out t several times so it is easy to see that we get a polynomial in t. To check the degree we group terms involving powers of t that are lower than n in the expression $O(t^{n-1})$

$$\begin{aligned}
\det(t1_V - A) &= \operatorname{vol}((t1_V - L)e_1, ..., (t1_V - L)e_n) \\
&= t\operatorname{vol}(e_1, (t1_V - L)e_2, ..., (t1_V - L)e_n) \\
&\quad - \operatorname{vol}(L(e_1), (t1_V - L)e_2, ..., (t1_V - L)e_n) \\
&= t\operatorname{vol}(e_1, (t1_V - L)e_2, ..., (t1_V - L)e_n) + O(t^{n-1}) \\
&= t^2\operatorname{vol}(e_1, e_2, ..., (t1_V - L)e_n) + O(t^{n-1}) \\
&\quad \vdots \\
&= t^n\operatorname{vol}(e_1, e_2, ..., e_n) + O(t^{n-1}) \\
&= t^n + O(t^{n-1}).
\end{aligned}$$

In chapter 2 we proved that $(t1_{\mathbb{F}^n} - A) = PU$, where

$$U = \begin{bmatrix} r_1(t) & * & \cdots & * \\ 0 & r_2(t) & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r_n(t) \end{bmatrix}$$

and P is the product of the elementary matrices: 1. I_{kl} interchanging rows, 2. $R_{kl}(r(t))$ which multiplies row l by a function $r(t)$ and adds it to row k, and 3. $M_k(\alpha)$ which simply multiplies row k by $\alpha \in \mathbb{F} - \{0\}$. For each fixed t we have

$$\begin{aligned} \det(I_{kl}) &= -1, \\ \det(R_{kl}(r(t))) &= 1, \\ \det(M_k(\alpha)) &= \alpha. \end{aligned}$$

This means that

$$\begin{aligned} \det(t1_{\mathbb{F}^n} - A) &= \det(PT) \\ &= \det(P)\det(T) \\ &= \det(P)\, r_1(t)\cdots r_n(t) \end{aligned}$$

where $\det(P)$ is a nonzero scalar that does not depend on t and $r_1(t)\cdots r_n(t)$ is the function that we used to define the characteristic polynomial in chapter 2. This shows that the two definitions have to agree. □

With this new definition of the characteristic polynomial we can establish some further interesting properties.

Proposition 34. *Assume that* $L : V \to V$ *has*

$$\chi_L(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0.$$

Then

$$\begin{aligned} a_{n-1} &= -\operatorname{tr} L, \\ a_0 &= (-1)^n \det L. \end{aligned}$$

Proof. To show the last property just note that

$$\begin{aligned} a_0 &= \chi_L(0) \\ &= \det(-L) \\ &= (-1)^n \det(L). \end{aligned}$$

The first property takes a little more thinking. We use the calculation that lead to the formula

$$\begin{aligned} \det(t1_V - A) &= \operatorname{vol}((t1_V - L)x_1, ..., (t1_V - L)x_n) \\ &= t^n + O\left(t^{n-1}\right) \end{aligned}$$

from the previous proof. Evidently we have to calculate the coefficient in front of t^{n-1}. That term must look like

$$t^{n-1}\left(\operatorname{vol}(-L(e_1), e_2, ..., e_n) + \cdots + \operatorname{vol}(e_1, e_2, ..., -L(e_n))\right).$$

Thus we have to show

$$\operatorname{tr}(L) = \operatorname{vol}(L(e_1), e_2, ..., e_n) + \cdots + \operatorname{vol}(e_1, e_2, ..., L(e_n)).$$

To see this expand

$$L(e_i) = \sum_{j=1}^{n} e_j \alpha_{ji}$$

so that $[\alpha_{ji}] = [L]$ and $\operatorname{tr}(L) = \alpha_{11} + \cdots + \alpha_{nn}$. Next note that if we insert that expansion in, say, $\operatorname{vol}(L(e_1), e_2, ..., e_n)$, then we have

$$\begin{aligned}\operatorname{vol}(L(e_1), e_2 ..., e_n) &= \operatorname{vol}\left(\sum_{j=1}^{n} e_j \alpha_{j1}, e_2, ..., e_n\right) \\ &= \operatorname{vol}(e_1 \alpha_{11}, e_2, ..., e_n) \\ &= \alpha_{11} \operatorname{vol}(e_1, e_2, ..., e_n) \\ &= \alpha_{11}.\end{aligned}$$

This implies that

$$\begin{aligned}\operatorname{tr}(L) &= \alpha_{11} + \cdots + \alpha_{nn} \\ &= \operatorname{vol}(L(e_1), e_2, ..., e_n) + \\ &\quad \cdots + \operatorname{vol}(e_1, e_2, ..., L(e_n)).\end{aligned}$$

□

Proposition 35. *Assume that $L : V \to V$ and that $M \subset V$ is an L invariant subspace, then $\chi_{L|_M}(t)$ divides $\chi_L(t)$.*

Proof. Select a basis $x_1, ..., x_n$ for V such that $x_1, .., x_k$ form a basis for M. Then the matrix representation for L in this basis looks like

$$[L] = \begin{bmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{bmatrix},$$

where $A_{11} \in \operatorname{Mat}_{k \times k}(\mathbb{F})$, $A_{12} \in \operatorname{Mat}_{k \times (n-k)}(\mathbb{F})$, and $A_{22} \in \operatorname{Mat}_{(n-k) \times (n-k)}(\mathbb{F})$. This means that

$$t1_{\mathbb{F}^n} - [L] = \begin{bmatrix} t1_{\mathbb{F}^k} - A_{11} & A_{12} \\ 0 & t1_{\mathbb{F}^{n-k}} - A_{22} \end{bmatrix}.$$

Thus we have

$$\begin{aligned}\chi_L(t) &= \chi_{[L]}(t) \\ &= \det(t1_{\mathbb{F}^n} - [L]) \\ &= \det(t1_{\mathbb{F}^k} - A_{11}) \det(t1_{\mathbb{F}^{n-k}} - A_{22}).\end{aligned}$$

Now A_{11} is the matrix representation for $L|_M$ so we have proven

$$\chi_L(t) = \chi_{L|_M}(t)\, p(t)$$

where $p(t)$ is some polynomial. □

7.1. Exercises.

(1) Let $K, L : V \to V$ be linear operators.
  (a) Show that $\det(K - tL)$ is a polynomial in t.
  (b) If K or L is invertible show that $\det(tI - L \circ K) = \det(tI - K \circ L)$.
  (c) Show part b. in general.

(2) Let V be a finite dimensional real vector space and $L : V \to V$ a linear operator.
  (a) Show that the number of complex roots of the characteristic polynomial is even. Hint: They come in conjugate pairs.
  (b) If $\dim_{\mathbb{R}} V$ is odd then L has an eigenvalue whose sign is the same as that of $\det L$.

(c) If $\dim_{\mathbb{R}} V$ is even and $\det L < 0$ then L has two real eigenvalues, one negative and one positive.

(3) If
$$A = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix},$$
then
$$\begin{aligned} \chi_A(t) &= t^2 - (\operatorname{tr} A)\, t + \det A \\ &= t^2 - (\alpha + \delta)\, t + (\alpha\delta - \beta\gamma). \end{aligned}$$

(4) If $A \in \mathrm{Mat}_{3\times 3}(\mathbb{F})$ and $A = [\alpha_{ij}]$, then
$$\chi_A(t) = t^3 - (\operatorname{tr} A)\, t^2 + (|A_{11}| + |A_{22}| + |A_{33}|)\, t - \det A,$$
where A_{ii} are the companion matrix we get from eliminating the i^{th} row and column in A.

(5) If L is invertible then
$$\chi_{L^{-1}}(t) = \frac{(-t)^n}{\det L} \chi_L\left(t^{-1}\right).$$

(6) Let $L : V \to V$ be a linear operator on a finite dimensional inner product space with
$$\chi_L(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0.$$
Show that
$$\chi_{L^*}(t) = t^n + \bar{a}_{n-1}t^{n-1} + \cdots + \bar{a}_1 t + \bar{a}_0.$$

(7) Let
$$\chi_L(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$
be the characteristic polynomial for $L : V \to V$. If vol is a volume form on V show that
$$\begin{aligned} & (-1)^k a_{n-k} \operatorname{vol}(x_1, ..., x_n) \\ = & \sum_{i_1 < i_2 < \cdots < i_k} \operatorname{vol}(.., x_{i_1 - 1}, L(x_{i_1}), x_{i_1+1}, ..., x_{i_k - 1}, L(x_{i_k}), x_{i_k+1}, ..), \end{aligned}$$
i.e., we are summing over all possible choices of $i_1 < i_2 < \cdots < i_k$ and in each summand replacing x_{i_j} by $L\left(x_{i_j}\right)$.

(8) Suppose we have a sequence $V_1 \stackrel{L_1}{\to} V_2 \stackrel{L_2}{\to} V_3$ of linear maps, where L_1 is one-to-one, L_2 is onto, and $\operatorname{im}(L_1) = \ker(L_2)$. Show that $\dim V_2 = \dim V_1 \dim V_3$. Assume furthermore that we have linear operators $K_i : V_i \to V_i$ such that the diagram commutes
$$\begin{array}{ccccc} V_1 & \stackrel{L_1}{\longrightarrow} & V_2 & \stackrel{L_2}{\longrightarrow} & V_3 \\ K_1 \uparrow & & K_2 \uparrow & & K_3 \uparrow \\ V_1 & \stackrel{L_1}{\longrightarrow} & V_2 & \stackrel{L_2}{\longrightarrow} & V_3 \end{array}$$
Show that
$$\chi_{K_2}(t) = \chi_{K_1}(t)\, \chi_{K_3}(t).$$

(9) Using the definition
$$\det A = \sum \operatorname{sign}(i_1, ..., i_n)\, \alpha_{i_1 1} \cdots \alpha_{i_n n}$$
reprove the results from this section for matrices.

(10) *(The Newton Identities)* In this exercise we wish to generalize the formulae $a_{n-1} = -\operatorname{tr} L$, $a_0 = (-1)^n \det L$, for the characteristic polynomial

$$t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 = (t - \lambda_1)\cdots(t - \lambda_n)$$

of L.

(a) Prove that

$$a_k = (-1)^{n-k} \sum_{i_1 < \cdots < i_{n-k}} \lambda_{i_1} \cdots \lambda_{i_{n-k}}.$$

(b) Prove that

$$\begin{aligned} (\operatorname{tr} L)^k &= (\lambda_1 + \cdots + \lambda_n)^k, \\ \operatorname{tr}\left(L^k\right) &= \lambda_1^k + \cdots + \lambda_n^k. \end{aligned}$$

(c) Prove

$$\begin{aligned} (\operatorname{tr} L)^2 &= \operatorname{tr}\left(L^2\right) + 2\sum_{i<j} \lambda_i \lambda_j \\ &= \operatorname{tr}\left(L^2\right) + 2a_{n-2}. \end{aligned}$$

(d) Prove more generally that

$$\begin{aligned} (\operatorname{tr} L)^k &= k!\,(-1)^k a_{n-k} \\ &\quad + \binom{k}{2} (\operatorname{tr} L)^{k-2} \operatorname{tr} L^2 \\ &\quad + \left(\binom{k}{3} - \binom{k}{2}\right) (\operatorname{tr} L)^{k-3} \operatorname{tr} L^3 \\ &\quad + \left(\binom{k}{4} - \binom{k}{3} + \binom{k}{2}\right) (\operatorname{tr} L)^{n-4} \operatorname{tr} L^4 \\ &\quad \vdots \\ &\quad + \left(\binom{k}{k} - \binom{k}{k-1} + \cdots + (-1)^k \binom{k}{2}\right) \operatorname{tr} L^k. \end{aligned}$$

(e) If $\operatorname{tr} L = 0$, then

$$\left(\binom{n}{n} - \binom{n}{n-1} + \cdots + (-1)^n \binom{n}{2}\right) \operatorname{tr} L^n = n! \det L.$$

(f) If $\operatorname{tr} L = \operatorname{tr} L^2 = \cdots = \operatorname{tr} L^n = 0$, then $\chi_L(t) = t^n$.

8. Differential Equations*

We are now going to apply the theory of determinants to the study of linear differential equations. We start with the system $L(x) = \dot{x} - Ax = b$, where

$$\begin{aligned} x(t) &\in \mathbb{C}^n, \\ b &\in \mathbb{C}^n \\ A &\in \operatorname{Mat}_{n\times n}(\mathbb{C}) \end{aligned}$$

and $x(t)$ is the vector valued function we need to find. We know that the homogeneous problem $L(x) = 0$ has n linearly independent solutions $x_1, ..., x_n$. More generally we can show something quite interesting about collections of solutions.

LEMMA 24. *Let $x_1, ..., x_n$ be solutions to the homogeneous problem $L(x) = 0$, then*

$$\frac{d}{dt}(\text{vol}(x_1, ..., x_n)) = \text{tr}(A)\text{vol}(x_1, ..., x_n).$$

In particular

$$\text{vol}(x_1, ..., x_n)(t) = \text{vol}(x_1, ..., x_n)(t_0)\exp(\text{tr}(A)(t - t_0)).$$

Moreover, $x_1, ..., x_n$ are linearly independent solutions if and only if $x_1(t_0)$, ..., $x_n(t_0) \in \mathbb{C}^n$ are linearly independent. Each of these two conditions in turn imply that $x_1(t)$, ..., $x_n(t) \in \mathbb{C}^n$ are linearly independent for all t.

PROOF. To compute the derivative we find the Taylor expansion for

$$\text{vol}(x_1, ..., x_n)(t + h)$$

in terms of h and then identify the term that is linear in h. This is done along the lines of our proof that $a_{n-1} = -\text{tr}\,A$, where a_{n-1} is the coefficient in front of t^{n-1} in the characteristic polynomial.

$$\begin{aligned}
& \text{vol}(x_1, ..., x_n)(t + h) \\
= \; & \text{vol}(x_1(t + h), ..., x_n(t + h)) \\
= \; & \text{vol}(x_1(t) + Ax_1(t)h + o(h), ..., x_n(t) + Ax_n(t)h + o(h)) \\
= \; & \text{vol}(x_1(t), ..., x_n(t)) \\
& +h\,\text{vol}(Ax_1(t), ..., x_n(t)) \\
& \vdots \\
& +h\,\text{vol}(x_1(t), ..., Ax_n(t)) \\
& +o(h) \\
= \; & \text{vol}(x_1(t), ..., x_n(t)) + h\,\text{tr}(A)\text{vol}(x_1(t), ..., x_n(t)) + o(h).
\end{aligned}$$

Thus

$$v(t) = \text{vol}(x_1, ..., x_n)(t)$$

solves the differential equation

$$\dot{v} = \text{tr}(A)v.$$

implying that

$$v(t) = v(t_0)\exp(\text{tr}(A)(t - t_0)).$$

In particular, we see that $v(t) \neq 0$ provided only $v(t_0) \neq 0$.

It remains to prove that $x_1, ..., x_n$ are linearly independent solutions if and only if $x_1(t_0), ..., x_n(t_0) \in \mathbb{C}^n$ are linearly independent. It is obvious that $x_1, ..., x_n$ are linearly independent if $x_1(t_0), ..., x_n(t_0) \in \mathbb{C}^n$ are linearly independent. Conversely, if we assume that $x_1(t_0), ..., x_n(t_0) \in \mathbb{C}^n$ are linearly dependent, then we can find $\alpha_1, ..., \alpha_n \in \mathbb{C}^n$ not all zero so that

$$\alpha_1 x_1(t_0) + \cdots + \alpha_n x_n(t_0) = 0.$$

Uniqueness of solutions to the initial value problem $L(x) = 0$, $x(t_0) = 0$, then implies that

$$x(t) = \alpha_1 x_1(t) + \cdots + \alpha_n x_n(t) \equiv 0$$

for all t. □

We now claim that the inhomogeneous problem can be solved provided we have found a linearly independent set of solutions $x_1, ..., x_n$ to the homogeneous equation. The formula comes from Cramer's rule but is known as the *variations of constants method*. We assume that the solution x to

$$\begin{aligned} L(x) &= \dot{x} - Ax = b, \\ x(t_0) &= 0 \end{aligned}$$

looks like

$$x(t) = c_1(t)\, x_1(t) + \cdots + c_n(t)\, x_n(t),$$

where $c_1(t), ..., c_n(t) \in C^\infty(\mathbb{R}, \mathbb{C})$ are functions rather than constants. Then

$$\begin{aligned} \dot{x} &= c_1 \dot{x}_1 + \cdots + c_n \dot{x}_n + \dot{c}_1 x_1 + \cdots + \dot{c}_n x_n \\ &= c_1 A x_1 + \cdots + c_n A x_n + \dot{c}_1 x_1 + \cdots + \dot{c}_n x_n \\ &= A(x) + \dot{c}_1 x_1 + \cdots + \dot{c}_n x_n. \end{aligned}$$

In other terms

$$L(x) = \dot{c}_1 x_1 + \cdots + \dot{c}_n x_n.$$

This means that for each t the values $\dot{c}_1(t), ..., \dot{c}_n(t)$ should solve the linear equation

$$\dot{c}_1 x_1 + \cdots + \dot{c}_n x_n = b.$$

Cramer's rule for solutions to linear systems then tells us that

$$\begin{aligned} \dot{c}_1(t) &= \frac{\mathrm{vol}(b, ..., x_n)(t)}{\mathrm{vol}(x_1, ..., x_n)(t)}, \\ &\vdots \\ \dot{c}_n(t) &= \frac{\mathrm{vol}(x_1, ..., b)(t)}{\mathrm{vol}(x_1, ..., x_n)(t)}, \end{aligned}$$

implying that

$$\begin{aligned} c_1(t) &= \int_{t_0}^{t} \frac{\mathrm{vol}(b, ..., x_n)(s)}{\mathrm{vol}(x_1, ..., x_n)(s)} ds, \\ &\vdots \\ c_n(t) &= \int_{t_0}^{t} \frac{\mathrm{vol}(x_1, ..., b)(s)}{\mathrm{vol}(x_1, ..., x_n)(s)} ds. \end{aligned}$$

In practice there are more efficient methods that can be used when we know something about b. These methods also use linear algebra in order to solve certain linear systems of equations.

Having dealt with systems we next turn to higher order equations: $L(x) = p(D)(x) = f$, where

$$p(D) = D^n + a_{n-1} D^{n-1} + \cdots + a_1 D + a_0$$

is a polynomial with complex or real coefficients and $f(t) \in C^\infty(\mathbb{R}, \mathbb{C})$. This can be translated into a system $\dot{z} - Az = b$, or

$$\dot{z} - \begin{bmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 \\ -a_0 & \cdots & -a_{n-2} & -a_{n-1} \end{bmatrix} z = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ f \end{bmatrix},$$

by using

$$z=\begin{bmatrix} x \\ Dx \\ \vdots \\ D^{n-1}x \end{bmatrix}.$$

If we have n functions $x_1, ..., x_n \in C^{\infty}(\mathbb{R}, \mathbb{C})$, then the *Wronskian*

$$\begin{aligned}
\mathrm{W}(x_1, ..., x_n)(t) &= \mathrm{vol}(z_1, ..., z_n)(t) \\
&= \det \begin{bmatrix} x_1(t) & \cdots & x_n(t) \\ (Dx_1)(t) & \cdots & (Dx_n)(t) \\ \vdots & & \vdots \\ \left(D^{k-1}x_1\right)(t) & \cdots & \left(D^{k-1}x_n\right)(t) \end{bmatrix}.
\end{aligned}$$

In the case where $x_1, ..., x_n$ solve $L(x) = p(D)(x) = 0$ this tells us that

$$\mathrm{W}(x_1, ..., x_n)(t) = \mathrm{W}(x_1, ..., x_n)(t_0)\exp(-a_{n-1}(t-t_0)).$$

Finally we can again try the variation of constants method to solve the inhomogeneous equation. It is slightly tricky to do this directly by assuming that

$$x(t) = c_1(t)x_1(t) + \cdots + c_n(t)x_n(t).$$

Instead we use the system $\dot{z} - Az = b$, and guess that

$$z = c_1(t)z_1(t) + \cdots + c_n(t)z_n(t).$$

This certainly implies that

$$x(t) = c_1(t)x_1(t) + \cdots + c_n(t)x_n(t),$$

but the converse is not true. As above we get

$$\begin{aligned}
c_1(t) &= \int_{t_0}^{t} \frac{\mathrm{vol}(b, ..., z_n)(s)}{\mathrm{vol}(z_1, ..., z_n)(s)} ds, \\
&\vdots \\
c_n(t) &= \int_{t_0}^{t} \frac{\mathrm{vol}(z_1, ..., b)(s)}{\mathrm{vol}(z_1, ..., z_n)(s)} ds.
\end{aligned}$$

Here

$$\mathrm{vol}(z_1, ..., z_n) = \mathrm{W}(x_1, ..., x_n).$$

The numerator can also be simplified by using a Laplace expansion along the column vector b. This gives us

$$\begin{aligned}
\mathrm{vol}(b, z_2, ..., z_n) &= \begin{vmatrix} 0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \cdots & \vdots \\ 0 & D^{n-2}x_2 & \cdots & D^{n-2}x_n \\ b & D^{n-1}x_2 & \cdots & D^{n-1}x_n \end{vmatrix} \\
&= (-1)^{n+1} b \begin{vmatrix} x_1 & \cdots & x_n \\ \vdots & \cdots & \vdots \\ D^{n-2}x_2 & \cdots & D^{n-2}x_n \end{vmatrix} \\
&= (-1)^{n+1} b\mathrm{W}(x_2, ..., x_n).
\end{aligned}$$

Thus

$$
\begin{aligned}
c_1(t) &= (-1)^{n+1} \int_{t_0}^{t} \frac{b(s)\,\mathrm{W}(x_2, ..., x_n)(s)}{\mathrm{W}(x_1, ..., x_n)(s)} ds, \\
&\vdots \\
c_n(t) &= (-1)^{n+n} \int_{t_0}^{t} \frac{b(s)\,\mathrm{W}(x_1, ..., x_{n-1})(s)}{\mathrm{W}(x_1, ..., x_n)(s)} ds
\end{aligned}
$$

and therefore a solution to the inhomogeneous equation is given by

$$
\begin{aligned}
x(t) &= \left((-1)^{n+1} \int_{t_0}^{t} \frac{b(s)\,\mathrm{W}(x_2, ..., x_n)(s)}{\mathrm{W}(x_1, ..., x_n)(s)} ds\right) x_1(t) + \cdots \\
&\quad + \left((-1)^{n+n} \int_{t_0}^{t} \frac{b(s)\,\mathrm{W}(x_1, ..., x_{n-1})(s)}{\mathrm{W}(x_1, ..., x_n)(s)} ds\right) x_n(t) \\
&= \sum_{k=1}^{n} (-1)^{n+k} x_k(t) \int_{t_0}^{t} \frac{b(s)\,\mathrm{W}(x_1, ..., \hat{x}_k, ..., x_n)(s)}{\mathrm{W}(x_1, ..., x_n)(s)} ds
\end{aligned}
$$

Let us try to solve a concrete problem using these methods.

EXAMPLE 101. *Find the complete set of solutions to* $\ddot{x} - 2\dot{x} + x = \exp(t)$*. We see that* $\ddot{x} - 2\dot{x} + x = (D-1)^2 x$*, thus the characteristic equation is* $(\lambda - 1)^2 = 1$*. This means that we only get one solution* $x_1 = \exp(t)$ *from the eigenvalue* $\lambda = 1$*. The other solution is then given by* $x_2(t) = t\exp(t)$*. We now compute the Wronskian to check that they are linearly independent.*

$$
\begin{aligned}
\mathrm{W}(x_1, x_2) &= \begin{vmatrix} \exp(t) & t\exp(t) \\ \exp(t) & (1+t)\exp(t) \end{vmatrix} \\
&= \exp(2t) \begin{vmatrix} 1 & t \\ 1 & (1+t) \end{vmatrix} \\
&= ((1+t) - t)\exp(2t) \\
&= \exp(2t).
\end{aligned}
$$

Note we could also have found x_2 *from our knowledge that*

$$
\mathrm{W}(x_1, x_2)(t) = \mathrm{W}(x_1, x_2)(t_0)\exp(2(t - t_0)).
$$

Assuming that $t_0 = 0$ *and we want* $\mathrm{W}(x_1, x_2)(t_0) = 1$*, we simply need to solve*

$$
\mathrm{W}(x_1, x_2)(t) = x_1\dot{x}_2 - \dot{x}_1 x_2 = \exp(2t).
$$

Since $x_1 = \exp(t)$*, this implies that*

$$
\dot{x}_2 - x_2 = \exp(t).
$$

Hence

$$
\begin{aligned}
x_2(t) &= \exp(t) \int_0^t \exp(-s)\exp(t)\, ds \\
&= t\exp(t)
\end{aligned}
$$

as expected.

The variation of constants formula now tells us to compute

$$\begin{aligned} c_1(t) &= (-1)^{2+1}\int_0^t \frac{f(s)\,x_2(s)}{\mathrm{W}(x_1,x_2)(s)}ds \\ &= -\int_0^t \frac{\exp(s)\,(s\exp(s))}{\exp(2s)}ds \\ &= -\int_0^t sds \\ &= -\frac{1}{2}t^2 \end{aligned}$$

and

$$\begin{aligned} c_2(t) &= (-1)^{2+2}\int_0^t \frac{f(s)\,x_1(s)}{\mathrm{W}(x_1,x_2)(s)}ds \\ &= \int_0^t 1ds \\ &= t \end{aligned}$$

Thus

$$\begin{aligned} x &= -\frac{1}{2}t^2x_1(t)+tx_2(t) \\ &= -\frac{1}{2}t^2\exp(t)+t\,(t\exp(t)) \\ &= \frac{1}{2}t^2\exp(t) \end{aligned}$$

solves the inhomogeneous problem and $x=\alpha_1\exp(t)+\alpha_2 t\exp(t)+\frac{1}{2}t^2\exp(t)$ *represents the complete set of solutions.*

8.1. Exercises.

(1) Let $p_0(t),...,p_n(t)\in\mathbb{C}[t]$ and assume that $t\in\mathbb{R}$. If

$$p_i(t)=a_{ni}t^n+\cdots+a_{1i}t+a_{0i},$$

show that

$$\begin{aligned} \mathrm{W}(p_0,...,p_n) &= \det\begin{bmatrix} p_0(t) & \cdots & p_n(t) \\ (Dp_0)(t) & \cdots & (Dp_n)(t) \\ \vdots & & \vdots \\ (D^np_0)(t) & \cdots & (D^np_n)(t) \end{bmatrix} \\ &= \det\begin{bmatrix} a_{00} & \cdots & a_{0n} \\ a_{10} & \cdots & a_{1n} \\ 2a_{20} & \cdots & 2a_{2n} \\ \vdots & & \vdots \\ n!a_{n0} & \cdots & n!a_{nn} \end{bmatrix} \\ &= n!\cdot(n-1)!\cdot\cdots\cdot 2\cdot 1\det\begin{bmatrix} a_{00} & \cdots & a_{0n} \\ a_{10} & \cdots & a_{1n} \\ a_{20} & \cdots & a_{2n} \\ \vdots & & \vdots \\ a_{n0} & \cdots & a_{nn} \end{bmatrix} \end{aligned}$$

(2) Let $x_1, ..., x_n$ be linearly independent solutions to

$$p(D)(x) = \left(D^n + a_{n-1}D^{n-1} + \cdots + a_0\right)(x) = 0.$$

Do the following questions without using what we know about existence and uniqueness of solutions to differential equations.

(a) Show that

$$p(D)(x) = \frac{\mathrm{W}(x_1..., x_n, x)}{\mathrm{W}(x_1..., x_n)}.$$

(b) Conclude that $p(D)(x) = 0$ if and only if $\mathrm{W}(x, x_1..., x_n) = 0$.

(c) If $\mathrm{W}(x, x_1..., x_n) = 0$, then x is a linear combination of $x_1, ..., x_n$.

(d) If x, y are solutions with the same initial values: $x(0) = y(0)$, $Dx(0) = Dy(0), ..., D^{n-1}x(0) = D^{n-1}y(0)$, then $x = y$.

(3) Assume two monic polynomials $p, q \in \mathbb{C}[t]$ have the property that $p(D)(x) = 0$ and $q(D)(x) = 0$ have the same solutions. Is it true that $p = q$? Hint if $p(D)(x) = 0 = q(D)(x)$, then $\gcd(p, q)(D)(x) = 0$.

(4) Assume that x is a solution to $p(D)(x) = 0$, where $p(D) = D^n + \cdots + a_1D + a_0$.

(a) Show that the phase shifts $x_\omega(t) = x(t + \omega)$ are also solutions.

(b) If the vectors

$$\begin{bmatrix} x(\omega_1) \\ Dx(\omega_1) \\ \vdots \\ D^{n-1}x(\omega_1) \end{bmatrix}, ..., \begin{bmatrix} x(\omega_n) \\ Dx(\omega_n) \\ \vdots \\ D^{n-1}x(\omega_n) \end{bmatrix}$$

form a basis for $\mathbb{C}^n$, then all solutions to $p(D)(x) = 0$ are linear combinations of the phase shifted solutions $x_{\omega_1}, ..., x_{\omega_n}$.

(c) If the vectors

$$\begin{bmatrix} x(\omega_1) \\ Dx(\omega_1) \\ \vdots \\ D^{n-1}x(\omega_1) \end{bmatrix}, ..., \begin{bmatrix} x(\omega_n) \\ Dx(\omega_n) \\ \vdots \\ D^{n-1}x(\omega_n) \end{bmatrix}$$

never form a basis for $\mathbb{C}^n$, then x is a solution to a k^{th} order equation for $k < n$. Hint: If x is not a solution to a lower order equation, the $x, Dx, ..., D^{n-1}x$ is a (cyclic) basis for the solution space.

(5) Find a formula for the real solutions to the system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} - \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix},$$

where $a, b \in \mathbb{R}$ and $b_1, b_2 \in C^\infty(\mathbb{R}, \mathbb{R})$.

(6) Find a formula for the real solutions to the equation

$$\ddot{x} + a\dot{x} + bx = f,$$

where $a, b \in \mathbb{R}$ and $f \in C^\infty(\mathbb{R}, \mathbb{R})$.

Bibliography

[Axler] S. Axler, *Linear Algebra Done Right*, New York, Springer Verlag, 1997.

[Bretscher] O. Bretscher, *Linear Algebra with Applications 2nd Edition,* Upper Saddle River, Prentice-Hall, 2001.

[Curtis] C.W. Curtis, *Linear Algebra, An Introductory Approach*, New York, Springer Verlag, 1984.

[Greub] W. Greub, *Linear Algebra, 4th Edition*, New York, Springer Verlag, 1981.

[Halmos] P.R. Halmos, *Finite-Dimensional Vector Spaces*, New York, Springer Verlag, 1987.

[Hoffman-Kunze] K. Hoffman and R. Kunze, *Linear Algebra,* Upper Saddle River, Prentice-Hall, 1961.

[Lang] S. Lang, *Linear Algebra 3rd Edition*, New York, Springer Verlag, 1987.

[Roman] S. Roman, *Advanced Linear Algebra 2nd Edition*, New York, Springer Verlag, 2005.

[Serre] D. Serre, *Matrices, Theory and Applications*, New York, Springer Verlag, 2002.

Index