Linear Algebra
Math 308

S. Paul Smith

Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195
E-mail address: smith@math.washington.edu

Contents

Chapter 0. Introduction 1
1. What it's all about 1
2. Some practical applications 2
3. The importance of asking questions 2

Chapter 1. Linear Geometry 3
1. Linearity 3
2. Lines in $\mathbb{R}^2$ 10
3. Points, lines, and planes in $\mathbb{R}^3$ 13
4. Higher dimensions 15
5. Parametric descriptions of lines, planes, etc. 15

Chapter 2. Matrices 17
1. What is a matrix? 17
2. A warning about our use of the word vector 18
3. Row and column vectors = points with coordinates 18
4. Matrix arithmetic: addition and subtraction 20
5. The zero matrix and the negative of a matrix 20
6. Matrix arithmetic: multiplication 21
7. Pitfalls and warnings 25
8. Transpose 25
9. Some special matrices 26
10. Solving an equation involving an upper triangular matrix 27
11. Some special products 28

Chapter 3. Matrices and motions in $\mathbb{R}^2$ and $\mathbb{R}^3$ 31
1. Linear transformations 31
2. Rotations in the plane 31
3. Projections in the plane 31
4. Contraction and dilation 31
5. Reflections in the plane 31
6. Reflections in $\mathbb{R}^3$ 31
7. Projections from $\mathbb{R}^3$ to a plane 31

Chapter 4. Systems of Linear Equations 33
1. Systems of equations 33
2. A single linear equation 36

3. Systems of linear equations 37
4. A system of linear equations is a single matrix equation 38
5. Specific examples 38
6. The number of solutions 41
7. A geometric view on the number of solutions 41
8. Homogeneous systems 42

Chapter 5. Row operations and row equivalence 45
1. Equivalent systems of equations 45
2. Echelon Form 45
3. An example 46
4. You already did this in high school 47
5. The rank of a matrix 48
6. Inconsistent systems 49
7. Consistent systems 49
8. Parametric equations for lines and planes 51
9. The importance of rank 52
10. The word “solution” 53
11. Elementary matrices 54

Chapter 6. The Vector space $\mathbb{R}^n$ 57
1. Arithmetic in $\mathbb{R}^n$ 57
2. The standard basis for $\mathbb{R}^n$ 58
3. Linear combinations and linear span 58
4. Some infinite dimensional vector spaces 60

Chapter 7. Subspaces 61
1. The definition and examples 61
2. The row and column spaces of a matrix 64
3. Lines, planes, and translations of subspaces 65
4. Linguistic difficulties: algebra vs. geometry 67

Chapter 8. Linear dependence and independence 69
1. The definition 69
2. Criteria for linear (in)dependence 69
3. Linear (in)dependence and systems of equations 73

Chapter 9. Non-singular matrices, invertible matrices, and inverses 75
1. Singular and non-singular matrices 75
2. Inverses 76
3. Elementary matrices are invertible 78
4. Making use of inverses 78
5. The inverse of a 2×2 matrix 79
6. If A is non-singular how do we find A^{-1}? 81

Chapter 10. Bases, coordinates, and dimension 83
1. Definitions 83

2. A subspace of dimension d is just like $\mathbb{R}^d$ 83
3. All bases for W have the same number of elements 84
4. Every subspace has a basis 84
5. Properties of bases and spanning sets 85
6. How to find a basis for a subspace 86
7. How to find a basis for the range of a matrix 86
8. Rank + Nullity 86
9. How to compute the null space and range of a matrix 90

Chapter 11. Linear transformations 91
1. A reminder on functions 91
2. First observations 92
3. Linear transformations and matrices 94
4. How to find the matrix representing a linear transformation 95
5. Invertible matrices and invertible linear transformations 96
6. How to find the formula for a linear transformation 96
7. Rotations in the plane 96
8. Reflections in $\mathbb{R}^2$ 97
9. Invariant subspaces 98
10. The one-to-one and onto properties 98
11. Two-to-two 98
12. Gazing into the distance: differential operators as linear transformations 99

Chapter 12. Determinants 103
1. The definition 103
2. Elementary row operations and determinants 106
3. The determinant and invertibility 108
4. Properties 108
5. Elementary column operations and determinants 109

Chapter 13. Eigenvalues 113
1. Definitions and first steps 113
2. Reflections in $\mathbb{R}^2$, revisited 114
3. The 2×2 case 115
4. The equation $A^2 + I$ 116
5. The characteristic polynomial 117
6. How to find eigenvalues and eigenvectors 118
7. The utility of eigenvectors 122

Chapter 14. Complex vector spaces and complex eigenvalues 125
1. The complex numbers 125
2. The complex numbers 125
3. Linear algebra over $\mathbb{C}$ 129
4. The complex norm 129
5. An extended exercise 131

Chapter 15. Orthogonality 133
1. Geometry 133
2. The dot product 133
3. Orthogonal vectors 134
4. Classical orthogonal polynomials 135
5. Orthogonal and orthonormal bases 135
6. The Gram-Schmidt process 136
7. Orthogonal matrices 138
8. Orthogonal projections 140
9. Least-squares "solutions" to inconsistent systems 143
10. Approximating data by polynomial curves 146
11. Gazing into the distance: Fourier series 147
12. Infinite sequences 147

Chapter 16. Similar matrices 149
1. Definition 149
2. Definition and first properties 149
3. Example 150
4. 150
5. Diagonalizable matrices 152

Chapter 17. Words and terminology 157
1. The need for clarity and precision 157
2. Some, all, each, every, and only 157
3. Singular and plural 159
4. The word *"it"* 159
5. "A" and "The" 160
6. If and only if 160

Chapter 18. Applications of linear algebra and vector spaces 161
1. Simple electrical circuits 161
2. Magic squares 162

Chapter 19. Last rites 165
1. A summary of notation 165
2. A sermon 166

CHAPTER 0

Introduction

1. What it's all about

The practical problem, solving systems of linear equations, that motivates the subject of Linear Algebra, is introduced in chapter 4. Although the problem is concrete and easily understood, the methods and theoretical framework required for a deeper understanding of it are abstract. Linear algebra can be approached in a completely abstract fashion, untethered from the problems that give rise to the subject.

Such an approach is daunting for the average student so we will strike a balance between the practical, specific, abstract, and general.

Linear algebra plays a central role in almost all parts of modern technology. Systems of linear equations involving hundreds, thousands, even *billions* of unknowns are solved every second of every day in all corners of the globe. One of the more fantastic uses is the way in which Google prioritizes pages on the web. All web pages are assigned a *page rank* that measures its importance. The page ranks are the unknowns in an enormous system of linear equations. To find the page rank one must solve the system of linear equations. To handle such large systems of linear equations one uses sophisticated techniques that are developed first as abstract results about linear algebra.

Systems of linear equations are rephrased in terms of matrix equations, i.e., equations involving matrices. The translation is straightforward but after mastering the basics of "matrix arithmetic" one must interpret those basics in geometric terms. That leads to linear geometry and the language of vectors and vector spaces.

Chapter 1 provides a brief account of linear geometry. As the name suggests, linear geometry concerns lines. The material about lines in the plane is covered in high school. Unless you know that material backwards and forwards linear algebra will be impossible for you. Linear geometry also involves higher dimensional analogues of lines, for examples, lines and planes in 3-space, or $\mathbb{R}^3$ as we will denote it. I am assuming you met that material in a multivariable calculus course. Unless you know *that* material backwards and forwards linear algebra will be impossible for you.[1]

[1] I expect you to *know* the material about linear geometry in $\mathbb{R}^2$ and $\mathbb{R}^3$. By that I don't mean that you have simply passed a course where that material is covered. I expect you to have understood and mastered that material and that you retain that mastery today. If

After reviewing linear geometry we will review basic facts about matrices in chapter 2. That will be familiar to some students. Very little from chapter 2 is required to understand the initial material on systems of linear equations in chapter 4.

2. Some practical applications

(1) solving systems of linear equations
(2) birth-death processes, Leslie matrices (see Ch. 6 in Difference equations. From rabbits to chaos), Lotka-Volterra
(3) Google page rank
(4) X-ray tomography, MRI, density of tissue, a slice through the body is pixellated and each pixel has a different density to be inferred/computed from the input/output of sending various rays through the body. Generally many more measurements than unknowns so almost always obtain an inconsistent system but want the least-squares solution.

3. The importance of asking questions

You will quickly find that this is a difficult course. Everyone finds it difficult. The best advice I can give you is to ask questions. When you read something you don't understand don't just skim over it thinking you will return to it later and then fail to return to it. Ask, ask, ask. The main reason people fail this course is because they are afraid to ask questions. They think asking a question will make them look stupid. Smart people aren't afraid to ask questions. No one has all the answers.

The second most common reason people fail this course is that they wait till the week before the exam to start thinking seriously about the material. If you are smart you will try to understand every topic in this course at the time it first appears.

---

you are not in command of the material in chapter 1 master it as soon as possible. That is essential if you want to pass this course.

CHAPTER 1

Linear Geometry

1. Linearity

The word linear comes from the word "line".

The geometric aspect of linear algebra involves lines, planes, and their higher dimensional analogues: e.g., lines in the plane, lines in 3-space, lines in 4-space, planes in 3-space, planes in 4-space, 3-planes in 4-space, 5-planes in 8-space, and so on, ad infinitum. Such things form the subject matter of linear geometry.

Curvy things play no role in linear algebra or linear geometry. We ignore circles, spheres, ellipses, parabolas, etc. All is linear.

1.1. What is a line? You already "know" what a line is. More accurately, you know something about lines in the plane, $\mathbb{R}^2$, or in 3-space, $\mathbb{R}^3$. In this course, you need to know something about lines in n-space, $\mathbb{R}^n$.

1.2. What is $\mathbb{R}^n$? $\mathbb{R}^n$ is our notation for the set of all n-tuples of real numbers. We run out of words after *pair, triple, quadruple, quintuple, sextuple, ...* so invent the word *n-tuple* to refer to an ordered sequence of n numbers where n can be any positive integer.

For example, (8,7,6,5,4,3,2,1) is an 8-tuple. It is not the same as the 8-tuple (1,2,3,4,5,6,7,8). We think of these 8-tuples as labels for two different points in $\mathbb{R}^8$. We call the individual entries in (8,7,6,5,4,3,2,1) the coordinates of the point (8,7,6,5,4,3,2,1); thus 8 is the first coordinate, 7 the second coordinate, etc.

Often we need to speak about a point in $\mathbb{R}^n$ when we don't know its coordinates. In that case we will say something like this: *let* $(a_1, a_2, \ldots, a_n)$ *be a point in* $\mathbb{R}^n$. Here $a_1, a_2, \ldots, a_n$ are some arbitrary real numbers.

1.3. The origin. The origin is a special point in $\mathbb{R}^n$: it is the point having all its coordinates equal to 0. For example, (0,0) is the origin in $\mathbb{R}^2$; (0,0,0) is the origin in $\mathbb{R}^3$; (0,0,0,0) is the origin in $\mathbb{R}^4$; and so on. We often write $\underline{0}$ for the origin.

There is a special notation for the set of all points in $\mathbb{R}^n$ except the origin, namely $\mathbb{R}^n - \{\underline{0}\}$. We use the minus symbol because $\mathbb{R}^n - \{\underline{0}\}$ is obtained by taking $\underline{0}$ away from $\mathbb{R}^n$. Here "taking away" is synonymous with "removing". This notation permits a useful brevity of expression: *"suppose* $p \in \mathbb{R}^n - \{\underline{0}\}$*"* means the same thing as *"suppose p is a point in $\mathbb{R}^n$ that is not $\underline{0}$"*.

1.4. Adding points in $\mathbb{R}^n$. We can add points in $\mathbb{R}^n$. For example, in $\mathbb{R}^4$, $(1,2,3,4)+(6,4,2,0)=(7,6,5,4)$. The origin is the unique point with the property that $\underline{0}+p=p$ for all points p in $\mathbb{R}^n$. For that reason we also call $\underline{0}$ zero.

We can also subtract: for example, $(6,4,2,0)-(1,2,3,4)=(5,2,-1,-4)$.

We can not add a point in $\mathbb{R}^4$ to a point in $\mathbb{R}^5$. More generally, if $m \neq n$, we can't add a point in $\mathbb{R}^m$ to a point in $\mathbb{R}^n$.

1.5. Multiplying a point in $\mathbb{R}^n$ by a number. First, some examples. Consider the point $p=(1,1,2,3)$ in $\mathbb{R}^4$. Then $2p=(2,2,4,6)$, $5p=(5,5,10,15)$, $-3p=(-3,-3,-6,-9)$; more generally, if t is any real number $tp=(t,t,2t,3t)$. In full generality, if λ is a real number and $p=(a_1,\ldots,a_n)$ is a point in $\mathbb{R}^n$, λp denotes the point $(\lambda a_1,\ldots,\lambda a_n)$; thus, the coordinates of λp are obtained by multiplying each coordinate of p by λ. We call λp a multiple of p.

1.6. Lines. We will now define what we mean by the word *line*. If p is a point in $\mathbb{R}^n$ that is not the origin, the line through the origin in the direction p is the set of all multiples of p. Formally, if we write $\mathbb{R}p$ to denote that line,[1]

$$\mathbb{R}p = \{\lambda p \mid \lambda \in \mathbb{R}\}.$$

If q is another point in $\mathbb{R}^n$, the line through q in the direction p is

$$\{q+\lambda p \mid \lambda \in \mathbb{R}\};$$

we often denote this line by $q+\mathbb{R}p$.

When we speak of a line in $\mathbb{R}^n$ we mean a subset of $\mathbb{R}^n$ of the form $q+\mathbb{R}p$. Thus, if I say L is a line in $\mathbb{R}^n$ I mean there is a point $p \in \mathbb{R}^n - \{\underline{0}\}$ and a point $q \in \mathbb{R}^n$ such that $L=q+\mathbb{R}p$. The p and q are not uniquely determined by L.

PROPOSITION 1.1. *The lines $L=q+\mathbb{R}p$ and $L'=q'+\mathbb{R}p'$ are the same if and only if p and p' are multiples of each other and $q-q'$ lies on the line $\mathbb{R}p$; i.e., if and only if $\mathbb{R}p=\mathbb{R}p'$ and $q-q' \in \mathbb{R}p$.*

Proof.[2] ($\Rightarrow$) Suppose the lines are the same, i.e., $L=L'$. Since q' is on the line L' it is equal to $q+\alpha p$ for some $\alpha \in \mathbb{R}$. Since q is on L, $q=q'+\beta p'$ for

[1]I like the notation $\mathbb{R}p$ for the set of all multiples of p because it is similar to the notation $2p$: when x and y are numbers we denote their product by xy, the juxtaposition of x and y. So $\mathbb{R}p$ consists of all products λp where λ ranges over the set of all real numbers.

[2]To show two sets X and X' are the same one must show that every element of X is in X', which is written as $X \subseteq X'$, and that every element of X' is in X.

To prove an "if and only if" statement one must prove each statement implies the other; i.e., the statement "A if and only if B" is true if the truth of A implies the truth of B *and* the truth of B implies the truth of A. Most of the time, when I prove a result of the form "A if and only if B" I will break the proof into two parts: I will begin the proof that A implies B by writing the symbol ($\Rightarrow$) and will begin the proof that B implies A by writing the symbol ($\Leftarrow$)

some $\beta \in \mathbb{R}$. Hence $q - q' = -\alpha p = \beta p'$. In particular, $q - q' \in \mathbb{R}p$. There are now two cases.

Suppose $q \neq q'$. Then α and β are non-zero so p and p' are multiples of each other whence $\mathbb{R}p' = \mathbb{R}p$.

Suppose $q = q'$. Since $q+p \in q+\mathbb{R}p = q'+\mathbb{R}p' = q+\mathbb{R}p'$, $q+p = q+\lambda p'$ for some $\lambda \in \mathbb{R}$. Thus $p = \lambda p'$. Likewise, $q + p' \in q + \mathbb{R}p' = q + \mathbb{R}p$ so $q + p' = q + \mu p$ for some $\mu \in \mathbb{R}$. Thus $p' = \mu p$. We have shown that p and p' are multiples of each other so $\mathbb{R}p = \mathbb{R}p'$.

($\Leftarrow$) Suppose $q - q' \in \mathbb{R}p$ and $\mathbb{R}p = \mathbb{R}p'$. Then $q - q' = \alpha p$ for some $\alpha \in \mathbb{R}$ and $p = \beta p'$ for some non-zero $\beta \in \mathbb{R}$.

If $\lambda \in \mathbb{R}$, then

$$q + \lambda p \;=\; q' + \alpha p + \lambda p \;=\; q' + (\alpha + \lambda)\beta p'$$

which is in $q' + \mathbb{R}p'$; thus $q + \mathbb{R}p \subseteq q' + \mathbb{R}p'$.

Similarly, if $\mu \in \mathbb{R}$, then

$$q' + \mu p' \;=\; q - \alpha p + \mu\beta^{-1}p \;==\; q + (\mu\beta^{-1} - \alpha)p$$

which is in $q + \mathbb{R}p$; thus $q' + \mathbb{R}p' \subseteq q + \mathbb{R}p$.

This completes the proof that $q' + \mathbb{R}p' = q + \mathbb{R}p$ if $q - q' \in \mathbb{R}p$ and $\mathbb{R}p = \mathbb{R}p'$. □

1.7. Fear and loathing. I know most of you are pretty worried about this mysterious thing called $\mathbb{R}^n$. What does it look like? What properties does it have? How can I work with it if I can't picture it? What the heck does he mean when he talks about points and lines in $\mathbb{R}^n$?

Although we can't picture $\mathbb{R}^n$ we can ask questions about it.

This is an important point. Prior to 1800 or so, mathematicians and scientists only asked questions about things they could "see" or "touch". For example, $\mathbb{R}^4$ wasn't really considered in a serious way until general relativity tied together space and time. Going further back, there was a time when negative numbers were considered absurd. Indeed, there still exist primitive cultures that have no concept of negative numbers. If you tried to introduce them to negative numbers they would think you were some kind of nut. Imaginary numbers were called that because they weren't really numbers. Even when they held that status there were a few brave souls who calculated with them by following the rules of arithmetic that applied to *real* numbers.

Because we have a *definition* of $\mathbb{R}^n$ we can grapple with it, explore it, and ask and answer questions about it. That is what we have been doing in the last few sections. In olden days, mathematicians rarely defined things. Because the things they studied were "real" it was "obvious" what the words meant. The great counterexample to this statement is Euclid's books on geometry. Euclid took care to define everything carefully and built geometry on that rock. As mathematics became increasingly sophisticated the need for precise definitions became more apparent. We now live in a sophisticated mathematical world where *everything* is defined.

So, take a deep breath, gather your courage, and plunge into the bracing waters. I will be there to help you if you start sinking. But I can't be everywhere at once, and I won't always recognize whether you are waving or drowning. Shout "help" if you are sinking. I'm not telepathic.

1.8. Basic properties of $\mathbb{R}^n$. Here are some things we will prove:

(1) If p and q are different points in $\mathbb{R}^n$ there is one, and only one, line through p and q. We denote it by $\overline{pq}$.
(2) If L is a line through the origin in $\mathbb{R}^n$, and q and q' are points in $\mathbb{R}^n$, then either $q + L = q' + L$ or $(q + L) \cap (q' + L) = \varnothing$.
(3) If L is a line through the origin in $\mathbb{R}^n$, and q and q' are points in $\mathbb{R}^n$, then $q + L = q' + L$ if and only if $q - q' \in L$.
(4) If p and q are different points in $\mathbb{R}^n$, then $\overline{pq}$ is the line through p in the direction $q - p$.
(5) If L and L' are lines in $\mathbb{R}^n$ such that $L \subseteq L'$, then $L = L'$. This is a consequence of (2).

If L is a line through the origin in $\mathbb{R}^n$, and q and q' are points in $\mathbb{R}^n$, we say that the lines $q + L$ and $q' + L$ are parallel.

Don't just accept these as facts to be memorized. Learning is more than knowing—learning involves understanding. To understand why the above facts are true you will need to look at how they are proved.

Proposition 1.2. *If p and q are different points in $\mathbb{R}^n$ there is one, and only one, line through p and q, namely the line through p in the direction $q - p$.*

Proof. The line through p in the direction $q - p$ is $p + \mathbb{R}(q - p)$. The line $p + \mathbb{R}(q - p)$ contains p because $p = p + 0 \times (q - p)$. It also contains q because $q = p + 1 \times (q - p)$. We have shown that the line through p in the direction $q - p$ passes through p and q.

It remains to show that this is the *only* line that passes through both p and q. To that end, let L be any line in $\mathbb{R}^n$ that passes though p and q. We will use Proposition 1.1 to show that L is equal to $p + \mathbb{R}(q - p)$.

By our definition of the word line, $L = q' + \mathbb{R}p'$ for some points $q' \in \mathbb{R}$ and $p' \in \mathbb{R} - \{\underline{0}\}$. By Proposition 1.1, $q' + \mathbb{R}p'$ is equal to $p + \mathbb{R}(q - p)$ if $\mathbb{R}p' = \mathbb{R}(q - p)$ and $q' - p \in \mathbb{R}p'$.

We will now show that $\mathbb{R}p' = \mathbb{R}(q - p)$ and $q' - p \in \mathbb{R}p'$.

Since $p \in L$ and $q \in L$, there are numbers λ and μ such that $p = q' + \lambda p'$, which implies that $q' - p \in \mathbb{R}p'$, and $q = q' + \mu p'$. Thus $p - q = q' + \lambda p - q' - \mu q' = (\lambda - \mu)q'$. Because $p \neq q$, $p - q \neq \underline{0}$; i.e., $(\lambda - \mu)p' \neq \underline{0}$. Hence $\lambda - \mu \neq 0$. Therefore $p' = (\lambda - \mu)^{-1}(p - q)$. It follows that every multiple of p' is a multiple of $p - q$ and every multiple of $p - q$ is a multiple of p'. Thus $\mathbb{R}p' = \mathbb{R}(q - p)$. We already observed that $q' - p \in \mathbb{R}p'$ so Proposition 1.1 tells us that $q' + \mathbb{R}p' = p + \mathbb{R}(q - p)$, i.e., $L = p + \mathbb{R}(q - p)$. $\square$

1.8.1. *Notation.* We will write $\overline{pq}$ for the unique line in $\mathbb{R}^n$ that passes through the points p and q (when $p \neq q$). Proposition 1.2 tells us that

$$\overline{pq} = p + \mathbb{R}(q-p).$$

Proposition 1.1 tells us that $\overline{pq}$ has infinitely many other similar descriptions. For example, $\overline{pq} = q + \mathbb{R}(p-q)$ and $\overline{pq} = q + \mathbb{R}(q-p)$.

1.8.2. Although we can't picture $\mathbb{R}^8$ we can ask questions about it. For example, does the point (1,1,1,1,1,1,1,1) lie on the line through the points (8,7,6,5,4,3,2,1) and (1,2,3,4,5,6,7,8)? Why? If you can answer this you understand what is going on. If you can't you don't, and should ask a question.

1.9. Parametric description of lines. You already know that lines in $\mathbb{R}^3$ can be described by a pair of equations or parametrically. For example, the line given by the equations

$$\begin{cases} x+y+z &= 4 \\ x+3y+2z &= 9 \end{cases} \tag{1-1}$$

is the set of points of the form $(t, 1+t, 3-2t)$ as t ranges over all real numbers; in set-theoretic notation, the line is

$$\{(t, 1+t, 3-2t) \mid t \in \mathbb{R}\}; \tag{1-2}$$

we call t a *parameter*; we might say that t parametrizes the line or that the line is parametrized by t.

The next result shows that every line in $\mathbb{R}^n$ can be described parametrically.

PROPOSITION 1.3. *If p and q are distinct points in $\mathbb{R}^n$, then*

$$\overline{pq} \;=\; \{tp + (1-t)q \mid t \in \mathbb{R}\}. \tag{1-3}$$

Proof. We must show that the sets $\overline{pq}$ and $\{tp + (1-t)q \mid t \in \mathbb{R}\}$ are the same. We do this by showing each set contains the other one.

Let p' be a point on $\overline{pq}$. Since $\overline{pq} = p + \mathbb{R}(q-p)$, $p' = p + \lambda(q-p)$ for some $\lambda \in \mathbb{R}$. Thus, if $t = 1-\lambda$, then

$$p' \;=\; (1-\lambda)p + \lambda q \;=\; tp + (1-t)q.$$

Therefore $\overline{pq} \;\subseteq\; \{tp + (1-t)q \mid t \in \mathbb{R}\}$. If t is any number, then

$$tp + (1-t)q \;=\; q + t(p-q) \;\in\; q + \mathbb{R}(p-q) \;=\; \overline{pq}$$

so $\{tp + (1-t)q \mid t \in \mathbb{R}\} \;\subseteq\; \overline{pq}$. Thus, $\overline{pq} = \{tp + (1-t)q \mid t \in \mathbb{R}\}$. $\square$

If you think of t as denoting *time*, then the parametrization in (1-3) can be thought of as giving the position of a moving point at time t; for example, at $t = 0$ the moving point is at q and at time $t = 1$, the moving point is at p; at time $t = \frac{1}{2}$ the moving point is exactly half-way between p and q. This perspective should help you answer the question in §1.8.2.

1.9.1. *Don't forget this remark.* One of the key ideas in understanding systems of linear equations is moving back and forth between the parametric description of linear subsets of $\mathbb{R}^n$ and the description of those linear subsets as solution sets to systems of linear equations. For example, (1-2) is a parametric description of the set of solutions to the system (1-1) of two linear equations in the unknowns x, y, and z. In other words, every solution to (1-1) is obtained by choosing a number t and then taking $x = t$, $y = 1+t$, and $z = 3 - 2t$.

1.9.2. Each line L in $\mathbb{R}^n$ has infinitely many parametric descriptions.

1.9.3. *Parametric descriptions of higher dimensional linear subsets of* $\mathbb{R}^n$*.*

1.10. Linear subsets of $\mathbb{R}^n$. Let L be a subset of $\mathbb{R}^n$. We say that L is linear if

(1) it is a point or
(2) whenever p and q are different points on L every point on the line $\overline{pq}$ lies on L.

1.11. What is a plane? Actually, it would be better if you thought about this question. How would you define a plane in $\mathbb{R}^n$? Look at the definition of a line for inspiration. We defined a line parametrically, not by a collection of equations. Did we really need to define a line in two steps, i.e., first defining a line through the origin, then defining a general line?

1.12. Hyperplanes. The dot product of two points $\underline{u} = (u_1, \dots, u_n)$ and $\underline{v} = (v_1, \dots, v_n)$ in $\mathbb{R}^n$ is the number

$$\underline{u} \cdot \underline{v} = u_1 v_1 + \cdots + u_n v_n.$$

Notice that $\underline{u} \cdot \underline{v} = \underline{v} \cdot \underline{u}$. If $\underline{u}$ and $\underline{v}$ are non-zero and $\underline{u} \cdot \underline{v} = 0$ we say $\underline{u}$ and $\underline{v}$ are orthogonal. If n is 2 or 3, the condition that $\underline{u} \cdot \underline{v} = 0$ is equivalent to the condition that the line $\overline{0\underline{u}}$ is perpendicular to the line $\overline{0\underline{v}}$.

Let $\underline{u}$ be a non-zero point in $\mathbb{R}^n$ and c any number. The set

$$H := \{\underline{v} \in \mathbb{R}^n \mid \underline{u} \cdot \underline{v} = c\}$$

is called a hyperplane in $\mathbb{R}^n$.

PROPOSITION 1.4. *If p and q are different points on a hyperplane H, then all the points on the line $\overline{pq}$ lie on H.*

Proof. Since H is a hyperplane there is a point $\underline{u} \in \mathbb{R}^n - \{\underline{0}\}$ and a number c such that $H = \{\underline{v} \in \mathbb{R}^n \mid \underline{u} \cdot \underline{v} = c\}$.

$\square$

1.13. Solutions to systems of equations: an example. A system of equations is just a collection of equations. For example, taken together,

$$x^2 + y^2 = z^2 \qquad \text{and} \qquad x + y + z = 1 \tag{1-4}$$

form a system of two equations. We call x, y, and z, *unknowns*. A solution to the system (1-4) consists of three numbers a, b, c such that $a^2 + b^2 = c^2$ *and* $a+b+c = 1$. Such a solution corresponds to the point (a, b, c) in 3-space, $\mathbb{R}^3$. For example, $\left(0, \frac{1}{2}, \frac{1}{2}\right)$ is a solution to this system of equations because

$$(0)^2 + \left(\frac{1}{2}\right)^2 = \left(\frac{1}{2}\right)^2 \qquad \text{and} \qquad 0 + \frac{1}{2} + \frac{1}{2} = 1.$$

Similarly, $\left(\frac{1}{4}, \frac{1}{3}, \frac{5}{12}\right)$ is a solution to the system of equations because

$$\left(\frac{1}{4}\right)^2 + \left(\frac{1}{3}\right)^2 = \left(\frac{5}{12}\right)^2 \qquad \text{and} \qquad \frac{1}{4} + \frac{1}{3} + \frac{5}{12} = 1.$$

Thus, we think of solutions to the system (1-4) as points in $\mathbb{R}^3$. These points form a geometric object. We use our visual sense to perceive them, and our visual sense organize those individual points into a single organized geometric object.

If you are really interested in math you might try finding all solutions to the system (1-4). If not all, several. How did I find the second solution? Can you find another solution?

1.14. Solutions to systems of equations. A solution to a system of equations in n unknowns $x_1, \ldots, x_n$ is a set of numbers $s_1, \ldots, s_n$ such that every equation is a true equality when each x_i is replaced by the corresponding number s_i. This is the famous "plugging in" procedure. We will think of $s_1, \ldots, s_n$ as the coordinates of a point in n-space, $\mathbb{R}^n$. Thus, each solution is a point $p = (s_1, \ldots, s_n)$ in $\mathbb{R}^n$.

1.15. Systems of linear equations. The distinguishing feature of a system of *linear* equations is that

> if p and q are different solutions to a system of linear equations, then every point on the line through p and q is a solution to the system.

It is this linearity feature that gives rise to the terminology *linear algebra*.

It is convenient to write $\overline{pq}$ for the line through p and q.

Suppose p, q, and r, are solutions to a system of linear equations and r is not on the line through p and q. Then every point on the three lines $\overline{pq}$, $\overline{pr}$, and $\overline{qr}$, is a solution to the system. Now take any point p' on $\overline{pq}$ and any point q' on $\overline{pr}$; since p' and q' are solutions to the linear system so is every point on the line $\overline{p'q'}$. Repeating this operation we can draw more and more lines. You should be able to convince yourself that *all* the lines we obtain in this way eventually fill up a plane, the plane in $\mathbb{R}^n$ that contains the points p, q, and r. We denote that plane by $\overline{pqr}$.

1.16. Grumbling and preaching. It has become popular over the last two or three decades to speak of "linear thinking" and "non-linear thinking". This is a fine example of the way in which scientific terms are hijacked by people who have no idea what they mean. To those people, "linear thinking" is not as "good" as "non-linear thinking". "Linear thinking" is considered rigid, not flexible, something "creative/imaginative" people don't engage in. This is utter nonsense promulgated by ignorant, pompous, people. (Yes, I'm pompous too but perhaps not so ignorant.)

The recognition of linearity in mathematics and the subsequent development of linear algebra has produced methods of tremendous power and extraordinarily wide applicability. Indeed, the modern world could not function as it does if it did not make use of linear algebra and linear geometry millions of times every second. I mean that literally. No exaggeration. Linear algebra is used millions of times every second, in every corner of the globe, to ensure that (some of) our society functions smoothly.

The methods that have been developed to address problems in linear algebra are so effective that it is often beneficial to approximate a non-linear problem (and here I use the word *non-linear* in a precise scientific sense) by a linear problem.

2. Lines in $\mathbb{R}^2$

2.1. An ordered pair of real numbers consists of two real numbers where their order matters. For example, $(0,0)$, $(0,1)$, $(1,1)$, $(-2,7)$, and $(-3,-5)$, are ordered pairs of real numbers, and they differ from the ordered pairs $(1,0)$, $(7,-2)$, and $(-5,-3)$.

$\mathbb{R}^2$ denotes the set of ordered pairs of real numbers. For example, $(0,0)$, $(0,1)$, $(1,1)$, $(-2,7)$, and $(-3,-5)$, are points in $\mathbb{R}^2$. We use the word *ordered* because $(1,2)$ and $(2,1)$ are different points of $\mathbb{R}^2$. A formal definition is

$$\mathbb{R}^2 := \{(a,b) \mid a,b \in \mathbb{R}\}.$$

At high school you learned about x- and y-axes and labelled points of in the plane by ordered pairs of real numbers. The point labelled $(3,7)$ is the point obtained by starting at the origin, going 3 units of distance in the x-direction, then 7 units of distance in the y-direction. Thus, we have a geometric view of the algebraically defined object $\mathbb{R}^2$.

Linear algebra involves a constant interplay of algebra and geometry. To master linear algebra one must keep in mind both the algebraic and geometric features. A simple example of this interplay is illustrated by the fact that the unique solution to the pair of equations

$$\begin{aligned} 2x + 3y &= 4 \\ 2x - 3y &= -8 \end{aligned}$$

is the point where the lines $2x + 3y = 4$ and $2x - 3y = -8$ intersect. This pair of equations is a system of two linear equations.

2.2. Notation. If p and q are two different points in the plane $\mathbb{R}^2$ or in 3-space, $\mathbb{R}^3$, we write $\overline{pq}$ for the line through them.

2.3. Set notation. We will use standard set notation throughout this course. You will find it helpful to read something about set notation. Use google.

2.4. Prerequisites for every linear algebra course. You *must* be able to do the following things:

- Find the slope of the line through two given points in $\mathbb{R}^2$.
- Find the equation of the line through two points in $\mathbb{R}^2$.
- Give a parametric form for a line that is given in the form $ax+by=c$. There are infinitely many different parametric forms for a given line. For example, the line $x=y$ is the line consisting of all points (t,t) as t ranges over $\mathbb{R}$, the set of real numbers. The same line is given by the parametrization $(1+2t, 1+2t)$, $t \in \mathbb{R}$. And so on.
- Give a parametric form for the line through two given points. If $p=(a,b)$ and $q=(c,d)$ are two different points in the plane the set of points $t(a,b)+(1-t)(c,d)$, or, equivalently, $tp+(1-t)q$, gives all points on $\overline{pq}$ as t ranges over all real numbers. For example, $t=0$ gives the point q, $t=1$ gives the point p, $t=\frac{1}{2}$ gives the point halfway between p and q. One gets all points between p and q by letting t range over the closed interval $[0,1]$. More formally, the set of points between p and q is $\{tp+(1-t)q \mid t \in [0,1]\}$. Similarly, $\overline{pq} = \{tp+(1-t)q \mid t \in \mathbb{R}\}$.

  Notice that $t(a,b)+(1-t)(c,d) = (ta+(1-t)c, tb+(1-t)d)$.
- Decide whether two lines are parallel.
- Decide whether two lines are perpendicular.
- Given a line L and a point not on L, find the line parallel to L that passes through the given point.
- Given a line L and a point not on L, find the line perpendicular to L that passes through the given point.
- Find the point at which two lines intersect if such a point exists.

PROPOSITION 2.1. *Let $p=(a,b)$ and $q=(c,d)$ be two different points in the plane, $\mathbb{R}^2$. The set of points*

$$\{tp+(1-t)q \mid t \in \mathbb{R}\}$$

is exactly the set of points on the line through p and q.

Proof. The line given by the equation

$$(c-a)(y-b) = (d-b)(x-a) \tag{2-1}$$

passes through p because when we plug in a for x and b for y (2-1) <u>*is*</u> an equality, namely $(c-a)(b-b) = (d-b)(a-a)$. The line given by equation (2-1) also passes through q because when we plug in c for x and d for y we get a true equality, namely $(c-a)(d-b) = (d-b)(c-a)$. Thus, the line given by equation (2-1) is the line through p and q which we denote by $\overline{pq}$.

Let's write L for the set of points $\{tp + (1-t)q \mid t \in \mathbb{R}\}$. Less elegantly, but more explicitly,

$$L = \Big\{ \big(ta + (1-t)c,\, tb + (1-t)d\big) \;\Big|\; t \in \mathbb{R} \Big\}.$$

The proposition claims that $L = \overline{pq}$. To prove this we must show that every point in L belongs to $\overline{pq}$ and every point on $\overline{pq}$ belongs to L.

We first show that $L \subseteq \overline{pq}$, i.e., every point in L belongs to $\overline{pq}$. A point in L has coordinates $\big(ta + (1-t)c,\, tb + (1-t)d\big)$. When we plug these coordinates into (2-1) we obtain

$$(c-a)(tb + (1-t)d - b) = (d-b)(ta + (1-t)c - a),$$

i.e., $(c-a)(1-t)(d-b) = (d-b)(1-t)(c-a)$. Since this really *is* an equality we have shown that $\big(ta+(1-t)c,\, tb+(1-t)d\big)$ lies on $\overline{pq}$. Therefore $L \subseteq \overline{pq}$.

To prove the opposite inclusion, take a point (x, y) that lies on $\overline{pq}$; we will show that (x, y) is in L. Do do that we must show there is a number t such that $(x, y) = (ta + (1-t)c,\, tb + (1-t)d)$. Because (x, y) lies on $\overline{pq}$, $(c-a)(y-b) = (d-b)(x-a)$. This implies that

$$\frac{x-c}{a-c} = \frac{y-d}{b-d}.$$

Let's call this number t. If $a = c$ we define t to be the number $(y-d)/(b-d)$; if $b = d$, we define t to be the number $(x-c)/(a-c)$; we can't have $a = c$ and $b = d$ because then $(a, b) = (c, d)$ which violates the hypothesis that (a, b) and (c, d) are different points.

In any case, we now have $x - c = t(a-c)$ and $y - d = t(b-d)$. We can rewrite these as $x = ta + (1-t)c$ and $y = tb + (1-t)d$. Thus $(x, y) = (ta + (1-t)c,\, tb + (1-t)d)$, i.e., (x, y) belongs to the set L. This completes the proof that $L \subseteq \overline{pq}$. $\square$

2.5. Remarks on the previous proof. You might ask *"How did you know that (2-1) is the line through (a, b) and (c, d)?*

Draw three points (a, b), (c, d), and (x, y), on a piece of paper. Draw the line segment from (a, b) to (c, d), and the line segment from (c, d) to (x, y). Can you see, or convince yourself, that (x, y) lies on the line through (a, b) and (c, d) if and only if those two line segments have the same slope? I hope so because that is the key idea behind the equation (2-1). Let me explain. The slopes of the two lines are

$$\frac{d-b}{c-a} \qquad \text{and} \qquad \frac{y-b}{x-a}.$$

Thus, (x, y) lies on the line through (a, b) and (c, d) if and only if

$$\frac{d-b}{c-a} = \frac{y-b}{x-a}.$$

It is possible that a might equal c in which case the expression on the left of the previous equation makes no sense. To avoid that I cross multiply and rewrite the required equality as $(d-b)(x-a) = (c-a)(y-b)$.

Of course, there are other reasonable ways to write the equation for the line $\overline{pq}$ but I like mine because it seems elegant and fits in nicely with the geometry of the situation, i.e., the statements I made about slopes.

2.6. About proofs. A proof is a narrative argument intended to convince other people of the truth of a statement.

By *narrative* I mean that the argument consists of sentences and paragraphs. The sentences should be grammatically correct and easy to understand. Those sentences will contain words and mathematical symbols. Not only must the words obey the rules of grammar, so too must the symbols. Thus, there are two kinds of grammatical rules: those that govern the English language and those that govern "mathematical phrases".

By saying *other people* I want to emphasize that you are writing for someone else, the reader. Make it easy for the reader. It is not enough that you understand what your sentences say. Others must understand them too. Indeed, the quality of your proof is measured by the effect it has on other people. If your proof does not convince other people you have done a poor job.

If your proof does not convince others it might be that your "proof" is incorrect. You might have fooled yourself. If your proof does not convince others it might be because your argument is too long and convoluted. In that case, you should re-examine your proof and try to make it simpler. Are parts of your narrative argument unnecessary? Have you said the same thing more than once? Have you used words or phrases that add nothing to your argument? Are your sentences too long? Is it possible to use shorter sentences. Short sentences are easier to understand. Your argument might fail to convince others because it is too short. Is some essential part of the argument missing? Is it clear how each statement follows from the previous ones? Have you used an undefined symbol, word, or phrase?

When I figure out how to prove something I usually rewrite the proof many times trying to make it as simple and clear as possible. Once I have convinced myself that my argument works I start a new job, that of polishing and refining the argument so it will convince others.

Even if you follow the rules of grammar you might write nonsense. A famous example is *"Red dreams sleep furiously"*. For some mathematical nonsense, consider the sentence *"The derivative of a triangle is perpendicular to its area"*.

3. Points, lines, and planes in $\mathbb{R}^3$

3.1. $\mathbb{R}^3$ denotes the set of ordered triples of real numbers. Formally,

$$\mathbb{R}^3 := \{(a,b,c) \mid a,b,c \in \mathbb{R}\}.$$

The corresponding geometric picture is 3-space. Elements of $\mathbb{R}^3$, i.e., ordered triples (a,b,c) label points in 3-space. We call a the x-coordinate of the point $p=(a,b,c)$, b the y-coordinate of p, and c the z-coordinate of p.

3.2. Notation. If p and q are two different points in $\mathbb{R}^3$ we write $\overline{pq}$ for the line through them. If p, q, and r, are three points in $\mathbb{R}^3$ that do not lie on a line, there is a unique plane that contains them. That plane will be labelled $\overline{pqr}$.

3.3. The first difference from $\mathbb{R}^2$ is that a single linear equation, $2x+y-3z=4$ for example, "gives" a plane in $\mathbb{R}^3$. By "gives" I mean the following. Every solution to the equation is an ordered triple of numbers, e.g., $(2,6,2)$ is a solution to the equation $2x+y-3z=4$ and it represents (is the label for) a point in $\mathbb{R}^3$. We say that the point $(2,6,2)$ is a solution to the equation. The collection (formally, the set) of all solutions to $2x+y-3z=4$ forms a plane in $\mathbb{R}^3$.

Two planes in $\mathbb{R}^3$ are said to be parallel if they do not intersect (meet).

3.4. Prerequisites for every linear algebra course. You *must* be able to do the following things:

- Fiind the equation of the plane $\overline{pqr}$ when p, q, and r, are three points in $\mathbb{R}^3$ that do not lie on a line. A relatively easy question of this type is to find the equation for the plane that contains $(0,0,0)$, $(2,3,7)$, and $(3,2,3)$. That equation will be of the form $ax+by+cz=d$ for some real numbers a,b,c,d. Since $(0,0,0)$ lies on the plane, $d=0$. Because $(2,3,7)$ and $(3,2,3)$ lie on the plane $ax+by+cz=0$ the numbers a,b,c must have the property that
$$\begin{aligned} 2a+3b+7c&=0 \qquad \text{and} \\ 3a+2b+3c&=0. \end{aligned}$$
This is a system of 2 linear equations in 3 unknowns. There are many ways you might solve this system but all are essentially the same. The idea is to multiply each equation by some number and add or subtract the two equations to get a simpler equation that a, b, and c, must satisfy.
- Find the equation of the line through two given points.
- Give a parametric form for a line that is given in the form $ax+by=c$. There are infinitely many different parametric forms for a given line. For example, the line $x=y$ is the line consisting of all points (t,t) as t ranges over $\mathbb{R}$, the set of real numbers. The same line is given by the parametrization $(1+2t,1+2t)$, $t\in\mathbb{R}$. And so on.
- Give a parametric form for the line through two given points. If $p=(a,b)$ and $q=(c,d)$ are two different points in the plane the set of points $t(a,b)+(1-t)(c,d)$, or, equivalently, $tp+(1-t)q$, gives all points on $\overline{pq}$ as t ranges over all real numbers. For example, $t=0$ gives the point q, $t=1$ gives the point p, $t=\frac{1}{2}$ gives the point

halfway between p and q. One gets all points between p and q by letting t range over the closed interval $[0,1]$. More formally, the set of points between p and q is $\{tp+(1-t)q \mid t \in [0,1]\}$. Similarly, $\overline{pq} = \{tp+(1-t)q \mid t \in \mathbb{R}\}$.

Notice that $t(a,b)+(1-t)(c,d) = (ta+(1-t)c, tb+(1-t)d)$.

- Decide whether two lines are parallel.
- Decide whether two lines are perpendicular.
- Given a line L and a point not on L, find the line parallel to L that passes through the given point.
- Given a line L and a point not on L, find the line perpendicular to L that passes through the given point.
- Find the point at which two lines intersect if such a point exists.

As t ranges over all real numbers the points $(1,2,3)+t(1,1,1)$ form a line in $\mathbb{R}^3$. The line passes through the point $(1,2,3)$ (just take $t=0$). We sometimes describe this line by saying *"it is the line through* $(1,2,3)$ *in the direction* $(1,1,1)$*."*

4. Higher dimensions

5. Parametric descriptions of lines, planes, etc.

The solutions to the system of equations $x+y-2z=0$ and $2x-y-z=3$ is a line in $\mathbb{R}^3$. Let's call it L. Although these two equations give a complete description of L that description does not make it easy to write down *any* points that lie on L. In a sense it is a useless description of L.

In contrast, it is easy to write down points that lie on the line $(1,2,3)+t(1,1,1)$, $t \in \mathbb{R}$; just choose any real number t and compute. For example, asking $t=-1$, $t=0$, $t=1$, and $t=2$, gives us the points $(0,1,2)$, $(1,2,3)$, $(2,3,4)$, and $(3,4,5)$. In fact, the line in this paragraph *is* the line in the previous paragraph.

Solving a system of linear equations means, roughly, taking a line (usually a higher dimensional linear space) given as in the first paragraph and figuring out how to describe that line by giving a description of it like that in the second paragraph.

5.1. Exercise. Show that the line $(1,2,3)+t(1,1,1)$, $t \in \mathbb{R}$, is the same as the line given by the equations $x+y-2z=0$ and $2x-y-z=3$. (Hint: to show two lines are the same it suffices to show they have two points in common.)

CHAPTER 2

Matrices

You can skip this chapter if you want, start reading at chapter 4, and return to this chapter whenever you need to.

Matrices are an essential part of the language of linear algebra and linear equations. This chapter isolates this part of the language so you can easily refer back to it when you need to.

1. What is a matrix?

1.1. An $m \times n$ matrix (we read this as "an m-by-n matrix") is a rectangular array of mn numbers arranged into m rows and n columns. For example,

$$A := \begin{pmatrix} 1 & 3 & 0 \\ -4 & 5 & 2 \end{pmatrix} \tag{1-1}$$

is a 2×3 matrix. The prefix $m \times n$ is called the size of the matrix.

1.2. We use upper case letters to denote matrices. The numbers in the matrix are called its entries. The entry in row i and column j is called the ij^{th} entry, and if the matrix is denoted by A we often write A_{ij} for its ij^{th} entry. The entries in the matrix A in (1-1) are

$$\begin{aligned} A_{11} &= 1, \quad & A_{12} &= 3, \quad & A_{13} &= 0 \\ A_{21} &= -4, \quad & A_{22} &= 5, \quad & A_{23} &= 2. \end{aligned}$$

In this example, we call 5 the 22-entry; read this as *two-two entry.* Likewise, the 21-entry (two-one entry) is 4.

We sometimes write $A = (a_{ij})$ for the matrix whose ij^{th} entry is a_{ij}. For example, we might write

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}.$$

Notice that a_{ij} is the entry in row i and column j

1.3. Equality of matrices. Two matrices A and B are equal if and only if they have the same size and $A_{ij} = B_{ij}$ for all i and j.

1.4. Square matrices. An $n \times n$ matrix is called a square matrix. For example,

$$A = \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix} \tag{1-2}$$

is a 2×2 square matrix.

2. A warning about our use of the word vector

In the past you have probably used the word vector to mean something with magnitude and direction. **That is not the way the word vector will be used in this course.**

Later we will define things called **vector spaces**. The familiar spaces $\mathbb{R}^2$ and $\mathbb{R}^3$ are vector spaces. But there are many other vector spaces. For example, the set of all polynomials in one variable is a vector space. The set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$ is a vector space. The set of all continuous functions $f : [0,1] \to \mathbb{R}$ is a vector space.The set of all polynomials of degree ≤ 56 fis a vector space; there is nothing special about 56. All vector spaces have various common properties so rather than proving such a property for this vector space, then that one, then another one, we develop a general theory of vector spaces proving results about all vector spaces at once.

That is what abstraction is about: by throwing away the inessential data and keeping the essential data we are able to prove results that apply to many different things at once.

When talking about vector spaces we need a name for the elements in them. The word used for an element in a vector space is **vector**. However, when we look at a particular vector space the word *vector* might be confusing. For example, the set of all polynomials is a vector space but rather than calling the elements in it vectors we call them *polynomials*.

One might argue that we should not have hijacked the word vector—I tend to agree with you, but the naming was done long ago and is now part of the language of linear algebra. We are stuck with it. Sometimes I will use the word **point** to refer to an element in a vector space. For example, it is common to call elements of the plane $\mathbb{R}^2$ *points*. You probably are used to calling elements of $\mathbb{R}^3$ *points*.

Bottom line: in this course, when you here the word *vector* think of a point or whatever is appropriate to the situation. For example, the row and column vectors we are about to define are just matrices of a particular kind. It is not helpful to think of row and column vectors as having magnitude and direction.

3. Row and column vectors = points with coordinates

3.1. Matrices having just one row or column are of particular importance and are often called vectors.

A matrix having a single row is called a row matrix or a row vector.

A matrix having a single column is called a <u>column matrix</u> or a <u>column vector</u>.

For example, the 1×4 matrix $(1\ 2\ 3\ 4)$ is a row vector, and the 4×1 matrix

$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$$

is a column vector.

In parts of this course it is better to call row and column vectors **points** and think of the entries in them as the coordinates of the points. For example, think of (1,2,3,4) and

$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$$

as points having 4 coordinates. Because it has 4 coordinates such a point belongs to **4-space** which we will denote by $\mathbb{R}^4$.

At high school you met points with 2 coordinates, points in the plane, $\mathbb{R}^2$. Either there, or at college, you met points in 3-space,$\mathbb{R}^3$, often labelled (x, y, z).

Points with n coordinates, $(a_1, \ldots, a_n)$ for example, belong to n**-space** which we denote by $\mathbb{R}^n$. We call the number n in the notation $\mathbb{R}^n$ the **dimension** of the space. Later we will give an abstract and formal definition of dimension but for now your intuition should suffice.

3.2. Underlining row and column vectors. Matrices are usually denoted by upper case letters but this convention is usually violated for row and column vectors. We usually denote a row or column vector by a lower case letter *that is underlined*. The underlining is done to avoid confusion between a lower case letters denoting numbers and lower case letters denoting row or column vectors. For example, I will write

$$\underline{u} = (1\ 2\ 3\ 4) \qquad \text{and} \qquad \underline{v} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}.$$

Many students ask me whether they can write $\vec{v}$ to denote a vector. My answer is "NO". It is best to avoid that notation because that arrow suggests *direction* and as I said in §2 we are not using the word vector to mean things with magnitude and direction. Also it takes more work to write $\vec{v}$ than $\underline{v}$.

Warning. .

4. Matrix arithmetic: addition and subtraction

4.1. We *add* two matrices of the same size by adding the entries of one to those of the other, e.g.,

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} + \begin{pmatrix} -1 & 2 & 0 \\ 3 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 4 & 3 \\ 7 & 3 & 7 \end{pmatrix}.$$

The result of adding two matrices is called their sum. Subtraction is defined in a similar way, e.g.,

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} - \begin{pmatrix} -1 & 2 & 0 \\ 3 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 3 \\ 1 & 7 & 5 \end{pmatrix}.$$

Abstractly, if (a_{ij}) and (b_{ij}) are matrices of the same size, then

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \qquad \text{and} \qquad (a_{ij}) - (b_{ij}) = (a_{ij} - b_{ij}).$$

4.2. Matrices of different sizes can not be added. The sum of two matrices of different sizes is not defined. Whenever we write $A + B$ we tacitly assume that A and B have the same size.

4.3. Addition of matrices is *commutative*:

$$A + B = B + A.$$

The commutativity is a simple consequence of the fact that addition of numbers is commutative.

4.4. Addition of matrices, like addition of numbers, is *associative*:

$$(A + B) + C = A + (B + C).$$

This allows us to dispense with the parentheses: the expression $A + B + C$ is unambiguous—you get the same answer whether you first add A and B, then C, or first add B and C, then A. Even more, because $+$ is commutative you also get the same answer if you first add A and C, then B.

5. The zero matrix and the negative of a matrix

The zero matrix is the matrix consisting entirely of zeroes. Of course, we shouldn't really say *the* zero matrix because there is one zero matrix of size $m \times n$ for each choice of m and n. We denote the zero matrix of any size by 0. Although the symbol 0 now has many meanings it should be clear from the context which zero matrix is meant.

The zero matrix behaves like the number 0:

(1) $A + 0 = A = 0 + A$ for all matrices A, and
(2) given a matrix A, there is a unique matrix A' such that $A + A' = 0$.

The matrix A' in (2) is denoted by $-A$ and its entries are the negatives of the entries in A.

After we define multiplication of matrices we will see that the zero matrix shares another important property with the number zero: the product of a zero matrix with any other matrix is zero.

6. Matrix arithmetic: multiplication

6.1. Let A be an $m \times n$ matrix and B a $p \times q$ matrix. The product AB is *only defined when $n = p$* and in that case the product is an $m \times q$ matrix. For example, if A is a 2×3 matrix and B a 3×4 matrix we can form the product AB but there is no product BA! In other words,

> the product AB can only be formed if the number of columns in A is equal to the number of rows in B.

The rule for multiplication will strike you as complicated and arbitrary at first though you will later understand why it is natural. Let A be an $m \times n$ matrix and B an $n \times q$ matrix. Before being precise, let me say that the

> the ij^{th} entry of AB is obtained by multiplying the i^{th} row of A by the j^{th} column of B.

What we mean by this can be seen by reading the next example carefully. The product AB of the matrices

$$A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 5 & 4 & 3 \\ 2 & 1 & 2 \end{pmatrix}$$

is the 2×3 matrix whose

$$\text{11-entry is (row 1)}\times\text{(column 1)} = (1\ 2) \times \begin{pmatrix} 5 \\ 2 \end{pmatrix} = 1 \times 5 + 2 \times 2 = 9$$

$$\text{12-entry is (row 1)}\times\text{(column 2)} = (1\ 2) \times \begin{pmatrix} 4 \\ 1 \end{pmatrix} = 1 \times 4 + 2 \times 1 = 6$$

$$\text{13-entry is (row 1)}\times\text{(column 3)} = (1\ 2) \times \begin{pmatrix} 3 \\ 2 \end{pmatrix} = 1 \times 3 + 2 \times 2 = 7$$

$$\text{21-entry is (row 2)}\times\text{(column 1)} = (0\ -1) \times \begin{pmatrix} 5 \\ 2 \end{pmatrix} = 0 \times 5 - 1 \times 2 = -2$$

$$\text{22-entry is (row 2)}\times\text{(column 2)} = (0\ -1) \times \begin{pmatrix} 4 \\ 1 \end{pmatrix} = 0 \times 4 - 1 \times 1 = -1$$

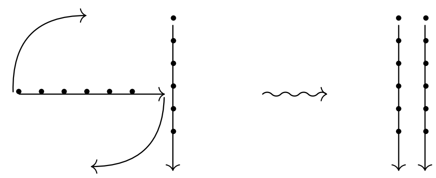
$$\text{23-entry is (row 2)}\times\text{(column 3)} = (0\ -1) \times \begin{pmatrix} 3 \\ 2 \end{pmatrix} = 0 \times 3 - 1 \times 2 = -2$$

In short,

$$AB = \begin{pmatrix} 9 & 6 & 7 \\ -2 & -1 & -2 \end{pmatrix}.$$

The product BA does not make sense in this case.

My own mental picture for remembering how to multiply matrices is encapsulated in the diagram



Then one computes the dot product.

6.2. Powers of a matrix. A square matrix, i.e., an $n \times n$ matrix, has the same number of rows as columns so we can multiply it by itself. We write A^2 rather that AA for the product. For example, if

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{then } A^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},\ A^3 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix},\ A^4 = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}.$$

Please check those calculations to test your understanding.

6.3. The formal definition of multiplication. Let A be an $m \times n$ matrix and B an $n \times q$ matrix. Then AB is the $m \times q$ matrix whose ij^{th} entry is

$$(AB)_{ij} = \sum_{t=1}^{n} A_{it} B_{tj}. \tag{6-1}$$

Do you understand this formula? Is it compatible with what you have understood above? If A is the 3×4 matrix with $A_{ij} = |4 - i - j|$ and B is the 4×3 matrix with $B_{ij} = ij - 4$, what is $(AB)_{23}$? If you can't answer this question there is something about the definition of multiplication or something about the notation I am using that you do not understand. Do yourself and others a favor by asking a question in class.

6.4. The zero matrix. For every m and n there is an $m \times n$ matrix we call zero. It is the $m \times n$ matrix with all its entries equal to 0. The product of any matrix with the zero matrix is equal to zero. Why?

6.5. The identity matrix. For every n there is an $n \times n$ matrix we call the $n \times n$ identity matrix. We often denote it by I_n, or just I if the n is clear from the context. It is the matrix with entries

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

In other words every entry on the NW-SE diagonal is 1 and all other entries are 0. For example, the 4×4 identity matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The key property of the $n \times n$ identity matrix I is that if A is any $m \times n$ matrix, then $AI = A$ and, if B is any $n \times p$ matrix $IB = B$. You should check this with a couple of examples to convince yourself it is true. Even better give a proof of it for all n by using the definition of the product. For example, if A is an $m \times n$ matrix, then

$$(AI)_{ij} = \sum_{k=1}^{n} A_{ik} I_{kj} = A_{ij}$$

where we used the fact that I_{kj} is zero except when kji, i.e., the only non-zero term in the sum is $A_{ij} I_{jj} = A_{ij}$.

6.6. Multiplication is associative. Another way to see whether you understand the definition of the product in (6-1) is to try using it to prove that matrix multiplication is associative, i.e., that

$$(AB)C = A(BC) \tag{6-2}$$

for any three matrices for which this product makes sense. This is an important property, just as it is for numbers: if a, b, and c, are real numbers then $(ab)c = a(bc)$; this allows us to simply write abc, or when there are four numbers $abcd$, because we know we get the same answer no matter how we group the numbers in forming the product. For example

$$(2 \times 3) \times (4 \times 5) = 6 \times 20 = 120$$

and

$$\big((2 \times 3) \times 4\big) \times 5 = (6 \times 4) \times 5 = 24 \times 5 = 120.$$

Formula (6-1) only defines the product of <u>*two*</u> matrices so to form the product of three matrices A, B, and C, of sizes $k \times \ell$, $\ell \times m$, and $m \times n$, respectively, we must use (6-1) twice. But there are two ways to do that: first compute AB, then multiply on the right by C; or first compute BC, then multiply on the left by A. The formula $(AB)C = A(BC)$ says that those two alternatives produce the same matrix. Therefore we can write ABC for that product (no parentheses!) without ambiguity. Before we can do that we must <u>*prove*</u> (6-2) by using the definition (6-1) of the product of two matrices.

6.7. Try using (6-1) to prove (6-2). To show two matrices are equal you must show their entries are the same. Thus, you must prove the ij^{th} entry of $(AB)C$ is equal to the ij^{th} entry of $A(BC)$. To begin, use (6-1) to compute $((AB)C)_{ij}$. I leave you to continue.

This is a test of your desire to pass the course. I know you want to pass the course, but do you want that enough to do this computation?[1]

Can you use the associative law to prove that if J is an $n \times n$ matrix with the property that $AJ = A$ and $JB = B$ for all $m \times n$ matrices A and all $n \times p$ matrices B, then $J = I_n$?

6.8. The distributive law. If A, B, and C, are matrices of sizes such that the following expressions make sense, then

$$(A + B)C = AC + BC.$$

6.9. The columns of the product AB. Suppose the product AB exists. It is sometimes useful to write $\underline{B}_j$ for the j^{th} column of B and write

$$B = [\underline{B}_1, \dots, \underline{B}_n].$$

The columns of AB are then given by the formula

$$AB = [A\underline{B}_1, \dots, A\underline{B}_n].$$

You should check this asssertion.

6.10. The product $A\underline{x}$. Suppose $A = [\underline{A}_1, \underline{A}_2, \dots, \underline{A}_n]$ is a matrix with n columns and

$$\underline{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Then

$$A\underline{x} = x_1\underline{A}_1 + x_2\underline{A}_2 + \cdots + x_n\underline{A}_n.$$

This last equation is *one of the most important equations in the course.* Tattoo it on your body. If you don't know this equation you will probably fail the course.

Try to prove it yourself. First do two simple examples, A a 2×3 matrix, and A a 3×2 matrix. Then try the general case, A an $m \times n$ matrix.

[1]Perhaps I will ask you to prove that $(AB)C = A(BC)$ on the midterm—would you prefer to discover whether you can do that now or then?

6.11. Multiplication by a scalar. There is another kind of multiplication we can do. Let A be an $m \times n$ matrix and let c be any real number. We define cA to be the $m \times n$ matrix obtained by multiplying every entry of A by c. Formally, $(cA)_{ij} = cA_{ij}$ for all i and j. For example,

$$3\begin{pmatrix} 1 & 3 & 0 \\ -4 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 9 & 0 \\ -12 & 15 & 6 \end{pmatrix}.$$

We also define the product Ac be declaring that it is equal to cA, i.e., $Ac = cA$.

7. Pitfalls and warnings

7.1. Warning: multiplication is not commutative. If a and b are numbers, then $ab = ba$. However, if A and B are matrices AB need not equal BA even if both products exist. For example, if A is a 2×3 matrix and B is a 3×2 matrix, then AB is a 2×2 matrix whereas BA is a 3×3 matrix.

Even if A and B are square matrices of the same size, which ensures that AB and BA have the same size, AB need not equal BA. For example,

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \tag{7-1}$$

but

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \tag{7-2}$$

7.2. Warning: a product of non-zero matrices can be zero. The calculation (7-2) shows AB can be zero when both A and B are non-zero.

7.3. Warning: you can't always cancel. If A is not zero and $AB = AC$ it need not be true that $B = C$. For example, in (7-2) we see that $AB = 0 = A0$ but the A cannot be cancelled to deduce that $B = 0$.

8. Transpose

The transpose of an $m \times n$ matrix A is the $n \times m$ matrix A^T defined by

$$(A^T)_{ij} := A_{ji}.$$

Thus the transpose of A is "the reflection of A in the diagonal", and the rows of A become the columns of A^T and the columns of A become the rows of A^T. An example makes it clear:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}.$$

Notice that $(A^T)^T = A$.

The transpose of a column vector is a row vector and vice versa. We often use the transpose notation when writing a column vector—it saves space[2] and looks better to write $\underline{v}^T = (1\ 2\ 3\ 4)$ rather than

$$\underline{v} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}.$$

Check that

$$(AB)^T = B^T A^T.$$

A lot of students get this wrong: they think that $(AB)^T$ is equal to $A^T B^T$. (If the product AB makes sense $B^T A^T$ need not make sense.)

9. Some special matrices

We have already met two special matrices, the identity and the zero matrix. They behave like the numbers 1 and 0 and their great importance derives from that simple fact.

9.1. Symmetric matrices. We call A a symmetric matrix if $A^T = A$. A symmetric matrix must be a square matrix. A symmetric matrix is symmetric about its main diagonal. For example

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 4 & 5 & 6 \\ 2 & 5 & 7 & 8 \\ 3 & 6 & 8 & 9 \end{pmatrix}$$

is symmetric.

A square matrix A is symmetric if $A_{ij} = A_{ji}$ for all i and j. For example, the matrix

$$\begin{pmatrix} 1 & -2 & 5 \\ -2 & 0 & 4 \\ 5 & 4 & -9 \end{pmatrix}$$

is symmetric. The name comes from the fact that the entries below the diagonal are the same as the corresponding entries above the diagonal where "corresponding" means, roughly, the entry obtained by reflecting in the diagonal. By the diagonal of the matrix above I mean the line from the top left corner to the bottom right corner that passes through the numbers 1, 0, and -9.

If A is any square matrix show that $A + A^T$ is symmetric.

Is AA^T symmetric?

Use the definition of multiplication to show that $(AB)^T = B^T A^T$.

---

[2]Printers dislike blank space because it requires more paper. They also dislike black space, like ▲, ★, ♣, ■, because it requires more ink.

9.2. Skew-symmetric matrices. A square matrix A is skew-symmetric if $A^T = -A$.

If B is a square matrix show that $B - B^T$ is skew symmetric.

What can you say about the entries on the diagonal of a skew-symmetric matrix.

9.3. Upper triangular matrices. A square matrix is upper triangular if all its entries below the diagonal are zero. For example,

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 4 & 5 & 6 \\ 0 & 0 & 7 & 8 \\ 0 & 0 & 0 & 9 \end{pmatrix}$$

is upper triangular.

9.4. Lower triangular matrices. A square matrix is lower triangular if all its entries above the diagonal are zero. For example,

$$\begin{pmatrix} 1 & 0 & 0 \\ 4 & 5 & 0 \\ 7 & 8 & 9 \end{pmatrix}$$

is lower triangular. The transpose of a lower triangular matrix is upper triangular and vice-versa.

10. Solving an equation involving an upper triangular matrix

Here is an easy problem: find numbers x_1, x_2, x_3, x_4 such that

$$A\underline{x} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = \underline{b}.$$

Multiplying the bottom row of the 4×4 matrix by the column $\underline{x}$ gives $2x_4$ and we want that to equal b_4 which is 4, so $x_4 = 2$. Multiplying the third row of the 4×4 matrix by $\underline{x}$ gives $-x_3 + x_4$ and we want that to equal b_3 which is 3. We already know $x_4 = 2$ so we must have $x_3 = -1$. Repeating this with the second row of A gives $2x_2 - x_3 = 2$, so $x_2 = \frac{1}{2}$. Finally the first row of A gives $x_1 + 2x_2 + 3x_3 + 4x_4 = 1$; plugging in the values we have found for x_4, x_3, and x_2, we get $x_1 + 1 - 3 + 8 = 1$ so $x_1 = -5$. We find that a solution is given by

$$\underline{x} = \begin{pmatrix} -5 \\ \frac{1}{2} \\ -1 \\ 4 \end{pmatrix}.$$

Is there any other solution to this equation? No. Our hand was forced at each stage.

Here is a hard problem:

11. Some special products

Here we consider an $m \times n$ matrix B and the effect of multiplying B on the left by some special $m \times m$ matrices. In what follows, let

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}.$$

11.1. Let D denote the $m \times m$ matrix on the left in the product.

$$\begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_{m-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_m \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} \lambda_1 x_1 \\ \lambda_2 x_2 \\ \vdots \\ \\ \vdots \\ \lambda_m x_m \end{pmatrix} \tag{11-1}$$

Since $DB = [D\underline{B}_1, \ldots, D\underline{B}_n]$ it follows from (11-1) that the i^{th} row of DB is λ_i times the i^{th} row of B.

A special case of this appears when we discuss elementary row operations in chapter 5. There we take $\lambda_i = c$ and all other λ_js equal to 1. In that case DB is the same as B except that the i^{th} row of DB is c times the i^{th} row of DB.

11.2. Fix two different integers i and j and let E be the $m \times m$ matrix obtained by interchanging the i^{th} and j^{th} rows of the identity matrix. If X is an $m \times 1$ matrix, then EX is the same as X except that the entries in the i^{th} and j^{th} positions of X are switched.

Thus, if B is an $m \times n$ matrix, then EB is the same as B except that the i^{th} and j^{th} rows are interchanged. (Check that.) This operation, switching two rows, will also appear in chapter 5 when we discuss elementary row operations.

11.3. Fix two different integers i and j and let F be the $m \times m$ matrix obtained from the identity matrix by changing the ij^{th} entry from zero to c. If X is an $m \times 1$ matrix, then FX is the same as X except that the entry x_i has been replaced by $x_i + cx_j$. Thus, if B is an $m \times n$ matrix, then FB is the same as B except that the i^{th} row is now the sum of the i^{th} row and c times the j^{th} row. (Check that.) This operation too appears when we discuss elementary row operations.

11.4. The matrices D, E, and F all have inverses, i.e., there are matrices D', E', and F', such that $I = DD' = D'D = EE' = E'E = FF' = F'F$, where I denotes the $m \times m$ identity matrix. (Oh, I need to be careful – here I mean D is the matrix in (11-1) with $\lambda_i = c$ and all other λ_js equal to 1.)

11.5. Easy question. Is there a positive integer n such that

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}?$$

If so what is the smallest such n? Can you describe all other n for which this equality holds?

CHAPTER 3

Matrices and motions in $\mathbb{R}^2$ and $\mathbb{R}^3$

1. Linear transformations

Functions play a central role in all parts of mathematics. The functions relevant to linear algebra are called *linear transformations*.

We write $\mathbb{R}^n$ for the set of $n \times 1$ column vectors. This has a linear structure:

(1) if $\underline{u}$ and $\underline{v}$ are in $\mathbb{R}^n$ so is $\underline{u} + \underline{v}$;
(2) if $c \in \mathbb{R}$ and $\underline{u} \in \mathbb{R}^n$, then $c\underline{u} \in \mathbb{R}^n$.

A non-empty subset W of $\mathbb{R}^n$ is called a subspace if it has these two properties: i.e.,

(1) if $\underline{u}$ and $\underline{v}$ are in W so is $\underline{u} + \underline{v}$;
(2) if $c \in \mathbb{R}$ and $\underline{u} \in W$, then $c\underline{u} \in W$.

A linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$ is a function $f : \mathbb{R}^n \to \mathbb{R}^m$ such that

(1) $f(\underline{u} + \underline{v}) = f(\underline{u}) + f(\underline{v})$ for all $\underline{u}, \underline{v} \in \mathbb{R}^n$, and
(2) $f(c\underline{u}) = cf(\underline{u})$ for all $c \in \mathbb{R}$ and all $\underline{u} \in \mathbb{R}^n$.

In colloquial terms, these two requirements say that linear transformations preserve the linear structure.

Left multiplication by an $m \times n$ matrix A is a linear function from $\mathbb{R}^n$ to $\mathbb{R}^m$. If $\underline{x} \in \mathbb{R}^n$, then $A\underline{x} \in \mathbb{R}^m$.

2. Rotations in the plane

3. Projections in the plane

4. Contraction and dilation

5. Reflections in the plane

6. Reflections in $\mathbb{R}^3$

7. Projections from $\mathbb{R}^3$ to a plane

CHAPTER 4

Systems of Linear Equations

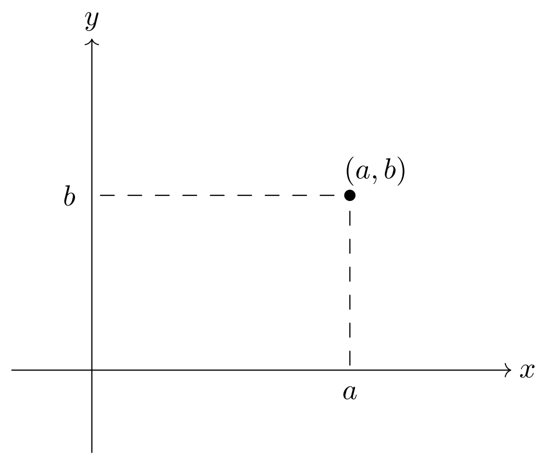
The meat of this chapter begins in §2 below. However, some of the terminology and framework for systems of linear equations applies to other systems of equations so §1 starts with a discussion of the general framework. Nevertheless, it is probably best to go directly to §2, read through to the end of the chapter then return to §1.

1. Systems of equations

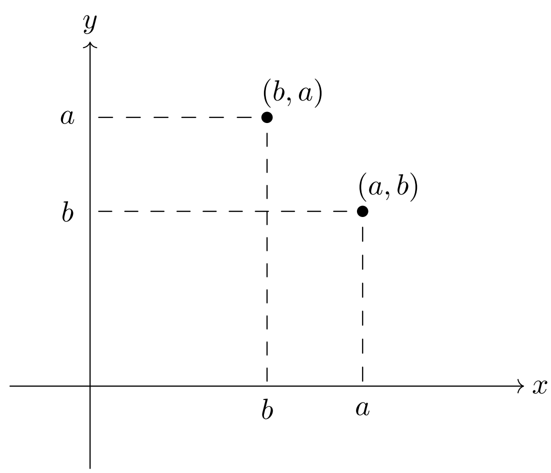
You have been solving equations for years. Sometimes you have considered the solutions to a single equation. For example, you are familiar with the fact that the solutions to the equation $y = x^2 - 4x + 1$ form a parabola. Likewise, the solutions to the equation $(x-2)^2 + (y-1)^2 + z^2 = 1$ form a sphere of radius 1 centered at the point $(2, 1, 0)$.

1.1. Let's consider these statements carefully. By a solution to the equation $y = x^2 - x - 4$ we mean a pair of numbers (a, b) that give a true statement when they are plugged into the equation, i.e., (a, b) is called a solution if b *does* equal $a^2 - 4a + 1$. If $a^2 - 4a + 1 \neq b$, then (a, b) is <u>*not*</u> a solution to $y = x^2 - x - 4$.

1.2. Pairs of numbers (a, b) also label points in the plane. More precisely, we can draw a pair of axes perpendicular to each other, usually called the x- and y-axes, and (a, b) denotes the point obtained by going a units along the x-axis and b-units along the y-axis. The picture below illustrates the situation:



When we label a point by a pair of numbers the *order* of the numbers matters. For example, if $a \neq b$, the points (a, b) and (b, a) are different. In the above example, we have



The order also matters when we say $(3, 2)$ is a solution to the equation $y = x^2 - x - 4$. Although $(3, 2)$ is a solution to $y = x^2 - x - 4$, $(2, 3)$ is not.

1.3. $\mathbb{R}^2$ and $\mathbb{R}^3$. We write $\mathbb{R}^2$ for the set of all ordered pairs of numbers (a, b). Here $\mathbb{R}$ denotes the set of real numbers and the superscript 2 in $\mathbb{R}^2$ indicates *pairs* of real numbers. The general principle is that a solution to an equation in 2 unknowns is an ordered pair of real numbers, i.e., a point in $\mathbb{R}^2$.

A solution to an equation in 3 unknowns, $(x - 2)^2 + (y - 1)^2 + z^2 = 1$ for example, is an ordered triple of numbers, i.e., a triple (a, b, c) such that $(a-2)^2 + (b-1)^2 + c^2$ *does* equal 1. The set of all ordered triples of numbers is denoted by $\mathbb{R}^3$.

1.4. A system of equations. We can consider more than one equation at a time. When we consider several equations at once we speak of a *system* of equations. For example, we can ask for solutions to the system of equations

$$\begin{cases} y = x^2 - x - 4 \\ y = 3x - 7. \end{cases} \tag{1-1}$$

A solution to this system of equations is an ordered pair of numbers (a, b) with the property that when we plug in a for x and b for y *both equations are true*. That is, (a, b) is a solution to the system (1-1) if $b = a^2 - a - 4$ *and* $b = 3a - 7$. For example, $(3, 2)$ is a solution to the system (1-1). So is $(1, -4)$. Although $(4, 8)$ is a solution to $y = x^2 - x - 4$ it is <u>not</u> a solution to the system (1-1) because $8 \neq 3 \times 4 - 7$.

On the other hand, $(4, 8)$ is *not* a solution to the system (1-1): it is a solution to $y = x^2 - x - 4$ but not a solution to $y = 3x - 7$ because $8 \neq 3 \times 4 - 7$.

1.5. More unknowns and $\mathbb{R}^n$. The demands of the modern world are such that we often encounter equations with many unknowns, sometimes billions of unknowns. Let's think about a modest situation, a system of 3 equations in 5 unknowns. For example, a solution to the system of equations

$$\begin{cases} x_1 + x_2^2 + x_3^3 + x_4^4 + x_5^5 = 100 \\ x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 = 0 \\ x_1x_2 + x_3x_4 - x_5^2 = -20 \end{cases} \tag{1-2}$$

is an ordered 5-tuple[1] of numbers, $(s_1, s_2, s_3, s_4, s_5)$, having the property that when we plug in s_1 for x_1, s_2 for x_2, s_3 for x_3, s_4 for x_4, and s_5 for x_5, all three of the equations in (1-2) become true. We use the notation $\mathbb{R}^5$ to denote the set of all ordered 5-tuples of real numbers. Thus, the solutions to the system (1-2) are elements of $\mathbb{R}^5$.

We often call elements of $\mathbb{R}^5$ *points* just as we call points in the plane *points*. A point in $\mathbb{R}^5$ has 5 coordinates, whereas a point in the plane has 2 coordinates.

More generally, solutions to a system of equations with n unknowns are, or can be thought of as, points in $\mathbb{R}^n$. We sometimes call $\mathbb{R}^n$ *n-space*. For example, we refer to the physical world around us as 3-space. If we fix an origin and x-, y-, and z-axes, each point in our physical world can be

[1]We run out of words after *pair, triple, quadruple, quintuple, sextuple, ...* so invent the word *n-tuple* to refer to an ordered sequence of n numbers where n can be any positive integer. For example, (8,7,6,5,4,3,2,1) is an 8-tuple. It is not the same as the 8-tuple (1,2,3,4,5,6,7,8). We think these 8-tuples as labels for two different points in $\mathbb{R}^8$. Although we can't picture $\mathbb{R}^8$ we can ask questions about it. For example, does (1,1,1,1,1,1,1,1) lie on the line through the points (8,7,6,5,4,3,2,1) and (1,2,3,4,5,6,7,8)? The answer is "yes". Why? If you can answer this you understand what is going on. If you can't you don't, and should ask a question.

labelled in a unique way by an ordered triple of numbers. If we take time as well as position into account we need 4-coordinates and then speak of $\mathbb{R}^4$. Physicists like to call $\mathbb{R}^4$ *space-time*. It has 3 space-like coordinates and 1 time coordinate.

1.6. Non-linear equations. The equations $y = x^2 - x - 4$ and $(x-2)^2 + (y-1)^2 + z^2 = 1$ are *not* linear equations.

2. A single linear equation

The general equation of a line in $\mathbb{R}^2$ is of the form

$$ax + by = c.$$

The general equation of a plane in $\mathbb{R}^3$ is of the form

$$ax + by + cz = d.$$

These are examples of *linear equations*.

A linear equation is an equation of the form

$$a_1x_1 + \cdots + a_nx_n = b \tag{2-1}$$

in which the a_is and b belong to $\mathbb{R}$ and $x_1, \ldots, x_n$ are unknowns. We call the a_is the coefficients of the unknowns.

A solution to (2-1) is an ordered n-tuple $(s_1, \ldots, s_n)$ of real numbers that when substituted for the x_is makes equation (2-1) true, i.e.,

$$a_1s_1 + \cdots + a_ns_n = b.$$

When $n = 2$ a solution is a pair of numbers (s_1, s_2) which we can think of as the coordinates of a point in the plane. When $n = 3$ a solution is a triple of numbers (s_1, s_2, s_3) which we can think of as the coordinates of a point in 3-space. We will use the symbol $\mathbb{R}^2$ to denote the plane and $\mathbb{R}^3$ to denote 3-space. The idea for the notation is that the $\mathbb{R}$ in $\mathbb{R}^3$ denotes the set of real numbers and the 3 means a triple of real numbers. The notation continues: $\mathbb{R}^4$ denotes quadruples (a, b, c, d) of real numbers and $\mathbb{R}^4$ is referred to as 4-space.[2]

A geometric view. If $n \geq 2$ and at least one a_i is non-zero, equation (2-1) has infinitely many solutions: for example, when $n = 2$ the solutions are the points on a line in the plane $\mathbb{R}^2$; when $n = 3$ the solutions are the points on a plane in 3-space $\mathbb{R}^3$; when $n = 4$ the solutions are the points on a 3-plane in $\mathbb{R}^4$; and so on.

It will be important in this course to have a geometric picture of the set of solutions. We begin to do this in earnest in chapter 6 but it is useful to keep this in mind from the outset. Solutions to equation (2-1) are ordered n-tuples of real numbers $(s_1, \ldots, s_n)$ and we think of the numbers s_i as the coordinates of a point in n-space, i.e., in $\mathbb{R}^n$.

---

[2]Physicists think of $\mathbb{R}^4$ as space-time with coordinates (x, y, z, t), 3 spatial coordinates, and one time coordinate.

The collection of *all* solutions to $a_1x_1 + \cdots + a_nx_n = b$ is a special kind of subset in n-space: it has a *linear structure* and that is why we call (2-1) a linear equation. By a "linear structure" we mean this:

PROPOSITION 2.1. *If the points $p = (s_1, \dots, s_n)$ and $q = (t_1, \dots, t_n)$ are different solutions to (2-1), then all points on the line through p and q are also solutions to (2-1).*

This result is easy to see once we figure out how to describe the points that lie on the line through p and q.

Let's write $\overline{pq}$ for the line through p and q. The prototypical line is the real number line $\mathbb{R}$ so we want to associate to each real number λ a point on $\overline{pq}$. We do that by presenting $\overline{pq}$ in parametric form: $\overline{pq}$ consists of all points of the form

$$\lambda p + (1-\lambda)q = (\lambda s_1 + (1-\lambda)t_1, \dots, \lambda s_n + (1-\lambda)t_n)$$

as λ ranges over all real numbers. Notice that p is obtained when $\lambda = 1$ and q is obtained when $\lambda = 0$.

Proof of Proposition 2.1. The result follows from the calculation

$$a_1\big(\lambda s_1 + (1-\lambda)t_1\big) + \cdots + a_n\big(\lambda s_n + (1-\lambda)t_n\big) = \\ \lambda\big(a_1s_1 + \cdots + a_ns_n\big) + (1-\lambda)(a_1t_1 + \cdots + a_nt_n)$$

which equals $\lambda \underline{b} + (1-\lambda)\underline{b}$, i.e., equals $\underline{b}$, if $(s_1, \dots, s_n)$ and $(t_1, \dots, t_n)$ are solutions to (2-1). $\Diamond$

3. Systems of linear equations

An $m \times n$ system of linear equations is a collection of m linear equations in n unknowns. We usually write out the general $m \times n$ system like this:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ \vdots \qquad\qquad\qquad & \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m. \end{aligned}$$

The unknowns are $x_1, \dots, x_n$, and the aim of the game is to find them when the a_{ij}s and b_is are specific real numbers. The a_{ij}s are called the coefficients of the system. We often arrange the coefficients into an $m \times n$ array

$$A := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

called the coefficient matrix.

4. A system of linear equations is a single matrix equation

We can assemble the b_is and the unknowns x_j into column vectors

$$\underline{b} := \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \qquad \text{and} \qquad \underline{x} := \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

The system of linear equations at the beginning of §3 can now be written as a single matrix equation

$$A\underline{x} = \underline{b}.$$

You should multiply out this equation and satisfy yourself that it is the same system of equations as at the beginning of chapter 3. This matrix interpretation of the system of linear equations will be center stage throughout this course.

We often arrange all the data into a single $m \times (n+1)$ matrix

$$(A|\,\underline{b}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & |\, b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & |\, b_2 \\ \vdots & & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & |\, b_m \end{pmatrix}$$

that we call the augmented matrix of the system.

5. Specific examples

5.1. A unique solution. The only solution to the 2×2 system

$$\begin{aligned} x_1 + x_2 &= 2 \\ 2x_1 - x_2 &= 1 \end{aligned}$$

is $(x_1, x_2) = (1, 1)$. You can think of this in geometric terms. Each equation determines a line in $\mathbb{R}^2$, the points (x_1, x_2) on each line corresponding to the solutions of the corresponding equation. The points that lie on *both* lines therefore correspond to simultaneous solutions to the pair of eqations, i.e., solutions to the 2×2 system of equations.

5.2. No solutions. The 2×2 system

$$\begin{aligned} x_1 + x_2 &= 2 \\ 2x_1 + 2x_2 &= 6 \end{aligned}$$

has no solution at all: if the numbers x_1 and x_2 are such that $x_1 + x_2 = 2$ then $2(x_1 + x_2) = 4$, *not* 6. It is enlightening to think about this system geometrically. The points in $\mathbb{R}^2$ that are solutions to the equation $x_1 + x_2 = 2$ lie on the line of slope -1 passing through $(0, 2)$ and $(2, 0)$. The points in $\mathbb{R}^2$ that are solutions to the equation $2(x_1 + x_2) = 6$ lie on the line of slope -1 passing through $(0, 3)$ and $(3, 0)$. Thus, the equations give two parallel lines:

there is no point lying on both lines and therefore no common solution to the pair of equations, i.e., no solution to the given system of linear equations.

5.3. No solutions. The 3×2 system

$$\begin{aligned} x_1 + x_2 &= 2 \\ 2x_1 - x_2 &= 1 \\ x_1 - x_2 &= 3 \end{aligned}$$

has no solutions because the only solution to the 2×2 system consisting of the first two equations is $(1,1)$ and that is *not* a solution to the third equation in the 3×2 system. Geometrically, the solutions to each equation lie on a line in $\mathbb{R}^2$ and the three lines do not pass through a common point.

5.4. A unique solution. The 3×2 system

$$\begin{aligned} x_1 + x_2 &= 2 \\ 2x_1 - x_2 &= 1 \\ x_1 - x_2 &= 0 \end{aligned}$$

has a unique solution, namely $(1,1)$. The three lines corresponding to the three equations all pass through the point $(1,1)$.

5.5. Infinitely many solutions. It is obvious that the system consisting of the single equation

$$x_1 + x_2 = 2$$

has infinitely many solutions, namely all the points lying on the line of slope -1 passing through $(0,2)$ and $(2,0)$.

5.6. Infinitely many solutions. The 2×2 system

$$\begin{aligned} x_1 + x_2 &= 2 \\ 2x_1 + 2x_2 &= 4 \end{aligned}$$

has infinitely many solutions, namely all the points lying on the line of slope -1 passing through $(0,2)$ and $(2,0)$ because the two equations actually give the *same* line in $\mathbb{R}^2$. A solution to the first equation is also a solution to the second equation in the system.

5.7. Infinitely many solutions. The 2×3 system

$$\begin{aligned} x_1 + x_2 + x_3 &= 3 \\ 2x_1 + x_2 - x_3 &= 4 \end{aligned}$$

also has infinitely many solutions. The solutions to the first equation are the points on the plane $x_1 + x_2 + x_3 = 3$ in $\mathbb{R}^3$. The solutions to the second equation are the points on the plane $2x_1 + x_2 - x_3 = 4$ in $\mathbb{R}^3$. The two planes meet one another in a line. That line can be described parametrically as the points

$$(1 + 2t, 2 - 3t, t)$$

as t ranges over all real numbers. You should check that when $x_1 = 1 + 2t$, $x_2 = 2 - 3t$, and $x_3 = t$, both equations in the 2×3 system are satisfied.

5.8. A unique solution. The 3×3 system

$$\begin{aligned} x_1 + x_2 + x_3 &= 3 \\ 2x_1 + x_2 - x_3 &= 4 \\ 4x_1 + 3x_2 - 2x_3 &= 13 \end{aligned}$$

has a unique solution, namely $(x_1, x_2, x_3) = (-1, 5, -1)$. The solutions to each equation are the points in $\mathbb{R}^3$ that lie on the plane given by the equation. There is a unique point lying on all three planes , namely $(-1, 5, -1)$. This is typical behavior: two planes in $\mathbb{R}^3$ meet in a line (unless they are parallel), and that line will (usually!) meet a third plane in a point. The next two example show this doesn't always happen: in Example 5.9 the third plane is *parallel* to the line that is the intersection of the first two planes; in Example 5.10 the third plane is *contains* the line that is the intersection of the first two planes.

5.9. No solution. We will now show that the 3×3 system

$$\begin{aligned} x_1 + x_2 + x_3 &= 3 \\ 2x_1 + x_2 - x_3 &= 4 \\ 3x_1 + x_2 - 3x_3 &= 0 \end{aligned}$$

has a no solution. In Example 5.7 we showed that all solutions to the system consisting of the first two equations in the 3×3 system we are now considering are of the form $(1 + 2t, 2 - 3t, t)$ for some t in $\mathbb{R}$. However, if $(x_1, x_2, x_3) = (1 + 2t, 2 - 3t, t)$, then

$$3x_1 + x_2 - 3x_3 = 3(1 + 2t) + (2 - 3t) - 3t = 5, \tag{5-1}$$

not 0, so no solution to the first two equations is a solution to the third equation. Thus the 3×3 system has no solution.

5.10. Infinitely many solutions. The 3×3 system

$$\begin{aligned} x_1 + x_2 + x_3 &= 3 \\ 2x_1 + x_2 - x_3 &= 4 \\ 3x_1 + x_2 - 3x_3 &= 5 \end{aligned}$$

has infinitely many solutions because, as equation (5-1) showed, every solution to the system consisting of the first two equations in the 3×3 system we are currently considering is a solution to the equation third equation $3x_1 + x_2 - 3x_3 = 5$.

6. The number of solutions

The previous examples show that a system of linear equations can have no solution, or a unique solution, or infinitely many solutions. The next proposition shows these are the only possibilities.

PROPOSITION 6.1. *If a system of linear equations has ≥ 2 solutions, it has infinitely many.*

Proof. Suppose $(s_1, \dots, s_n)$ and $(t_1, \dots, t_n)$ are different solutions to the $m \times n$ system

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i, \qquad (1 \leq i \leq m).$$

Then

$$(\lambda s_1 + (1-\lambda)t_1, \dots, \lambda s_n + (1-\lambda)t_n) \tag{6-1}$$

is also a solution for every $\lambda \in \mathbb{R}$ because

$$\begin{aligned} a_{i1}(\lambda s_1 + (1-\lambda)t_1) + \cdots + a_{in}(\lambda s_n + (1-\lambda)t_n) = \\ \lambda(a_{i1}s_1 + \cdots + a_{in}s_n) + (1-\lambda)(a_{i1}t_1 + \cdots + a_{in}t_n) \\ = \lambda b_i + (1-\lambda)b_i \\ = b_i. \end{aligned}$$

Since there are infinitely many λs in $\mathbb{R}$ there are infinitely many solutions to the system. □

If we think of the solutions to an $m \times n$ system as points in $\mathbb{R}^n$, the points in (6-1) are the points on the line through the points $(s_1, \dots, s_n)$ and $(t_1, \dots, t_n)$. Thus, the proof of Proposition 6.1 says that if two points in $\mathbb{R}^n$ are solutions to $A\underline{x} = \underline{b}$, so are all points on the line through them. It is this linear nature of the set of solutions that gives rise to the name *linear* equation. It is also why we call this subject linear algebra. I think *Linear algebra and linear geometry* would be a better name.

The following result is an immediate consequence of Proposition 6.1.

COROLLARY 6.2. *A system of linear equations has either*

1. *a unique solution or*
2. *no solutions or*
3. *infinitely many solutions.*

A system of linear equations is consistent if it has a solution, and inconsistent if it does not.

7. A geometric view on the number of solutions

Two lines in the plane intersect at either

1. a unique point or
2. no point (they are parallel) or
3. infinitely many points (they are the same line).

Lines in the plane are "the same things" as equations $a_1x + a_1'y = b_1$. The points on the line are the solutions to the equation. The solutions to a pair (system) of equations $a_1x + a_1'y = b_1$ and $a_2x + a_2'y = b_2$ are the points that lie on both lines, i.e., their intersection.

In 3-space, which we will denote by $\mathbb{R}^3$, the solutions to a single equation form a plane. Two planes in $\mathbb{R}^3$ intersect at either

(1) no point (they are parallel) or
(2) infinitely many points (they are not parallel).

In the second case the intersection is a line if the planes are different, and a plane if they are the same.

Three planes in $\mathbb{R}^3$ intersect at either

(1) a unique point or
(2) no point (all three are parallel) or
(3) infinitely many points (all three planes are the same or the intersection of two of them is a line that lies on the third plane).

I leave you to consider the possibilities for three lines in the plane and four planes in $\mathbb{R}^3$. Discuss with friends if necessary.

8. Homogeneous systems

A system of linear equations of the form $A\underline{x} = 0$ is called a homogeneous system. A homogeneous system always has a solution, namely $\underline{x} = 0$, i.e., $x_1 = \cdots = x_n = 0$. This is called the trivial solution because little brainpower is needed to find it. Other solutions to $A\underline{x} = 0$ are said to be non-trivial.

For a homogeneous system the issue is to describe the set of *non-trivial* solutions.

8.1. A trivial but important remark. If $(s_1, \ldots, s_n)$ is a solution to a homogeneous system so is $(\lambda s_1, \ldots, \lambda s_n)$ for all $\lambda \in \mathbb{R}$, i.e., all points on the line through the origin $0 = (0, \ldots, 0)$ and $(s_1, \ldots, s_n)$ are solutions.

8.2. A geometric view. The next result, Proposition 8.1, shows that solutions to the system of equations $A\underline{x} = \underline{b}$ are closely related to solutions to the homogeneous system of equations $A\underline{x} = 0$.[3] We can see this relationship in the setting of a single equation in 2 unknowns.

The solutions to the equation $2x + 3y = 0$ are points on a line in the plane $\mathbb{R}^2$. Draw that line: it is the line through the origin with slope $-\frac{2}{3}$. The origin is the trivial solution. Other points on the line such as $(3, -2)$ are non-trivial solutions. The solutions to the non-homogeneous equation $2x + 3y = 1$ are also points on a line in $\mathbb{R}^2$. Draw it. This line has slope $-\frac{2}{3}$ too. It is parallel to the line $2x + 3y = 0$ but doesn't go through the origin.

Pick any point on the second line, i.e., any solution to $2x+3y = 1$. Let's pick $(-1, 1)$. Now take a solution to the first equation, say $(3, -2)$ and add

[3] Students seem to have a hard time understanding Proposition 8.1. Section 8.3 discusses an analogy to Proposition 8.1 that will be familiar to you from your calculus courses.

it to $(-1, 1)$ to obtain $(2, -1)$. The point $(2, -1)$ is on the line $2x + 3y = 1$. In fact, if we take any solution to $2x + 3y = 0$, say (a, b), and add it to $(-1, 1)$ we obtain a solution to $2x + 3y = 1$ because

$$(a, b) + (-1, 1) = (a - 1, b + 1)$$

and

$$2(a - 1) + 3(b + 1) = 2a + 3b - 2 + 3 = 0 + 1 = 1.$$

Every solution to $2x + 3y = 1$ can be obtained this way. That is what Proposition 8.1 says, though in much greater generailty.

There was nothing special about our choice of $(-1, 1)$. Everything would work in the same way if we had chosen $(5, -3)$ for example. Check it out!

The line $2x + 3y = 1$ is obtained by translating (moving) the line $2x + 3y = 0$ to the parallel line through $(-1, 1)$. Alternatively, the line $2x+3y = 1$ is obtained by translating the line $2x + 3y = 0$ to the parallel line through $(5, -3)$. The picture in chapter 3 might increase your understanding of this important point (though a different equation is used there). The discussion in chapter 3 might also help.

If I had taken $2x+3y = -3$ instead of $2x+3y = 1$ the same sort of thing happens. The solutions to $2x+3y = -3$ lie on a line parallel to $2x+3y = 0$. In fact, every line parallel to $2x+3y = 0$ is the set of solutions to $2x+3y = c$ for a suitable c.

Proposition 8.1. *Suppose $\underline{u}$ is a solution to the equation $A\underline{x} = \underline{b}$. Then the set of all solutions to $A\underline{x} = \underline{b}$ consists of all vectors $\underline{u} + \underline{v}$ in which $\underline{v}$ ranges over all solutions to the homogeneous equation $A\underline{x} = 0$.*

Proof. Fix a solution $\underline{u}$ to the equation $A\underline{x} = \underline{b}$; i.e., $A\underline{u} = \underline{b}$. If $\underline{u}'$ is a solution to $A\underline{x} = \underline{b}$, then $\underline{u}' - \underline{u}$ is a solution to the homogeneous equation $A\underline{x} = 0$, and $\underline{u}' = \underline{u} + (\underline{u}' - \underline{u})$.

Conversely, if $A\underline{v} = 0$, i.e., if $\underline{v}$ is a solution to the homogeneous equation $A\underline{x} = 0$, then $A(\underline{u} + \underline{v}) = A\underline{u} + A\underline{v} = \underline{b} + 0 = \underline{b}$, so $\underline{u} + \underline{v}$ is a solution to $A\underline{x} = \underline{b}$. □

As we shall later see, the set of solutions to a system of homogeneous linear equations is a subspace. Subspaces are fundamental objects in linear algebra. You should compare Proposition 8.1 with the statement of Proposition 3.1. The two results say the same thing in slightly different words.

Corollary 8.2. *Suppose the equation $A\underline{x} = \underline{b}$ has a solution. Then $A\underline{x} = \underline{b}$ has a unique solution if and only if $A\underline{x} = \underline{0}$ has a unique solution.*

Proof. Let $\underline{u}$ be a solution to the equation $A\underline{x} = \underline{b}$; i.e., $A\underline{u} = \underline{b}$. Let $\underline{v} \in \mathbb{R}^n$. Then $A(\underline{u}+\underline{v}) = \underline{b} + A\underline{v}$ so $\underline{u}+\underline{v}$ is a solution to the equation $A\underline{x} = \underline{b}$ if and only if $\underline{v}$ is a solution to the equation $A\underline{x} = \underline{0}$. □

You might find it easier to understand what Proposition 8.1 is telling you by looking at it in conjunction with chapter 7.1.

8.3. An analogy for understanding Proposition 8.1. You probably know that every solution to the differential equation $\frac{dy}{dx} = 2x$ is of the form $x^2 + c$ where c is an arbitrary constant. One particular solution to the equation $\frac{dy}{dx} = 2x$ is x^2. Now consider the equation $\frac{dy}{dx} = 0$; the solutions to this are the constant functions c, $c \in \mathbb{R}$. Thus every solution to $\frac{dy}{dx} = 2x$ is obtained by adding the particular solution x^2 to a solution to $\frac{dy}{dx} = 0$.

Compare the previous paragraph with the statement of Proposition 8.1: $2x$ is playing the role of $\underline{b}$, x^2 is playing the role of $\underline{u}$, and c is playing the role of $\underline{v}$.

In Proposition 8.1 it doesn't matter which $\underline{u}$ we choose; all solutions to $A\underline{x} = \underline{b}$ are given by $\underline{u} + \underline{v}$ where $\underline{v}$ runs over all solutions to $A\underline{x} = \underline{0}$.

Similarly, we can take any solution to $\frac{dy}{dx} = 2x$, $x^2+17\pi$ for example, and still all solutions to $\frac{dy}{dx} = 2x$ are obtained by adding $x^2 + 17\pi$ to a solution to $\frac{dy}{dx} = 0$. That is, every solution to $\frac{dy}{dx} = 2x$ is of the form $x^2 + 17\pi + c$ for some $c \in \mathbb{R}$.

8.4. A natural bijection between solutions to $A\underline{x} = 0$ and solutions to $A\underline{x} = \underline{b}$. A <u>bijection</u> between two sets X and Y is a rule that sets up a one-to-one correspondence between the elements on X and the elements of Y. We sometimes write $x \leftrightarrow y$ to denote the fact that an element x in X corresponds to the element y in Y. For example, there is a bijection between the set of all integers and the set of even integers given by $n \leftrightarrow 2n$. There is also a bijection between the even numbers and the odd numbers given by $2m \leftrightarrow 2m + 1$.

Suppose the equation $A\underline{x} = \underline{b}$ has a solution, say $\underline{u}$. Then Proposition 8.1 says there is a bijection between the set of solutions to $A\underline{x} = \underline{b}$ and the set of solutions to $A\underline{x} = 0$ given by

$$\underline{v} \longleftrightarrow \underline{u} + \underline{v}.$$

In other words, $\underline{v}$ is a solution to $A\underline{x} = 0$ if and only if $\underline{u} + \underline{v}$ is a solution to $A\underline{x} = \underline{b}$. In plainer language, if $A\underline{v} = 0$, then $A(\underline{u} + \underline{v}) = \underline{b}$ and conversely.

This is an arithmetic explanation, and generalization, of what was said in the discussion prior to Proposition 8.1. There

$$(a, b) \longleftrightarrow (a, b) + (-1, 1).$$

As I said before there is nothing special about our choice of $(-1, 1)$. We could take any point on $2x + 3y = 1$. For example, if we pick $(5, -3)$ we obtain another bijection between the solutions to $2x + 3y = 0$ and the solutions to $2x + 3y = 1$, namely

$$(a, b) \longleftrightarrow (a, b) + (5, -3).$$

CHAPTER 5

Row operations and row equivalence

1. Equivalent systems of equations

Two systems of linear equations are equivalent if they have the same solutions. An important strategy for solving a system of linear equations is to repeatedly perform operations on the system to get simpler but equivalent systems, eventually arriving at an equivalent system that is very easy to solve. The simplest systems to solve are those in row-reduced echelon form. We discuss those in the next chapter. In this chapter we discuss the three "row operations" you can perform on a system to obtain a simpler but equivalent system.

We will write R_i to denote the i^{th} row in a matrix.

The three elementary row operations on a matrix are the following:

(1) switch the positions of R_i and R_j;
(2) replace R_i by a non-zero multiple of R_i;
(3) replace R_i by $R_i + cR_j$ for any number c.

If A' can be obtained from A by a single row operation, then A can be obtained from A' by a single row operation. We say that two matrices are row equivalent if one can be obtained from the other by a *sequence* of elementary row operations.

PROPOSITION 1.1. *Two $m \times n$ systems of linear equations $A\underline{x} = \underline{b}$ and $A'\underline{x} = \underline{b}'$ are equivalent if and only if the augmented matrices $(A|\underline{b})$ and $(A'|\underline{b}')$ are row equivalent.*

You might take a look back at chapter 11 to better understand the elementary row operations.

1.1. Exercise. Find conditions on a, b, c, d such that the matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & -3 \\ 0 & 0 \end{pmatrix}$$

are row equivalent. (Use the fact that two matrices are row equivalent if they have the same sets of solutions.)

2. Echelon Form

A matrix E is in row echelon form (REF) if

(1) all rows consisting entirely of zeroes are at the bottom of E; and

(2) in each non-zero row the left-most non-zero entry, called the leading entry of that row, is to the right of the leading entry in the row above it.

A matrix E is in row-reduced echelon form (RREF) if

(1) it is in row echelon form, and
(2) every leading entry is a 1, and
(3) every column that contains a leading entry has all its other entries equal to zero.

For example,

$$\begin{pmatrix} 0 & 1 & 0 & 2 & 1 & 0 & 0 & 3 \\ 0 & 0 & 1 & 3 & 1 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

is in RREF.

THEOREM 2.1. *Given a matrix A, there is a unique row-reduced echelon matrix that is row equivalent to A.*

Proof. □

The uniqueness result in Theorem 2.1 allows us to speak of *the* row-reduced echelon matrix that is equivalent to A. We will denote it by

$$\text{rref}(A).$$

2.1. Reminder. It is important to know there are infinitely many sequences of elementry row operations that can get you from A to rref(A).

In an exam, if you are given a specific matrix A and asked to *put A in row reduced echelon form* there is a unique matrix, rref(A), that you must produce, but the row operations that one student uses to get from A to rref(A) will probably not be the same as the row operations used by another student to get from A to rref(A). There is *no best way* to proceed in doing this and therefore no guiding rule I can give you to do this. Experience and practice will teach you how to minimize the number and complexity of the operations and how to keep the intermediate matrices reasonably "nice". I often don't swap the order of the rows until the very end. I begin by trying to get zeroes in the columns, i.e., all zeroes in some columns, and only one non-zero entry in other columns, and I don't care which order of columns I do this for.

3. An example

Doing elementary row operations by hand to put a matrix in row-reduced echelon form can be a pretty tedious task. It is an ideal task for a computer! But, let's take a deep breath and plunge in. Suppose the system is

MORE TO DO

4. You already did this in high school

You probably had to solve systems of equations like

$$\begin{aligned} x_1 + x_2 + x_3 &= 3 \\ 2x_1 + x_2 - x_3 &= 4 \\ 4x_1 + 3x_2 - 2x_3 &= 13 \end{aligned}$$

in high school. (This is the system in chapter 5.8.) I want to persuade you that the approach you used then is pretty much identical to the method we are using here, i.e., putting the matrix $(A \,|\, \underline{b})$ in row-reduced echelon form.

A typical high school approach to the problem is to add the first two equations (to eliminate the x_3 variable) and to add twice the first equation to the third equation to get another equation without an x_3 term. The two new equations are

$$\begin{aligned} 3x_1 + 2x_2 &= 7 \\ 6x_1 + 5x_2 &= 19 \end{aligned}$$

Now subtract twice the first of these two equations from the second to get $x_2 = 5$. Substitute this into $3x_1 + 2x_2 = 7$ and get $x_1 = -1$. Finally, from the first of the original equations, $x_1 + x_2 + x_3 = 3$, we obtain $x_3 = -1$. Thus, the system has a unique solution, $(x_1, x_2, x_3) = (-1, 5, -1)$.

Let's rewrite what we did in terms of row operations. The first two operations we performed are, in matrix notation,

$$(A \,|\, \underline{b}) = \begin{pmatrix} 1 & 1 & 1 & | & 3 \\ 2 & 1 & -1 & | & 4 \\ 4 & 1 & 1 & | & 13 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1 & 1 & | & 3 \\ 3 & 2 & 0 & | & 7 \\ 6 & 5 & 0 & | & 19 \end{pmatrix}.$$

Then we subtracted twice the second row from the third to get

$$\begin{pmatrix} 1 & 1 & 1 & | & 3 \\ 3 & 2 & 0 & | & 7 \\ 0 & 1 & 0 & | & 5 \end{pmatrix}.$$

The last row tells us that $x_2 = 5$. Above, we substituted $x_2 = 5$ into $3x_1 + 2x_2 = 7$ and solved for x_1. That is the same as subtracting twice the third row from the second, then dividing by three, i.e.,

$$\begin{pmatrix} 1 & 1 & 1 & | & 3 \\ 3 & 2 & 0 & | & 7 \\ 0 & 1 & 0 & | & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1 & 1 & | & 3 \\ 3 & 0 & 0 & | & -3 \\ 0 & 1 & 0 & | & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1 & 1 & | & 3 \\ 1 & 0 & 0 & | & -1 \\ 0 & 1 & 0 & | & 5 \end{pmatrix}$$

which gives $x_1 = -1$. Now subtract the second and third rows from the top row to get

$$\begin{pmatrix} 1 & 1 & 1 & | & 3 \\ 1 & 0 & 0 & | & -1 \\ 0 & 1 & 0 & | & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 0 & 1 & | & -1 \\ 1 & 0 & 0 & | & -1 \\ 0 & 1 & 0 & | & 5 \end{pmatrix}$$

which gives $x_3 = -1$. Admittedly the last matrix is not in row-reduced echelon form because the left-most ones do not proceed downwards in the southeast direction, but that is fixed by one more row operation, moving the top row to the bottom, i.e.,

$$\begin{pmatrix} 0 & 0 & 1 & \mid & -1 \\ 1 & 0 & 0 & \mid & -1 \\ 0 & 1 & 0 & \mid & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & \mid & -1 \\ 0 & 1 & 0 & \mid & 5 \\ 0 & 0 & 1 & \mid & -1 \end{pmatrix}.$$

5. The rank of a matrix

The rank of an $m \times n$ matrix A is the number

$$\text{rank}(A) := \text{ the number of non-zero rows in } \mathsf{rref}(A).$$

5.1. A very important remark about rank. Later on we will see that the rank of A is equal to the dimension of the range of A. After proving that equality it will be important to keep in mind these two different interpretations of $\text{rank}(A)$, i.e., as the number of non-zero rows in $\mathsf{rref}(A)$ and as the dimension of the range of A.

5.2. Remark. If $\mathsf{rref}(A) = \mathsf{rref}(B)$, then $\text{rank}(A) = \text{rank}(B)$.

PROPOSITION 5.1. *If A is an $m \times n$ matrix, then*

$$\text{rank}(A) \le m$$

and

$$\text{rank}(A) \le n.$$

Proof. The rank of A is at most the number of rows in $\mathsf{rref}(A)$. But $\mathsf{rref}(A)$ and A have the same size so $\text{rank}(A) \le m$.

Each non-zero row of $\mathsf{rref}(A)$ has a left-most 1 in it so the rank of A is the number of left-most 1s. But a column of $\mathsf{rref}(A)$ contains at most one left-most 1, so the rank of A is at most the number of columns in A, i.e., $\text{rank}(A) \le n$. □

PROPOSITION 5.2. *Let A be an $n \times n$ matrix. Then*

1. $\text{rank}(A) = n$ *if and only if* $\mathsf{rref}(A) = I$*, the identity matrix;*
2. *if* $\text{rank}(A) < n$*, then* $\mathsf{rref}(A)$ *has a row of zeroes.*

Proof. (1) If $\text{rank}(A) = n$, then $\mathsf{rref}(A)$ has n non-zero rows and each of those rows has a left-most 1, i.e., every row of $\mathsf{rref}(A)$ contains a left-most 1. Suppose the left-most 1 in row i appear in column c_i. The 1s move at least one column to the right each time we go from each row to the one below it so

$$1 \le c_1 < c_2 < \cdots < c_n \le n.$$

It follows that $c_1 = 1$, $c_2 = 2, \ldots, c_n = n$. In other words, the left-most 1 in row j appears in column j; i.e., all the left-most 1s lie on the diagonal. Therefore $\mathsf{rref}(A) = I$.

(2) This is clear. □

6. Inconsistent systems

A system of linear equations is inconsistent if it has no solution (section 6). If a row of the form

$$(0\,0\,\cdots\,0 \mid b) \tag{6-1}$$

with $b \neq 0$ appears after performing some row operations on the augmented matrix $(A \mid \underline{b})$, then the system is inconsistent because row (6-1) says the equation $0x_1 + \cdots + 0x_n = b$ appears in a system that is equivalent to the original system of equations, and it is utterly clear that there is no solution to the equation $0x_1 + \cdots + 0x_n = b$ when $b \neq 0$, and therefore no solution to the original system of equations.

7. Consistent systems

Suppose $A\underline{x} = \underline{b}$ is a consistent $m \times n$ system of linear equations .

- Form the augmented matrix $(A \,|\, \underline{b})$.
- Perform elementary row operations on $(A \,|\, \underline{b})$ until you obtain $(\underline{\mathsf{rref}}(A) \,|\, \underline{d})$.
- If column j contains the left-most 1 that appears in some row of $\underline{\mathsf{rref}}(A)$ we call x_j a <u>dependent variable</u>.
- The other x_js are called <u>independent</u> or <u>free variables</u>.
- The number of dependent variables equals $\operatorname{rank}(A)$ and, because A has n columns, the number of independent/free variables is $n - \operatorname{rank}(A)$.
- All solutions are now obtained by allowing each independent variable to take any value and the dependent variables are now completely determined by the equations corresponding to $(\underline{\mathsf{rref}}(A) \mid \underline{d})$ and the values of the independent/free variables.

An example will clarify my meaning. If

$$(\underline{\mathsf{rref}}(A) \mid \underline{d}) \;=\; \begin{pmatrix} 1 & 0 & 2 & 0 & 0 & 3 & 4 & \mid & 1 \\ 0 & 1 & 3 & 0 & 0 & 4 & 0 & \mid & 3 \\ 0 & 0 & 0 & 1 & 0 & -2 & 1 & \mid & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & -2 & \mid & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mid & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mid & 0 \end{pmatrix} \tag{7-1}$$

the variables are x_1, x_2, x_4, and x_5. The independent/free variables x_3, x_6, and x_7, may take any values and then the dependent variables are determined by the equations

$$\begin{aligned}
x_1 &= 1 - 2x_3 - 3x_6 - 4x_7 \\
x_2 &= 3 - 3x_3 - 4x_6 \\
x_3 &= \phantom{3 - {}} x_3 \\
x_4 &= \phantom{3 - 3x_3 - {}} 2x_6 + x_7 \\
x_5 &= 5 \phantom{{} - 3x_3} - x_6 + 2x_7 \\
x_6 &= \phantom{3 - 3x_3 - {}} x_6 \\
x_7 &= \phantom{3 - 3x_3 - 4x_6 + {}} x_7
\end{aligned}$$

In other words, the set of all solutions to this system is given by

$$\underline{x} = \begin{pmatrix} 1 - 2x_3 - 3x_6 - 4x_7 \\ 3 - 3x_3 - 4x_6 \\ x_3 \\ 2x_6 + x_7 \\ 5 - x_6 + 2x_7 \\ x_6 \\ x_7 \end{pmatrix}$$

or, equivalently,

$$\underline{x} = \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \\ 5 \\ 0 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} -2 \\ -3 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_6 \begin{pmatrix} -3 \\ -4 \\ 0 \\ 2 \\ -1 \\ 1 \\ 0 \end{pmatrix} + x_7 \begin{pmatrix} -4 \\ 0 \\ 0 \\ 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} \tag{7-2}$$

as x_3, x_6, x_7 range over all real numbers. We call (7-2) the <u>general solution</u> to the system.[1]

7.1. Particular vs. general solutions. If we make a particular choice of x_3, x_6, and x_7, we call the resulting $\underline{x}$ a <u>particular solution</u> to the system.

[1]You will later see that the vectors obtained from the three right-most terms of (7-2) as x_3, x_6, and x_7, vary over all of $\mathbb{R}$ form a subspace, namely the null space of A. Thus (7-2) is telling us that the solutions to $A\underline{x} = \underline{b}$ belong to a translate of the null space of A by a particular solution of the equation, the particular solution being the term immediately to the right of the equal sign in (7-2). See chapter 3 and Proposition 3.1 below for more about this.

For example, when $(x_3, x_6, x_7) = (0, 0, 0)$ we obtain the *particular* solution

$$\begin{pmatrix} 1 \\ 3 \\ 0 \\ 5 \\ 0 \\ 0 \end{pmatrix}.$$

Notice that

$$\begin{pmatrix} -2 \\ -3 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} -3 \\ -4 \\ 0 \\ 2 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} -4 \\ 0 \\ 0 \\ 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}$$

are solutions to the homogeneous system $A\underline{x} = 0$. The general solution is obtained by taking one particular solution, say $\underline{u}$, perhaps that given by setting all the independent variables to zero, and adding to it solutions to the homogeneous equation $A\underline{x} = 0$. That is exactly what Proposition 8.1 below says.

The number of independent variables, in this case 3, which is $n-\mathrm{rank}(A)$, gives a measure of "how many" solutions there are to the equation $A\underline{x} = \underline{b}$. The fact that x_3, x_6, and x_7, can be any real numbers says there are 3 degrees of freedom for the solution space. Later we will introduce more formal language which will allow us to say that the space of solutions is a translate of a 3-dimensional subspace of $\mathbb{R}^7$. That 3-dimensional subspace is called the *null space* of A. You will understand this paragraph later. I hope you read it again after you have been introduced to the null space,

The discussion in chapter 3 is also relevant to what we have discussed in this chapter. In the language of chapter 3, the solutions to $A\underline{x} = \underline{b}$ are obtained by translating the solutions to $A\underline{x}$, i.e., the null space of A, by a particular solution to $A\underline{x} = \underline{b}$.

Sections 8.2 and 8.4 are also related to the issue of particular versus general solutions. Section 8.2 discusses the particular solution $(-1, 1)$ to the equation $2x + 3y = 1$ and the general solution $(-1, 1) + \lambda(3, -2)$ where λ runs over all real numbers. As λ runs over all real numbers the points $\lambda(3, -2)$ give all the points on the line $2x + 3y = 0$.

8. Parametric equations for lines and planes

You should review the material about parametric equations for curves and surfaces that you encountered in a course prior to this. The only curves and surfaces relevant to this course are lines and planes. These have particularly simple parametric descriptions.

For example, the line $2x - 3y = 1$ in the plane consists of all points of the form $(3t + 2, 2t + 1)$, $t \in \mathbb{R}$. Another way of saying this is the line is given by the equations

$$\begin{aligned} x &= 3t + 2 \\ y &= 2t + 1. \end{aligned}$$

In other words, t is allowed to be any real number, each choice of t gives exactly one point in the plane, and the totality of all points obtained is exactly all points that lie on the line $2x - 3y = 1$. Another way of looking at this is that the points in the plane that are solutions to the equation $2x - 3y = 1$ are the points on the line. For example, when $t = 0$ we get the solution $x = 2$ and $y = 1$ or, equivalently, the point $(2, 1)$; when $t = -5$ we get the solution $(x, y) = (-13, -9)$; when $t = 4$ we get the solution $(x, y) = (14, 9)$; and so on.

In a similar fashion, the points on the plane $2x - y - z = 3$ are given by the parametric equations

$$\begin{aligned} x &= \frac{1}{2}(3 + s + t) \\ y &= s \\ z &= t \end{aligned}$$

or, if you prefer,

$$\begin{aligned} x &= \frac{3}{2} + s + t \\ y &= 2s \\ z &= 2t. \end{aligned}$$

As (s, t) ranges over all points of $\mathbb{R}^2$, i.e., as s and t range over $\mathbb{R}$, the points $(\frac{3}{2} + s + t, 2s, 2t)$ are all points on the plane $2x - y - z = 3$.

In a similar fashion, the points on the line that is the intersection of the planes $2x-y-z = 3$ and $x+y+z = 4$ are given by the parametric equations

$$\begin{aligned} x &= \\ y &= \\ z &= \end{aligned}$$

9. The importance of rank

We continue to discuss a consistent $m \times n$ system $A\underline{x} = \underline{b}$.

- We have seen that $\operatorname{rank}(A) \leq m$ and $\operatorname{rank}(A) \leq n$ (Proposition 5.1) and that the number of independent variables is $n - \operatorname{rank}(A)$.
- If $\operatorname{rank}(A) = n$ there are no independent variables, so the system has a *unique solution*.
- If $\operatorname{rank}(A) < n$ there is at least one independent variable, so the system has *infinitely many solutions*.

THEOREM 9.1. *Let A be an $n \times n$ matrix and consider the equation $A\underline{x} = \underline{b}$. If $\text{rank}(A) = n$, and the elementary row operations on the augmented matrix $(A \mid \underline{b})$ produce $(\underline{\mathsf{rref}}(A) \mid \underline{d}) = (I \mid \underline{d})$ where I is the identity matrix, then $\underline{d}$ is the unique matrix such that $A\underline{d} = \underline{b}$.*

Proof. By Proposition 5.2, $\underline{\mathsf{rref}}(A) = I$. Hence the elementary row operations change $(A \mid \underline{b})$ to $(I \mid \underline{d})$ where I is the identity matrix. Therefore the equations $A\underline{x} = \underline{b}$ and $I\underline{x} = \underline{d}$ have the same set of solutions. But $I\underline{x} = \underline{x}$ so the only solution to $I\underline{x} = \underline{d}$ is $\underline{x} = \underline{d}$. □

PROPOSITION 9.2. *Let $A\underline{x} = \underline{0}$ be an $m \times n$ system of homogeneous linear equations. If $m < n$, the system has a non-trivial solution.*

Proof. By Proposition 5.1, $\text{rank}(A) \leq m$. The number of independent variables for the equation $A\underline{x} = \underline{0}$ is $n - \text{rank}(A) \geq n - m \geq 1$. Hence there are infinitely many solutions by the remarks in chapter 9. □

A shorter, simpler version of Proposition 9.2 is the following.

COROLLARY 9.3. *A homogeneous system of equations with more unknowns than equations always has a non-trivial solution.*

9.1. A simple proof of Corollary 9.3. Let $A\underline{x} = \underline{0}$ be a homogeneous system of m equations in n unknowns and suppose $m < n$. Since $\underline{\mathsf{rref}}(A)$ has more columns than rows there will be a column that does not have a leading 1. Hence there will be at least one independent variable. That variable can be anything; in particular, it can be given a non-zero value which leads to a non-trivial solution.

10. The word "solution"

A midterm contained the following question: *Suppose $\underline{u}$ is a solution to the equation $A\underline{x} = \underline{b}$ and that $\underline{v}$ is a solution to the equation $A\underline{x} = \underline{0}$. Write out a single equation, involving several steps, that shows $\underline{u} + \underline{v}$ is a solution to the equation $A\underline{x} = \underline{b}$.*

The correct answer is

$$A(\underline{u} + \underline{v}) = A\underline{u} + A\underline{v} = \underline{b} + \underline{0} = \underline{b}.$$

Done! I talked to some students who could not answer the question. They did not understand the meaning of the phrase *"$\underline{u}$ is a solution to the equation $A\underline{x} = \underline{b}$"*. The meaning is that $A\underline{u} = \underline{b}$. In principle, it is no more complicated than the statement *"2 is a solution to the equation $x^2 + 3x = 10$"* which means that when you plug in 2 for x you obtain the true statement $4 + 6 = 10$.

11. Elementary matrices

The $n \times n$ identity matrix, which is denoted by I_n, or just I when n is clear from the context, is the $n \times n$ matrix having each entry on its diagonal equal to 1 and 0 elsewhere. For example, the 4×4 identity matrix is

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

An elementary matrix is a matrix that is obtained by performing a *single* elementary row operation on an identity matrix. For example, if we switch rows 2 and 4 of I_4 we obtain the elementary matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

If we multiply the third row of I_4 by a non-zero number c we get the elementary matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

If we replace the first row of I_4 by itself $+$ c times the second row we get the elementary matrix

$$\begin{pmatrix} 1 & c & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

THEOREM 11.1. *Let E be the elementary matrix obtained by performing an elementary row operation on the $m \times m$ identity matrix. If we perform the same elementary row operation on an $m \times n$ matrix A the resulting matrix is equal to EA.*

We won't prove this. The proof is easy but looks a little technical because of the notation. Let's convince ourselves that the theorem is plausible by looking at the three elementary matrices above and the matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 1 & 1 & 1 \\ -1 & 0 & 2 \end{pmatrix}.$$

Now carry out the following three multiplications and check your answers:

$$\begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\\1&1&1\\-1&0&2\end{pmatrix}=\begin{pmatrix}1&2&3\\-1&0&2\\1&1&1\\3&2&1\end{pmatrix};$$

and

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&c&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\\1&1&1\\-1&0&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\\c&c&c\\-1&0&2\end{pmatrix};$$

and

$$\begin{pmatrix}1&c&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\\1&1&1\\-1&0&2\end{pmatrix}=\begin{pmatrix}1+3c&2+2c&3+c\\3&2&1\\1&1&1\\-1&0&2\end{pmatrix}.$$

THEOREM 11.2. *The following conditions on an $n \times n$ matrix A are equivalent:*

(1) $\underline{\mathsf{rref}}(A) = I_n$*;*
(2) *A is a product of elementary matrices;*
(3) *A is invertible.*

Proof. (1) $\Longrightarrow$ (2) Suppose $\underline{\mathsf{rref}}(A) = I_n$. Then I_n can be obtained from A by a sequence of elementary row operations. Therefore A can be obtained from I_n by a sequence of elementary row operations. By Theorem 11.1, the result of each of those elementary row operations is the same as the result obtained by multiplying on the left by an elementary matrix. Therefore a sequence of elementary row operations on I_n produces a matrix of the form $E_k E_{k-1} \cdots E_1$ where each E_j is an elementary matrix, i.e., $A = E_k E_{k-1} \cdots E_1$ for a suitable collection of elementary matrices $E_1, \ldots, E_k$.

(2) $\Longrightarrow$ (3)

(3) $\Longrightarrow$ (1) □

CHAPTER 6

The Vector space $\mathbb{R}^n$

We write $\mathbb{R}^n$ for the set of all $n \times 1$ column vectors. Elements of $\mathbb{R}^n$ are called vectors or points in $\mathbb{R}^n$. We call them points to encourage you to think of $\mathbb{R}^n$ as a geometric object, a space, in the same sort of way as you think of the number line $\mathbb{R}$, the case $n = 1$, and the plane $\mathbb{R}^2$, in which the points of $\mathbb{R}^2$ are labelled by row vectors (a, b) after choosing a coordinate system, and 3-space $\mathbb{R}^3$, the space in which we live or, when you include time, $\mathbb{R}^4$.

Solutions to an $m \times n$ system $A\underline{x} = \underline{b}$ of linear equations are therefore points in $\mathbb{R}^n$. The totality of all solutions is a certain subset of $\mathbb{R}^n$. As we said just after Proposition 6.1, the set of solutions has a linear nature: if p and q are solutions to $A\underline{x} = \underline{b}$ so are all points on the line $\overline{pq}$.

1. Arithmetic in $\mathbb{R}^n$

Because the elements of $\mathbb{R}^n$ are matrices, we can add them to one another, and we can multiply them by scalars (numbers). These operations have the following properties which we have been using for some time now:

(1) if $\underline{u}, \underline{v} \in \mathbb{R}^n$ so is $\underline{u} + \underline{v}$;
(2) if $\underline{u} \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$, then $\lambda\underline{u} \in \mathbb{R}^n$;
(3) $\underline{u} + \underline{v} = \underline{v} + \underline{u}$ for all $\underline{u}, \underline{v} \in \mathbb{R}^n$;
(4) $(\underline{u} + \underline{v}) + \underline{w} = \underline{u} + (\underline{v} + \underline{w})$ for all $\underline{u}, \underline{v}, \underline{w} \in \mathbb{R}^n$;
(5) there is an element $0 \in \mathbb{R}^n$ having the property that $0 + \underline{u} = \underline{u}$ for all $\underline{u} \in \mathbb{R}^n$;[1]
(6) if $\underline{u} \in \mathbb{R}^n$ there is an element $\underline{u}' \in \mathbb{R}^n$ such that $\underline{u} + \underline{u}' = 0$;[2]
(7) $(\alpha\beta)\underline{u} = \alpha(\beta\underline{u})$ for all $\alpha, \beta \in \mathbb{R}$ and all $\underline{u} \in \mathbb{R}^n$;
(8) $\lambda(\underline{u} + \underline{v}) = \lambda\underline{u} + \lambda\underline{v}$ for all $\lambda \in \mathbb{R}$ and all $\underline{u}, \underline{v} \in \mathbb{R}^n$;
(9) $(\alpha + \beta)\underline{u} = \alpha\underline{u} + \beta\underline{u}$ for all $\alpha, \beta \in \mathbb{R}$ and all $\underline{u} \in \mathbb{R}^n$;
(10) $1.\underline{u} = \underline{u}$ for all $\underline{u} \in \mathbb{R}^n$.

[1] It is important to observe that there is only one element with this property—if $0' \in \mathbb{R}^n$ has the property that $0' + \underline{u} = \underline{u}$ for all $\underline{u} \in \mathbb{R}^n$, then $0 = 0' + 0 = 0 + 0' = 0'$ where the first equality holds because $0' + \underline{u} = \underline{u}$ for all $\underline{u}$, the second equality holds because of the commutativity property in (3), and the third equality holds because $0 + \underline{u} = \underline{u}$ for all $\underline{u}$.

[2] We denote $\underline{u}'$ by $-\underline{u}$ after showing that it is unique—it is unique because if $\underline{u} + \underline{u}' = \underline{u} + \underline{u}'' = 0$, then

$$\underline{u}' = \underline{u}' + 0 = \underline{u}' + (\underline{u} + \underline{u}'') = (\underline{u}' + \underline{u}) + \underline{u}'' = (\underline{u} + \underline{u}') + \underline{u}'' = 0 + \underline{u}'' = \underline{u}''.$$

2. The standard basis for $\mathbb{R}^n$

The vectors

$$\begin{aligned}
\underline{e}_1 &:= (1, 0, \dots, 0, 0), \\
\underline{e}_2 &:= (0, 1, 0, \dots, 0), \\
\vdots &\quad \vdots \\
\underline{e}_n &:= (0, 0, \dots, 0, 1)
\end{aligned}$$

in $\mathbb{R}^n$ will appear often from now on. We call $\{\underline{e}_1, \dots, \underline{e}_n\}$ the standard basis for $\mathbb{R}^n$. The notion of a basis is defined and discussed in chapter 10 below. From now on the symbols

$$\underline{e}_1, \dots, \underline{e}_n$$

will be reserved for the special vectors just defined. There is some potential for ambiguity since we will use $\underline{e}_1$ to denote the vector $(1, 0)$ in $\mathbb{R}^2$, the vector $(1, 0, 0)$ in $\mathbb{R}^3$, the vector $(1, 0, 0, 0)$ in $\mathbb{R}^4$, etc. Likewise for the other $\underline{e}_i$s. It will usually be clear from the context which one we mean.

One reason for the importance of the $\underline{e}_j$s is that

$$(a_1, \dots, \alpha_n) = a_1\underline{e}_1 + a_2\underline{e}_2 + \cdots + a_n\underline{e}_n.$$

In other words, every vector in $\mathbb{R}^n$ can be written as a sum of multiples of the $\underline{e}_j$s in a unique way.

3. Linear combinations and linear span

A linear combination of vectors $\underline{v}_1, \dots, \underline{v}_n$ in $\mathbb{R}^m$ is a vector that can be written as

$$a_1\underline{v}_1 + \cdots + a_n\underline{v}_n$$

for some numbers $a_1, \dots, a_n \in \mathbb{R}$. We say the linear combination is non-trivial if at least one of the a_is is non-zero.

The set of all linear combinations of $\underline{v}_1, \dots, \underline{v}_n$ is called the linear span of $\underline{v}_1, \dots, \underline{v}_n$ and denoted

$$\mathrm{Sp}(\underline{v}_1, \dots, \underline{v}_n) \qquad \text{or} \qquad \langle \underline{v}_1, \dots, \underline{v}_n \rangle.$$

For example, the linear span of $\underline{e}_1, \dots, \underline{e}_n$ is $\mathbb{R}^n$ itself: if $(a_1, a_2, \dots, a_n)$ is any vector in $\mathbb{R}^n$, then

$$(a_1, a_2, \dots, a_n) = a_1\underline{e}_1 + a_2\underline{e}_2 + \cdots + a_n\underline{e}_n.$$

3.1. Note that the linear span of $\underline{v}_1, \dots, \underline{v}_n$ has the following properties:

(1) $0 \in \mathrm{Sp}(\underline{v}_1, \dots, \underline{v}_n)$;
(2) if $\underline{u}$ and $\underline{v}$ are in $\mathrm{Sp}(\underline{v}_1, \dots, \underline{v}_n)$ so are $\underline{u} + \underline{v}$;
(3) if $a \in \mathbb{R}$ and $\underline{v} \in \mathrm{Sp}(\underline{v}_1, \dots, \underline{v}_n)$ so is $a\underline{v}$.

You should check these three properties hold. We will return to them later on – they are the defining properties of a subspace of $\mathbb{R}^n$ (see chapter 1).

PROPOSITION 3.1. *Let A be any $m \times n$ matrix and $\underline{x} \in \mathbb{R}^n$. Then $A\underline{x}$ is a linear combination of the columns of A. Explicitly,*

$$A\underline{x} = x_1\underline{A}_1 + \cdots + x_n\underline{A}_n \tag{3-1}$$

where $\underline{A}_j$ denotes the j^{th} column of A.

Proof. Let's write $A = (a_{ij})$ and $\underline{x} = (x_1, \ldots, x_n)^T$. Then

$$\begin{aligned}
x_1\underline{A}_1 + \cdots + x_n\underline{A}_n &= x_1 \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} + x_2 \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} \\
&= \begin{pmatrix} a_{11}x_1 \\ a_{21}x_1 \\ \vdots \\ a_{m1}x_1 \end{pmatrix} + \begin{pmatrix} a_{12}x_2 \\ a_{22}x_2 \\ \vdots \\ a_{m2}x_2 \end{pmatrix} + \cdots + \begin{pmatrix} a_{1n}x_n \\ a_{2n}x_n \\ \vdots \\ a_{mn}x_n \end{pmatrix} \\
&= \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \qquad\qquad\qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix} \\
&= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \\
&= A\underline{x}.
\end{aligned}$$

The above calculation made use of scalar multiplication (6.11): if $r \in \mathbb{R}$ and B is a matrix, then rB is the matrix whose ij^{th} entry is rB_{ij}; since r and B_{ij} are numbers $rB_{ij} = B_{ij}r$. □

A useful way of stating Proposition 3.1 is that for a fixed A the set of values $A\underline{x}$ takes as $\underline{x}$ ranges over all of $\mathbb{R}^n$ is $\operatorname{Sp}(\underline{A}_1, \ldots, \underline{A}_n)$, the linear span of the columns of A. Therefore, if $\underline{b} \in \mathbb{R}^m$, the equation $A\underline{x} = \underline{b}$ has a solution if and only if $\underline{b} \in \operatorname{Sp}(\underline{A}_1, \ldots, \underline{A}_n)$. This is important enough to state as a separate result.

COROLLARY 3.2. *Let A be an $m \times n$ matrix and $\underline{b} \in \mathbb{R}^m$. The equation $A\underline{x} = \underline{b}$ has a solution if and only if $\underline{b}$ is a linear combination of the columns of A.*

4. Some infinite dimensional vector spaces

You already know some infinite dimensional vector spaces. Perhaps the most familiar one is the set of all polynomials with real coefficients. We denote it by $\mathbb{R}[x]$.

4.1. Polynomials. At high school one considers polynomial functions of arbitrary degree. If $f(x)$ and $g(x)$ are polynomials so is their sum $f(x)+g(x)$; if $\lambda \in \mathbb{R}$ the function $\lambda f(x)$ is a polynomial whenever f is; the zero polynomial has the wonderful property that $f(x)+0 = 0+f(x) = f(x)$. Of course, other properties like associativity and commutativity of addition hold, and the distributive rules $\lambda(f(x)+g(x) = \lambda f(x) + \lambda g(x)$ and $\lambda + \mu)f(x) = \lambda f(x)+\mu f(x)$ hold. Every polynomial is a <u>finite</u> linear combination of the powers $1, x, x^2, \ldots$ of x. The powers of x are linearly independent because the only way $a_0 + a_1 x + \cdots + a_n x^n$ can be the zero polynomial is if all the a_is are zero. The powers of x form a basis for the space of polynomials. Thus $\mathbb{R}[x]$ is an infinite dimensional vector space.

4.2. Other spaces of functions. One need not restrict attention to polynomials. Let $C^1(\mathbb{R})$ denote the set of all differentiable functions $f : \mathbb{R} \to \mathbb{R}$. This is also a vector space: you can add 'em, multiply 'em by scalars, etc, and the usual associative, commutative and distributive rules apply. Likewise, $C(\mathbb{R})$, the set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$ is a vector space.

MORE to say...

4.3. Infinite sequences. The set of all infinite sequences $\underline{s} = (s_0, s_1, \ldots)$ of real numbers is a vector space with respect to the following addition and scalar multiplication:

$$(s_0, s_1, \ldots)+(t_0, t_1, \ldots) = (s_0+t_0, s_1+t_1, \ldots), \qquad \lambda(t_0, t_1, \ldots) = (\lambda t_0, \lambda t_1, \ldots).$$

CHAPTER 7

Subspaces

Let W denote the set of solutions to a system of homogeneous equations $A\underline{x} = \underline{0}$. It is easy to see that W has the following properties: (a) $0 \in W$; (b) if $\underline{u}$ and $\underline{v}$ are in W so is $\underline{u} + \underline{v}$; (c) if $\underline{u} \in W$ and $\lambda \in \mathbb{R}$, then $\lambda\underline{u} \in W$. Subsets of $\mathbb{R}^n$ having this property are called subspaces and are of particular importance in all aspects of linear algebra. It is also important to know that every subspace *is* the set of solutions to some system of homogeneous equations.

Another important way in which subspaces turn up is that the linear span of a set of vectors is a subspace.

Now we turn to the official definition.

1. The definition and examples

A subset W of $\mathbb{R}^n$ is called a subspace if

(1) $0 \in W$, and
(2) $\underline{u} + \underline{v} \in W$ for all $\underline{u}, \underline{v} \in W$, and
(3) $\lambda\underline{u} \in W$ for all $\lambda \in \mathbb{R}$ and all $\underline{u} \in W$.

The book gives a different definition but then proves that a subset W of $\mathbb{R}^n$ is a subspace if and only if it satisfies these three conditions. We will use our definition not the book's.

We now give numerous examples.

1.1. The zero subspace. The set $\{\underline{0}\}$ consisting of the zero vector in $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$. We call it the zero subspace. It is also common to call it the *trivial subspace*.

1.2. $\mathbb{R}^n$ itself is a subspace. This is clear.

1.3. The null space and range of a matrix. Let A be an $m \times n$ matrix. The null space of A is

$$\mathcal{N}(A) := \{\underline{x} \mid A\underline{x} = \underline{0}\}.$$

The range of A is

$$\mathcal{R}(A) := \{A\underline{x} \mid \underline{x} \in \mathbb{R}^n\}.$$

PROPOSITION 1.1. *Let A be an $m \times n$ matrix. Then $\mathcal{N}(A)$ is a subspace of $\mathbb{R}^n$ and $\mathcal{R}(A)$ is a subspace of $\mathbb{R}^m$.*

Proof. First, we consider $\mathcal{N}(A)$. Certainly $\underline{0} \in \mathcal{N}(A)$ because $A\underline{0} = \underline{0}$. now suppose that $\underline{u}$ and $\underline{v}$ belong to $\mathcal{N}(A)$ and that $a \in \mathbb{R}$. Then

$$A(\underline{u} + \underline{v}) = A\underline{u} + A\underline{v} = \underline{0} + \underline{0} = \underline{0}$$

and

$$A(a\underline{u}) = aA\underline{u} = a\underline{0} = \underline{0}$$

so both $\underline{u} + \underline{v}$ and $a\underline{u}$ belong to $\mathcal{N}(A)$. Hence $\mathcal{N}(A)$ is a subspace of $\mathbb{R}^n$.

Now consider $\mathcal{R}(A)$. Certainly $\underline{0} \in \mathcal{R}(A)$ because $A\underline{0} = \underline{0}$. now suppose that $\underline{u}$ and $\underline{v}$ belong to $\mathcal{R}(A)$ and that $a \in \mathbb{R}$. Then there exist $\underline{x}$ and $\underline{y}$ in $\mathbb{R}^n$ such that $\underline{u} = A\underline{x}$ and $\underline{v} = A\underline{y}$. Therefore

$$\underline{u} + \underline{v} = A\underline{x} + A\underline{y} = A(\underline{x} + \underline{y})$$

and

$$a\underline{u} = aA\underline{x} = Aa\underline{x}$$

so both $\underline{u} + \underline{v}$ and $a\underline{u}$ belong to $\mathcal{R}(A)$. Hence $\mathcal{R}(A)$ is a subspace of $\mathbb{R}^m$. □

It is sometimes helpful to think of $\mathcal{R}(A)$ as all "multiples" of A where a "multiple of A" means a vector of the form $A\underline{x}$. It is clear that a multiple of AB is a multiple of A; explicitly, $AB\underline{x} = A(B\underline{x})$. It follows that

$$\mathcal{R}(AB) \subseteq \mathcal{R}(A).$$

The following analogy might be helpful: every multiple of 6 is a multiple of 2 because $6 = 2 \times 3$. In set-theoretic notation

$$\{6x \mid x \in \mathbb{Z}\} \subseteq \{2x \mid x \in \mathbb{Z}\}.$$

Similarly,

$$\{AB\underline{x} \mid \underline{x} \in \mathbb{R}^n\}. \subseteq \{A\underline{x} \mid \underline{x} \in \mathbb{R}^n\}$$

which is the statement that $\mathcal{R}(AB) \subseteq \mathcal{R}(A)$.

There is a similar inclusion for null spaces. If $B\underline{x} = 0$, then $AB\underline{x} = 0$, so

$$\mathcal{N}(B) \subseteq \mathcal{N}(AB).$$

1.4. Lines through the origin are subspaces. Let $\underline{u} \in \mathbb{R}^n$. We introduce the notation

$$\mathbb{R}\underline{u} := \{\lambda\underline{u} \mid \lambda \in \mathbb{R}\}$$

for the set of all real multiples of $\underline{u}$. We call $\mathbb{R}\underline{u}$ a <u>line</u> if $\underline{u} \neq 0$. If $\underline{u} = 0$, then $\mathbb{R}\underline{u}$ is the zero subspace.

LEMMA 1.2. *Let $\underline{u} \in \mathbb{R}^n$. Then $\mathbb{R}\underline{u}$ is a subspace of $\mathbb{R}^n$.*

Proof. The zero vector is a multiple of $\underline{u}$ so is in $\mathbb{R}\underline{u}$. A sum of two multiples of $\underline{u}$ is again a multiple of $\underline{u}$, and a multiple of a multiple of $\underline{u}$ is again a multiple of $\underline{u}$. □

1.5. Planes through the origin are subspaces. Suppose that $\{\underline{u}, \underline{v}\}$ is linearly independent subset of $\mathbb{R}^n$. We introduce the notation

$$\mathbb{R}\underline{u} + \mathbb{R}\underline{v} := \{a\underline{u} + b\underline{v} \mid a, b \in \mathbb{R}\}.$$

We call $\mathbb{R}\underline{u} + \mathbb{R}\underline{v}$ the plane through $\underline{u}$ and $\underline{v}$.

LEMMA 1.3. *$\mathbb{R}\underline{u} + \mathbb{R}\underline{v}$ is a subspace of $\mathbb{R}^n$.*

Proof. Exercise. It is also a special case of Proposition 1.4 below. □

You already know something about the geometry of $\mathbb{R}^3$. For example, if you are given three points in $\mathbb{R}^3$ that do not lie on a single line, then there is a unique plane containing them. In the previous paragraph the hypothesis that $\{\underline{u}, \underline{v}\}$ is linearly independent implies that 0, $\underline{u}$, and $\underline{v}$, do not lie on a single line. (In fact, the linear independence is equivalent to that statement–why?) The unique plane containing 0, $\underline{u}$, and $\underline{v}$ is $\mathbb{R}\underline{u} + \mathbb{R}\underline{v}$.

You also know, in $\mathbb{R}^3$, that given two lines meeting at a point, there is a unique plane that contains those lines. Here, the lines $\mathbb{R}\underline{u}$ and $\mathbb{R}\underline{v}$ meet at 0, and $\mathbb{R}\underline{u} + \mathbb{R}\underline{v}$ is the unique plane containing them.

1.6. The linear span of any set of vectors is a subspace.

PROPOSITION 1.4. *If $\underline{v}_1, \ldots, \underline{v}_d$ are vectors in $\mathbb{R}^n$, then their linear span $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_d)$ is a subspace of $\mathbb{R}^n$. It is the smallest subspace of $\mathbb{R}^n$ containing $\underline{v}_1, \ldots, \underline{v}_d$.*

Proof. We leave the reader to show that $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_d)$ is a subspace of $\mathbb{R}^n$. That is a straightforward exercise that you should do in order to check that you not only understand the meanings of *linear combination*, *linear span*, and *subspace*, but can put those ideas together in a simple proof.

Suppose we have shown that $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_d)$ is a subspace of $\mathbb{R}^n$. It certainly contains $\underline{v}_1, \ldots, \underline{v}_d$. However, if V is a subspace of $\mathbb{R}^n$, it contains all linear combinations of any set of elements in it. Thus if V is a subspace containing $\underline{v}_1, \ldots, \underline{v}_d$ it contains all linear combinations of those vectors, i.e., V contains $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_d)$. Hence $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_d)$ is the smallest subspace of $\mathbb{R}^n$ containing $\underline{v}_1, \ldots, \underline{v}_d$. □

PROPOSITION 1.5. *The range of a matrix is equal to the linear span of its columns.*[1]

---

[1]This result can be viewed as a restatement of Corollary 3.2 which says that $A\underline{x} = \underline{b}$ has a solution if and only if $\underline{b}$ is a linear combination of the columns of A because the range of an $m \times n$ matrix can be described as

$$\begin{aligned}\mathcal{R}(A) &= \{\underline{b} \in \mathbb{R}^m \mid \underline{b} = A\underline{x} \text{ for some } \underline{x} \in \mathbb{R}^n\} \\ &= \{\underline{b} \in \mathbb{R}^m \mid \text{the equation } \underline{b} = A\underline{x} \text{ has a solution}\}.\end{aligned}$$

Proof. Let A be an $m \times n$ matrix with columns $\underline{A}_1, \ldots, \underline{A}_n$. If $\underline{x} \in \mathbb{R}^n$, then

$$A\underline{x} = x_1\underline{A}_1 + \cdots + x_n\underline{A}_n$$

so

$$\mathcal{R}(A) = \{x_1\underline{A}_1 + \cdots + x_n\underline{A}_n \mid x_1, \ldots, x_n \in \mathbb{R}\}.$$

But the right hand side is the set of all linear combinations of the columns of A, i.e., the linear span of those columns. □

2. The row and column spaces of a matrix

The row space of a matrix A is the linear span of its rows. The column space of a matrix A is the linear span of its columns.

Lemma 2.1. *If A and B are equivalent matrices they have the same row space.*

Proof. Since equivalent matrices are obtained from one another by a sequence of elementary row operations it suffices to show that the row space does not change when we perform a single elementary row operation on A.

Let $R_1, \ldots, R_m$ denote the rows of A. If R_i and R_j are switched the row space certainly stays the same. If R_i is replaced by λR_i for any non-zero number λ the row space stays the same. Since $aR_i + bR_j = a(R_i + \lambda R_j) + (b - \lambda a)R_j$ the row space does not change when R_i is replaced by $R_i + \lambda R_j$. □

2.1. Sums of subspaces are subspaces.

If S and T are subsets of $\mathbb{R}^n$, their sum is the set

$$S + T := \{\underline{u} + \underline{v} \mid \underline{u} \in S \text{ and } \underline{v} \in T\}.$$

Lemma 2.2. *If U and V are subspaces of $\mathbb{R}^n$ so is $U + V$.*

Proof. Since U and V are subspaces, each contains 0. Hence $0 + 0 \in U + V$; i.e., $U + V$ contains 0.

If $\underline{x}, \underline{x}' \in U + V$, then $\underline{x} = \underline{u} + \underline{v}$ and $\underline{x}' = \underline{u}' + \underline{v}'$ for some $\underline{u}, \underline{u}' \in U$ and $\underline{v}, \underline{v}' \in V$. Using the fact that U and V are subspaces, it follows that

$$\underline{x} + \underline{x}' = (\underline{u} + \underline{v}) + (\underline{u}' + \underline{v}') = (\underline{u} + \underline{u}') + (\underline{v} + \underline{v}') \in U + V$$

and, if $a \in \mathbb{R}$, then

$$a\underline{x} = a(\underline{u} + \underline{v}) = a\underline{u} + a\underline{v} \in U + V.$$

Hence $U + V$ is a subspace. □

The result can be extended to sums of more than subspaces using an induction argument. You'll see the idea by looking at the case of three subspaces U, V, and W, say. First, we define

$$U + V + W = \{\underline{u} + \underline{v} + \underline{w} \mid \underline{u} \in U,\ \underline{v} \in V, \text{ and } \underline{w} \in W\}.$$

It is clear that $U + V + W = (U + V) + W$. By the lemma, $U + V$ is a subspace. Now we may apply the lemma to the subspaces $U + V$ and W;

the lemma then tells us that $(U+V)+W$ is a subspace. Hence $U+V+W$ is a subspace.

As an example of the sum of many subspaces, notice that $\mathrm{Sp}(\underline{v}_1,\ldots,\underline{v}_d) = \mathbb{R}\underline{v}_1+\cdots+\mathbb{R}\underline{v}_d$ so repeated application of the lemma tells us that the linear span of any set of vectors is a subspace. This gives an alternative proof of Proposition 1.4.

2.2. Intersections of subspaces are subspaces.

LEMMA 2.3. *If U and V are subspaces of $\mathbb{R}^n$ so is $U\cap V$.*

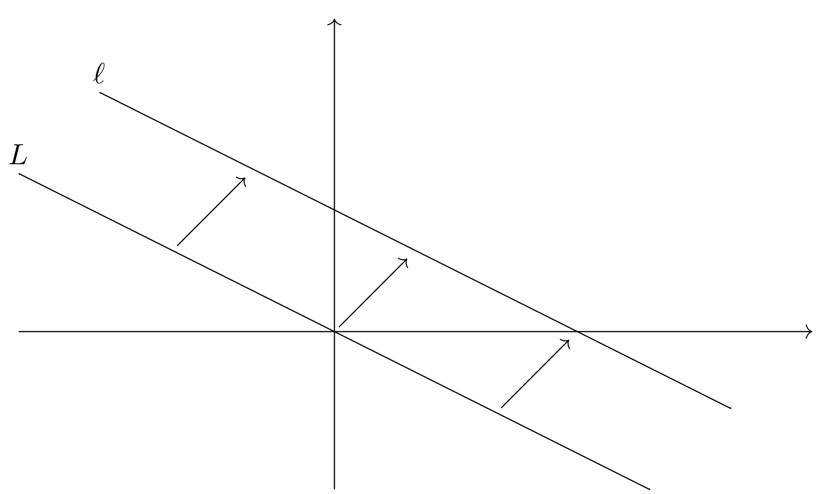
Proof. Because U and V are subspaces each of them contains the zero vector. Hence $\underline{0}\in U\cap V$. Now suppose $\underline{u}$ and $\underline{v}$ belong to $U\cap V$, and that $a\in\mathbb{R}$. Because $\underline{u}$ and $\underline{v}$ belong to the subspace U so does $\underline{u}+\underline{v}$; similarly, $\underline{u}$ and $\underline{v}$ belong to V so $\underline{u}+\underline{v}\in V$. Hence $\underline{u}+\underline{v}\in U\cap V$. Finally if $\underline{w}\in U\cap V$ and $a\in\mathbb{R}$, then $a\underline{w}\in U$ because U is a subspace and $a\underline{w}\in V$ because V is a subspace so $a\underline{w}\in U\cap V$. □

2.3. Planes through the origin are subspaces. If the set $\{\underline{u},\underline{v}\}$ is linearly independent we call the linear span of $\underline{u}$ and $\underline{v}$ a plane.

3. Lines, planes, and translations of subspaces

Let m and c be non-zero real numbers. Let ℓ be the line $y=mx+c$ and L the line $y=mx$. Both lines lie in $\mathbb{R}^2$. Now L is a subspace but ℓ is not because it does not contain $(0,0)$. However, ℓ is parallel L, and can be obtained by sliding L sideways, not changing the slope, so the it passes through $(0,c)$. We call the line $y=mx+c$ a *translation* of the line $y=mx$; i.e., ℓ is a translation of the subspace L. The picture below is an example in which

$$\ell \text{ is } y=-\tfrac{1}{2}(x-3) \text{ and } L \text{ is } y=-\tfrac{1}{2}x$$



Returning to the general case, every point on ℓ is the sum of $(0, c)$ and a point on the line $y = mx$ so, if we write L for the subspace $y = mx$, then

$$\begin{aligned} \ell &= (0, c) + L \\ &= \{(0, c) + \underline{v} \mid \underline{v} \in L\} \\ &= \{(0, c) + (x, mx) \mid x \in \mathbb{R}\} \\ &= (0, c) + \mathbb{R}(1, m). \end{aligned}$$

Let V be a subspace of $\mathbb{R}^n$ and $\underline{z} \in \mathbb{R}^n$. We call the subset

$$\underline{z} + V := \{\underline{z} + \underline{v} \mid \underline{v} \in V\}$$

the <u>translation of V by $\underline{z}$</u>. We also call $\underline{z} + V$ a <u>translate</u> of V.

Proposition 3.1. *Let $\mathcal{S}$ be the set of solutions to the equation $A\underline{x} = \underline{b}$ and let V be the set of solutions to the homogeneous equation $A\underline{x} = 0$. Then $\mathcal{S}$ is a translate of V: if $\underline{z}$ is any solution to $A\underline{x} = \underline{b}$, then $\mathcal{S} = \underline{z} + V$.*

Proof. Let $\underline{x} \in \mathbb{R}^n$. Then $A(\underline{z} + \underline{x}) = \underline{b} + A\underline{x}$, so $\underline{z} + \underline{x} \in \mathcal{S}$ if and only if $\underline{x} \in V$. The result follows. □

Now would be a good time to re-read chapter 7: that chapter talks about obtaining solutions to an equation $A\underline{x} = \underline{b}$ by translating $\mathcal{N}(A)$ by a particular solution to the equation $A\underline{x} = \underline{b}$. In fact, Proposition 3.1 and Proposition 8.1 really say the same thing in slightly different languages, and the example in chapter 7 illustrates what these results mean in a concrete situation.

3.1. The linear geometry of $\mathbb{R}^3$. This topic should already be familiar.

Skew lines, parallel planes, intersection of line and plane, parallel lines.

For example, find an equation for the subspace of $\mathbb{R}^3$ spanned by $(1, 1, 1)$ and $(1, 2, 3)$. Since the vectors are linearly independent that subspace will be a plane with basis $\{(1, 1, 1), (1, 2, 3)\}$. A plane in $\mathbb{R}^3$ is given by an equation of the form

$$ax + by + cz = d$$

and is a subspace if and only if $d = 0$. Thus we want to find $a, b, c \in \mathbb{R}$ such that $ax + by + cz = 0$ is satisfied by $(1, 1, 1)$ and $(1, 2, 3)$. More concretely, we want to find $a, b, c \in \mathbb{R}$ such that

$$\begin{aligned} x + y + z &= 0 \\ x + 2y + 3z &= 0. \end{aligned}$$

This is done in the usual way:

$$\begin{pmatrix} 1 & 1 & 1 & | & 0 \\ 1 & 2 & 3 & | & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1 & 1 & | & 0 \\ 0 & 1 & 2 & | & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & -1 & | & 0 \\ 0 & 1 & 2 & | & 0 \end{pmatrix}.$$

Thus c is an independent variable and $a = c$ and $b = -2c$. We just want a particular solution so take $c = 1$, $a = 1$, and $b = -2$. The subspace we seek is given by the equation

$$x - 2y + z = 0.$$

The fact that c can be anything is just saying that this plane can also be given by non-zero multiples of the equation $x - 2y + z = 0$. For example, $2x - 4y + 2z = 0$ is another equation for the same plane. And so on.

4. Linguistic difficulties: algebra vs. geometry

A midterm question asked students to find all points on the plane

$$\begin{aligned} x_1 - 2x_2 + 3x_3 - 4x_4 &= 0 \\ x_1 - x_2 - x_3 + x_4 &= 0 \end{aligned}$$

in $\mathbb{R}^4$. I was surprised how many students found this a hard problem. But I suspect they could have answered the question *find all solutions to the system of equations*

$$\begin{aligned} x_1 - 2x_2 + 3x_3 - 4x_4 &= 0 \\ x_1 - x_2 - x_3 + x_4 &= 0. \end{aligned}$$

The two problems are identical! The students' problem was linguistic not mathematical. The first problem sounds geometric, the second algebraic. A first course on linear algebra contains many new words and ideas. To understand linear algebra you must understand the connections and relationship between the new words and ideas. Part of this involves the interaction between algebra and geometry. This interaction is a fundamental aspect of mathematics. You were introduced to it in high school. There you learned that the solutions to an equation like $y = 3x - 2$ "are" the points on a line in $\mathbb{R}^2$; that the solutions to the equation $2x^2 + 3y^2 = 4$ "are" the points on an ellipse ;and so on. Translating between the two questions at the start of this chapter is the same kind of thing.

The reason students find the question of finding all solutions to the system of equations easier is that they have a *recipe* for finding the solutions: find $\underline{\mathsf{rref}}(A)$, find the independent variables, etc. Recipes are a very important part of linear algebra—after all we *do* want to solve problems and we want to find methods to solve particular kinds of problems. But linear algebra involves *ideas*, and connections and interactions between those ideas. As you understand these you will learn how to come up with new recipes, and learn to recognize when a particular recipe can be used even if the problem doesn't have the "code words" that suggest a particular recipe can be used.

CHAPTER 8

Linear dependence and independence

The notion of linear independence is central to the course from here on out.

1. The definition

A set of vectors $\{\underline{v}_1, \ldots, \underline{v}_n\}$ is <u>linearly independent</u> if the only solution to the equation

$$a_1\underline{v}_1 + \cdots + a_n\underline{v}_n = 0$$

is $a_1 = \cdots = a_n = 0$. We say $\{\underline{v}_1, \ldots, \underline{v}_n\}$ is <u>linearly dependent</u> if it is not linearly independent.

In other words, $\{\underline{v}_1, \ldots, \underline{v}_n\}$ is <u>linearly dependent</u> if there are numbers $a_1, \ldots, a_n \in \mathbb{R}$, not all zero, such that

$$a_1\underline{v}_1 + \cdots + a_n\underline{v}_n = \underline{0}.$$

1.1. The standard basis for $\mathbb{R}^n$ is linearly independent. Because

$$a_1\underline{e}_1 + a_2\underline{e}_2 + \cdots + a_n\underline{e}_n = (a_1, a_2, \ldots, a_n)$$

this linear combination is zero if and only if $a_1 = a_2 = \cdots = a_m = 0$. The $\underline{e}_i$s form the prototypical example of a linearly independent set.

1.2. Example. Any set containing the zero vector is linearly dependent because

$$1.\underline{0} + 0\underline{v}_1 + \cdots + 0.\underline{v}_n = \underline{0}.$$

2. Criteria for linear (in)dependence

I won't ask you to prove the next theorem on the exam but you will learn a lot if you read and re-read its proof until you understand it.

THEOREM 2.1. *The non-zero rows of a matrix in row echelon form are linearly independent.*

Proof. The key point is that the left-most non-zero entries in each non-zero row of a matrix in echelon form move to the right as we move downwards from row 1 to row 2 to row 3 to ... etc. We can get an idea of the proof by looking at a single example. The matrix

$$E = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

is in echelon form. Its non-zero rows are

$$\begin{aligned} \underline{v}_1 &= (1,2,3,4,5,6), \\ \underline{v}_2 &= (0,1,2,3,4,5), \\ \underline{v}_3 &= (0,0,0,1,2,3). \end{aligned}$$

To show these are linearly independent we must show that the only solution to the equation

$$a_1\underline{v}_1 + a_2\underline{v}_2 + a_3\underline{v}_3 = \underline{0}$$

is $a_1 = a_2 = a_3 = 0$. Suppose $a_1\underline{v}_1 + a_2\underline{v}_2 + a_3\underline{v}_3 = 0$. The sum $a_1\underline{v}_1 + a_2\underline{v}_2 + a_3\underline{v}_3$ is equal to

$$(a_1, 2a_1, 3a_1, 4a_1, 5a_1, 6a_1) + (0, a_2, 2a_2, 3a_2, 4a_2, 5a_2) + (0, 0, 0, a_3, 2a_3, 3a_3).$$

The left most entry of this sum is a_1 so the fact that the sum is equal to $\underline{0} = (0,0,0,0,0,0)$ implies that $a_1 = 0$. It follows that $a_2\underline{v}_2 + a_3\underline{v}_3 = \underline{0}$. But $a_2\underline{v}_2 + a_3\underline{v}_3 = (0, a_2, \ldots)$ (we don't care about what is in the positions $\ldots$) so we must have $a_2 = 0$. Therefore $a_3 v_3 = \underline{0}$; but $a_3 v_3 = \begin{pmatrix} 0 & 0 & 0 & a_3 & 2a_3 & 3a_3 \end{pmatrix}$ so we conclude that $a_3 = 0$ too. Hence $\{\underline{v}_1, \underline{v}_2, \underline{v}_3\}$ is linearly independent. $\square$

THEOREM 2.2. *Vectors $\underline{v}_1, \ldots, \underline{v}_n$ are linearly dependent if and only if some $\underline{v}_i$ is a linear combination of the other $\underline{v}_j$s.*

Proof. ($\Rightarrow$) Suppose $\underline{v}_1, \ldots, \underline{v}_n$ are linearly dependent. Then there are numbers $a_1, \ldots, a_n$, not all zero, such that $a_1\underline{v}_1 + \cdots + a_n\underline{v}_n = 0$. Suppose $a_i \neq 0$. Then

$$\underline{v}_i = \sum_{j \neq i} (-a_i^{-1} a_j)\underline{v}_j.$$

($\Leftarrow$) Suppose $\underline{v}_i$ is a linear combination of the other $\underline{v}_j$s. Then there are numbers b_j such that

$$\underline{v}_i = \sum_{j \neq i} b_j \underline{v}_j.$$

Therefore

$$1.\underline{v}_i - \sum_{j \neq i} b_j \underline{v}_j = 0,$$

thus showing that $\underline{v}_1, \ldots, \underline{v}_n$ are linearly dependent. $\square$

2.1. Using Theorem 2.2. Theorem 2.2 is an excellent way to show that a set of vectors is linearly dependent. For example, it tells us that the vectors

$$\begin{pmatrix}0\\1\\2\end{pmatrix}, \quad \begin{pmatrix}1\\3\\4\end{pmatrix}, \quad \begin{pmatrix}1\\4\\6\end{pmatrix},$$

are linearly dependent because

$$\begin{pmatrix}1\\4\\6\end{pmatrix} = \begin{pmatrix}0\\1\\2\end{pmatrix} + \begin{pmatrix}1\\3\\4\end{pmatrix}.$$

Please understand why this shows these three vectors are linearly independent by re-writing it as

$$1\begin{pmatrix}0\\1\\2\end{pmatrix} + 1\begin{pmatrix}1\\3\\4\end{pmatrix} + (-1)\begin{pmatrix}1\\4\\6\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix}$$

and re-reading the definition of linear dependence.

2.2. Remark. The important word in the next theorem is the word *unique*. It is this uniqueness that leads to the idea of coordinates which will be taken up in chapter 10.

THEOREM 2.3. *Vectors $\underline{v}_1, \ldots, \underline{v}_n$ are linearly independent if and only if each vector in their linear span can be written as a linear combination of $\underline{v}_1, \ldots, \underline{v}_n$ in a unique way.*

Proof. Since $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_n)$ is, by definition, the set of linear combinations of $\underline{v}_1, \ldots, \underline{v}_n$ we must prove that the linear independence condition is equivalent to the uniqueness condition.

($\Rightarrow$) Suppose $\underline{v}_1, \ldots, \underline{v}_n$ are linearly independent. Let $\underline{w} \in \mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_n)$. If $\underline{w} = a_1\underline{v}_1 + \cdots + a_n\underline{v}_n$ and $\underline{w} = b_1\underline{v}_1 + \cdots + b_n\underline{v}_n$, then

$$\begin{aligned} 0 &= \underline{w} - \underline{w} \\ &= \big(a_1\underline{v}_1 + \cdots + a_n\underline{v}_n\big) \; - \; \big(b_1\underline{v}_1 + \cdots + b_n\underline{v}_n\big) \\ &= (a_1 - b_1)\underline{v}_1 + \cdots + (a_n - b_n)\underline{v}_n. \end{aligned}$$

Because the set $\{\underline{v}_1, \ldots, \underline{v}_n\}$ is linearly independent,

$$a_1 - b_1 = \cdots = a_n - b_n = 0.$$

Hence the two representations of $\underline{w}$ as a linear combination of $\underline{v}_1, \ldots, \underline{v}_n$ are the same, i.e., there is a unique way of writing $\underline{w}$ as a linear combination of those vectors.

($\Leftarrow$) Suppose each element in $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_n)$ can be written as a linear combination of $\underline{v}_1, \ldots, \underline{v}_n$ in a unique way. In particular, there is only one way to write the zero vector as a linear combination. But $0 = 0\underline{v}_1 + \cdots + 0\underline{v}_n$ so if $a_1\underline{v}_1 + \cdots + a_n\underline{v}_n = 0$, then $a_1 = 0$, $a_2 = 0, \ldots, a_n = 0$. In other words, the set $\{\underline{v}_1, \ldots, \underline{v}_n\}$ is linearly independent. $\square$

Theorem 2.4. *Every subset of* $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_d)$ *having* $\geq d+1$ *vectors is linearly dependent.*

Proof. Let $r \geq d+1$ and let $\underline{w}_1, \ldots, \underline{w}_r$ be vectors in $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_d)$. For each $i = 1, \ldots, r$ there are numbers $a_{i1}, \ldots, a_{id} \in \mathbb{R}$ such that

$$\underline{w}_i = a_{i1}\underline{v}_1 + a_{i2}\underline{v}_2 \cdots + a_{id}\underline{v}_d. \tag{2-1}$$

The homogeneous system

$$\begin{aligned} a_{11}c_1 + a_{21}c_2 + \cdots + a_{r1}c_r &= 0 \\ a_{12}c_1 + a_{22}c_2 + \cdots + a_{r2}c_r &= 0 \\ \vdots \quad & \quad \vdots \\ a_{1d}c_1 + a_{2d}c_2 + \cdots + a_{rd}c_r &= 0 \end{aligned}$$

of d equations in the unknowns $c_1, \ldots, c_r$ has more unknowns than equations so has a non-trivial solution; i.e., there are numbers $c_1, \ldots, c_r$, not all equal to zero, that satisfy this system of equations. It follows from this that

$$\begin{aligned} c_1\underline{w}_1 + \cdots + c_r\underline{w}_r &= (c_1a_{11} + c_2a_{21} + \cdots + c_ra_{r1})\underline{v}_1 + \\ &\quad\ (c_1a_{12} + c_2a_{22} + \cdots + c_ra_{r2})\underline{v}_2 + \\ &\quad\quad \vdots \\ &\quad\ (c_1a_{1d} + c_2a_{2d} + \cdots + c_ra_{rd})\underline{v}_d \\ &= \underline{0}. \end{aligned}$$

This shows that $\{\underline{w}_1, \ldots, \underline{w}_r\}$ is linearly dependent. □

Corollary 2.5. *All bases for a subspace have the same number of elements.*

Proof. Suppose that $\{\underline{v}_1, \ldots, \underline{v}_d\}$ and $\{\underline{w}_1, \ldots, \underline{w}_r\}$ are bases for W. Then

$$W = \mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_d) = \mathrm{Sp}(\underline{w}_1, \ldots, \underline{w}_r)$$

and the sets $\{\underline{v}_1, \ldots, \underline{v}_d\}$ and $\{\underline{w}_1, \ldots, \underline{w}_r\}$ are linearly independent.

By Theorem 2.4, a linearly independent subset of $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_d)$ has $\leq d$ elements so $r \leq d$. Likewise, by Theorem 2.4, a linearly independent subset of $\mathrm{Sp}(\underline{w}_1, \ldots, \underline{w}_r)$ has $\leq r$ elements so $d \leq r$. Hence $d = r$. □

The next result is a special case of Theorem 2.4 because $\mathbb{R}^n = \mathrm{Sp}\{\underline{e}_1, \ldots, \underline{e}_n\}$. Nevertheless, we give a different proof which again emphasizes the fact that a homogeneous system of equations in which there are more unknowns than equations has a non-trivial solution.

Theorem 2.6. *If* $n > m$, *then every set of* n *vectors in* $\mathbb{R}^m$ *is linearly dependent.*

Proof. Let's label the vectors $\underline{A}_1, \ldots, \underline{A}_n$ and make them into the columns of an $m \times n$ matrix that we call A. Then $A\underline{x} = x_1\underline{A}_1 + \cdots + x_n\underline{A}_n$ so the equation $A\underline{x} = 0$ has a non-trivial solution (i.e., a solution with some

$x_i \neq 0$) if and only if $\underline{A}_1, \ldots, \underline{A}_n$ are linearly dependent. But $A\underline{x} = 0$ has a non-trivial solution because it consists of m equations in n unknowns and $n > m$ (see Proposition 9.2 and Corollary 9.3). □

3. Linear (in)dependence and systems of equations

THEOREM 3.1. *The homogeneous system $A\underline{x} = 0$ has a non-trivial solution if and only if the columns $\underline{A}_1, \ldots, \underline{A}_n$ of A are linearly dependent.*

Proof. The proof of Theorem 2.6 used the fact that $A\underline{x} = x_1\underline{A}_1 + \cdots + x_n\underline{A}_n$ to conclude that $A\underline{x} = 0$ has a non-trivial solution (i.e., a solution with some $x_i \neq 0$) if and only if $\underline{A}_1, \ldots, \underline{A}_n$ are linearly dependent. □

The next result is obtained directly from the previous one —it is the *contrapositive*. By that we mean the following general principle of logic: if a statement P is true if and only if a statement Q is true, then P is false if and only if Q is false.

We apply this principle to Theorem 3.1 by noting that "not having a non-trivial solution" is the same as "having only the trivial solution" (which is the same as having a unique solution for a homogeneous system), and "not linearly dependent" is the same as "linearly independent".

THEOREM 3.2. *The homogeneous system $A\underline{x} = 0$ has a unique solution if and only if the columns $\underline{A}_1, \ldots, \underline{A}_n$ of A are linearly independent.*

The reason for restating Theorem 3.1 as Theorem 3.2 is to emphasize the parallel between Theorem 3.2 and Theorem 3.3.

THEOREM 3.3. *The system $A\underline{x} = \underline{b}$ has a unique solution if and only if $\underline{b}$ is a linear combination of the columns $\underline{A}_1, \ldots, \underline{A}_n$ of A and $\underline{A}_1, \ldots, \underline{A}_n$ are linearly independent.*

Proof. We have already proved that $A\underline{x} = \underline{b}$ has a solution if and only if $\underline{b}$ is a linear combination of the columns of A; see Corollary 3.2 and the discussion just before it.

($\Rightarrow$) Suppose $A\underline{x} = \underline{b}$ has a unique solution. Because $A\underline{x} = \underline{b}$ has a solution, Corollary 3.2 and the discussion just before it tell us that $\underline{b}$ is a linear combination of the columns of A.

We will now use the fact that $A\underline{x} = \underline{b}$ has a *unique* solution to show that the columns of A are linearly independent. Suppose $c_1\underline{A}_1 + \cdots + c_n\underline{A}_n = 0$; in other words $A\underline{c} = \underline{0}$ where

$$\underline{c} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}.$$

If $\underline{u}$ is a solution to $A\underline{x} = \underline{b}$, so is $\underline{u} + \underline{c}$ because

$$A(\underline{u} + \underline{c}) = A\underline{u} + A\underline{c} = \underline{b} + \underline{0} = \underline{b}.$$

But $A\underline{x} = \underline{b}$ has a *unique* solution so $\underline{u} = \underline{u} + \underline{c}$. It follows that $\underline{c} = 0$. In other words, the only solution to the equation $c_1\underline{A}_1 + \cdots + c_n\underline{A}_n = 0$ is $c_1 = \cdots = c_n = 0$ which shows that the columns of A are linearly independent.

($\Leftarrow$) Suppose that $\underline{b}$ is a linear combination of the columns $\underline{A}_1, \ldots, \underline{A}_n$ of A and the columns are linearly independent. The first of these assumptions tells us there are numbers $c_1, \ldots, c_n \in \mathbb{R}$ such that $\underline{b} = c_1\underline{A}_1 + \cdots + c_n\underline{A}_n$; i.e., $A\underline{c} = \underline{b}$ where $\underline{c}$ is the $n \times 1$ matrix displayed above. If

$$\underline{d} = \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$$

were another solution to $A\underline{x} = \underline{b}$, then $\underline{b} = A\underline{d} = d_1\underline{A}_1 + \cdots + d_n\underline{A}_n$ so

$$(c_1 - d_1)\underline{A}_1 + \cdots + (c_n - d_n)\underline{A}_n = A\underline{c} - A\underline{d} = \underline{b} - \underline{b} = \underline{0}.$$

However, $\underline{A}_1, \ldots, \underline{A}_n$ are linearly independent so $c_1 = d_1, \ldots, c_n = d_n$, i.e., $\underline{c} = \underline{d}$ thereby showing that $A\underline{x} = \underline{b}$ has a unique solution. $\square$

Lemma 2.1 tells us that equivalent matrices have the same row space.

Proposition 3.4. *Let A be any matrix. Then A and $\underline{\mathsf{rref}}(A)$ have the same row space, and the non-zero rows of $\underline{\mathsf{rref}}(A)$ are linearly independent.*

Proof. Let $E = \underline{\mathsf{rref}}(A)$. The fact that A and E have the same row space is a special case of Lemma 2.1. Suppose $\underline{r}_1, \ldots, \underline{r}_t$ are the non-zero rows of E. Suppose the left-most 1 in $\underline{r}_i$ appears in the j_i^{th} column. Then $j_1 < j_2 < \ldots < j_t$.

Now suppose that $a_1\underline{r}_1 + \cdots + a_t\underline{r}_t = 0$.

The entry in column j_1 of $\underline{r}_1$ is 1 and the entry in column j_1 of all other $\underline{r}_i$s is 0, so the entry in column j_1 of $a_1\underline{r}_1 + \cdots + a_t\underline{r}_t$ is a_1. Hence $a_1 = 0$.

The entry in column j_2 of $\underline{r}_2$ is 1 and the entry in column j_2 of all other $\underline{r}_i$s is 0, so the entry in column j_2 of $a_1\underline{r}_1 + \cdots + a_t\underline{r}_t$ is a_2. Hence $a_2 = 0$.

Carry on in this way to deduce that each a_i is zero. We will then have shown that the only solution to the equation $a_1\underline{r}_1 + \cdots + a_t\underline{r}_t = 0$ is $a_1 = a_2 = \cdots = a_t = 0$. Hence $\{\underline{r}_1, \ldots, \underline{r}_t\}$ is linearly independent. $\square$

After we have defined the word *basis* you will see that Proposition 3.4 says that the non-zero rows of $\underline{\mathsf{rref}}(A)$ are a basis for the row space of A.

If one is interested in the column space of a matrix A rather than its row space, one can replace A by A^T and perform elementary row operations on A^T. The transposes of the rows of $\underline{\mathsf{rref}}(A^T)$ span the column space of A. We will see later that they form a basis for the column space of A.

CHAPTER 9

Non-singular matrices, invertible matrices, and inverses

The adjectives *singular, non-singular,* and *invertible*, apply to square matrices and square matrices only.

1. Singular and non-singular matrices

An $n \times n$ matrix A is called non-singular if the only solution to the equation $A\underline{x} = 0$ is $\underline{x} = 0$. We say A is singular if $A\underline{x} = 0$ has a non-trivial solution.

When we say *the following are equivalent* in the next theorem what we mean is that if one of the three statements is true so are the others. It also means that if one of the three statements is false so are the others. Therefore to prove the theorem we must do the following: assume one of the statements is true and then show that assumption forces the other two to be true. In the proof below we show that (1) is true if and only if (2) is true. Then we show that (3) is true if (2) is. Finally we show (1) is true if (3) is. Putting all those implications together proves that the truth of any one of the statements implies the truth of the other two.

THEOREM 1.1. *Let A be an $n \times n$ matrix. The following are equivalent:*

(1) *A is non-singular;*
(2) *$\{\underline{A}_1, \ldots, \underline{A}_n\}$ is linearly independent.*
(3) *$A\underline{x} = \underline{b}$ has a unique solution for all $\underline{b} \in \mathbb{R}^n$.*

Proof. (1) $\Leftrightarrow$ (2) This is exactly what Theorem 3.2 says.

(2) $\Rightarrow$ (3) Suppose that (2) is true.

Let $\underline{b} \in \mathbb{R}^n$. By Theorem 2.6, the $n+1$ vectors $\underline{b}, \underline{A}_1, \ldots, \underline{A}_n$ in $\mathbb{R}^n$ are linearly dependent so there are numbers $a_1, \ldots, a_n, a_{n+1}$, not all zero, such that

$$a_0\underline{b} + a_1\underline{A}_1 + \cdots + a_n\underline{A}_n = 0.$$

I claim that a_0 can not be zero.

Suppose the claim is false. Then $a_1\underline{A}_1 + \cdots + a_n\underline{A}_n = 0$, But $\underline{A}_1, \ldots, \underline{A}_n$ are linearly independent so $a_1 = \cdots = a_n = 0$. Thus if $a_0 = 0$, then *all* the a_is are zero. That contradicts the fact (see the previous pragraph) that not all the a_is are zero. Since the assumption that $a_0 = 0$ leads to a contradiction we conclude that a_0 must be non-zero.

Hence

$$\underline{b} = (-a_0^{-1}a_1)\underline{A}_1 + \cdots + (-a_0^{-1}a_n)\underline{A}_n.$$

Thus $\underline{b}$ is a linear combination of $\underline{A}_1, \ldots, \underline{A}_n$. By hypothesis, $\underline{A}_1, \ldots, \underline{A}_n$ linearly independent. Hence Theorem 3.3 tells us there is a unique solution to $A\underline{x} = \underline{b}$.

(3) $\Rightarrow$ (1) Assume (3) is true. Then, in particular, the equation $A\underline{x} = 0$ has a unique solution; i.e., A is non-singular, so (1) is true. $\square$

2. Inverses

Mankind used whole numbers, integers, before using fractions. Fractions were created because they are useful in the solution of equations. For example, the equation $3x = 7$ has no solution if we require x to be an integer but it does have a solution if we allow x to be a fraction, that solution being $\frac{7}{3}$.

One could take the sophisticated (too sophisticated?) view that this solution was found by multiplying both sides of the equation by the inverse of 3. Explicitly, $3x$ is equal to 7 if and only if $\frac{1}{3} \times 3x$ equals $\frac{1}{3} \times 7$. Now use the associative law for multiplication and perform the complicated equation

$$\frac{1}{3} \times 3x = \left(\frac{1}{3} \times 3\right) \times x = 1 \times x = x$$

so the previous sentence now reads $3x$ is equal to 7 if and only if x equals $\frac{1}{3} \times 7$. Presto! we have solved the equation.

Sometimes one encounters a matrix equation in which one can perform the same trick. Suppose the equation is $A\underline{x} = \underline{b}$ and suppose you are in the fortunate position of knowing there is a matrix E such that $EA = I$, the identity matrix. Then $A\underline{x} = \underline{b}$ implies that $E \times A\underline{x} = E \times \underline{b}$. Thus, using the associative law for multiplication $A\underline{x} = \underline{b}$ implies

$$E\underline{b} = E \times \underline{b} = E \times A\underline{x} = (E \times A) \times \underline{x} = I \times \underline{x} = \underline{x}.$$

Presto! We have found a solution, namely $\underline{x} = E\underline{b}$. We found this by the same process as that in the previous paragraph.

Let's look at an explicit example. Suppose we want to solve

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -1 \\ 5 \end{pmatrix}. \tag{2-1}$$

I know that the matrix

$$E = \frac{1}{2} \begin{pmatrix} -4 & 2 \\ 3 & -1 \end{pmatrix}$$

has the property that $EA = I$. You should check that. The analysis in the previous paragraph tells me that a solution to the equation (2-1) is

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = E \begin{pmatrix} -1 \\ 5 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} -4 & 2 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} -1 \\ 5 \end{pmatrix} = \begin{pmatrix} 7 \\ -4 \end{pmatrix}.$$

LEMMA 2.1. *Let A be an $n \times n$ matrix and I the $n \times n$ identity matrix. If there are matrices E and E' such that*

$$EA = AE' = I$$

then $E = E'$.

Proof. This is a single calculation:

$$E' = IE' = (EA)E' = E(AE') = EI = E.$$

All we used was the associative law. □

The inverse of an $n \times n$ matrix A is the matrix A^{-1} with the property

$$AA^{-1} = I = A^{-1}A,$$

provided it exists. If A has an inverse we say that A is invertible.

2.1. Uniqueness of A^{-1}. Our definition says that *the* inverse is *the* matrix .... The significance of Lemma 2.1 is that it tells us there is *at most one matrix, E say, with the property that $AE = EA = I$.* Check you understand that!

2.2. Not every square matrix has an inverse. The phrase *provided it exists* suggests that not every $n \times n$ matrix has an inverse—that is correct. For example, the zero matrix does not have an inverse. We will also see examples of non-zero square matrices that do not have an inverse.

2.3. The derivative of a function $f(x)$ at $a \in \mathbb{R}$ is defined to be

$$\lim_{h \to 0} \frac{f(a+h) - f(a)}{h}$$

provided this limit exists. The use of the phrase *"provided it exists"* in the definition of the inverse of a matrix plays the same role as the phrase *"provided this limit exists"* plays in the definition of the derivative.

2.4. The inverse or an inverse. You should compare our definition of *inverse* with that in the book. The book says an $n \times n$ matrix is invertible if there is a matrix A^{-1} such that $AA^{-1} = A^{-1}A = I$ and calls such A^{-1} *an* inverse of A (if it exists). Lemma 2.1 tells us there is at most one inverse so we can immediately speak of *the* inverse (provided it exists). You might want to look at the definition of the inverse in several books to gain a finer appreciation of this fine point.

Here is the definiton from the second edition of *Linear Algebra* by M. O'Nan:

> If A is an $m \times m$ matrix and there is an $m \times m$ matrix B such that $AB = BA = I$, A is said to be **invertible** and B is said to be the **inverse** of A.
>
> Having made this definition, the first natural question to ask is whether a matrix A can have two different inverses. Theorem 2 shows this is impossible.

Theorem 2 Let A be an $m \times m$ matrix with inverse B. If C is another matrix such that $AC = CA = I$, then $C = B$.

3. Elementary matrices are invertible

As we will now explain, the fact that elementary matrices are invertible is essentially the same as the fact that if a matrix B can be obtained from a matrix A by performing a single elementary row operation, then A can be obtained from B by performing a single elementary row operation

First recall that elementary matrices are, by definition, those matrices obtained by performing a single elementary row operation on an identity matrix.

Let A be an $m \times n$ matrix. By Theorem 11.1, the result of performing an elementary row operation on A produces a matrix that is equal to EA for a suitable $m \times m$ elementary matrix E. Since E is obtained from I_m by an elementary row operation, I_m can be obtained from E by performing an elementary row operation. Therefore $I_m = E'E$ for some elementary matrix E'. If you check each of the three elementary row operations you will see that the transpose of an elementary matrix is an elementary matrix. Hence E^T is an elementary matrix and by the argument just given, there is an elementary matrix F such that $FE^T = I_m$. Hence $EF^T = I_m = E'E$. By Lemma 2.1, the fact that $EF^T = I = E'E$ implies $F^T = E'$. Hence $E'E = EE' = I$ and E' is the inverse of E.

4. Making use of inverses

4.1. If A has an inverse and $AB = C$, then $B = A^{-1}C$. To see this just multiply both sides of the equality $AB = C$ on the left by A^{-1} to obtain $A^{-1}C = A^{-1}(AB) = (A^{-1}A)B = IB = B$.

4.2. Solving $A\underline{x} = \underline{b}$ when A is invertible. The only solution to this equation is $\underline{x} = A^{-1}\underline{b}$. This is a special case of the previous remark. In chapter 2 we put this remark into practice for an explicit example.

4.3. Wicked notation. Never, never, never write B/A to denote BA^{-1}.

4.4. If $AB = 0$ and $B \neq 0$, then A is not invertible. If A is invertible and B is a non-zero matrix such that $AB = 0$, then $B = IB = (A^{-1}A)B = A^{-1}(AB) = 0$ so contradicting the fact that B is non-zero. We are therefore forced to conclude that if $AB = 0$ for some non-zero matrix B, then A is not invertible. Likewise, if $BA = 0$ for some non-zero matrix B, then A is not invertible.

This is a useful observation because it immediately gives a large source of matrices that are not invertible. For example, the matrix

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

does not have an inverse because

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix};$$

in particular, the product can never be the identity matrix because the 22-entry is zero regardless of what w, x, y, z are.

4.5. We can cancel invertible matrices. Let A be an $n \times n$ matrix. If $AB = AC$, then $B = C$ because $AB = AC$ implies $A^{-1}(AB) = A^{-1}(AC)$ and the associative law then allows us to replace $A(A^{-1}$ by I to obtain $IB = IC$, i.e., $B = C$. I prefer the argument

$$B = IB = (A^{-1}A)B = A^{-1}(AB) = A^{-1}(AC) = (A^{-1}A)C = IC = C.$$

A similar argument shows that if A is invertible and $EA = FA$, then $E = F$.

Be warned though that you cannot cancel in an expression like $AB = CA$ because matrices do not necessarily commute with each other.

4.6. The inverse of a product. If A and B are $n \times n$ matrices have inverses, then AB is invertible and its inverse is $B^{-1}A^{-1}$ because

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$$

and similarly $(B^{-1}A^{-1})(AB) = I$.

A popular error is to claim that the inverse of AB is $A^{-1}B^{-1}$. An analogy might be helpful: the inverse to the operation *put on socks then shoes* is *take off shoes then socks*. The inverse to a composition of operations is the composition of the inverses of the operations in the reverse order.

5. The inverse of a 2×2 matrix

There is a simple arithmetic criterion for deciding if a given 2×2 matrix has an inverse.

THEOREM 5.1. *The matrix*

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

has an inverse if and only if $ad - bc \neq 0$. *If* $ad - bc \neq 0$, *then*

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Proof. ($\Longrightarrow$) Suppose A has an inverse. Just prior to this theorem, in chapter 4.4, we observed that

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

does not have an inverse, so either c or d must non-zero. Therefore

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} \neq \begin{pmatrix} d \\ -c \end{pmatrix} = A^{-1}A \begin{pmatrix} d \\ -c \end{pmatrix} = A^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d \\ -c \end{pmatrix} = A^{-1} \begin{pmatrix} ad - bc \\ 0 \end{pmatrix}$$

so we conclude that $ad - bc \neq 0$.

($\Longleftarrow$) If $ad - bc \neq 0$ a simple calculation shows that the claimed inverse is indeed the inverse. $\square$

The number $ad - bc$ is called the determinant of

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We usually write $\det(A)$ to denote the determinant of a matrix. Theorem 5.1 therefore says that a 2×2 matrix A has an inverse if and only if $\det(A) \neq 0$.

In chapter 12 we define the determinant for $n \times n$ matrices and a prove that an $n \times n$ matrix A has an inverse if and only if $\det(A) \neq 0$. That is a satisfying result. Although the formula for the determinant appears complicated at first it is straightforward to compute, even for large n, if one has a computer handy. It is striking that the invertibility of a matrix can be determined by a single computation even if doing the computation by hand can be long and prone to error.

THEOREM 5.2. *Let A be an $n \times n$ matrix. Then A has an inverse if and only if it is non-singular.*

Proof. ($\Rightarrow$) Suppose A has an inverse. If $A\underline{x} = 0$, then

$$\underline{x} = I\underline{x} = (A^{-1}A)\underline{x} = A^{-1}(A\underline{x}) = A^{-1}.0 = 0$$

so A is non-singular.

($\Leftarrow$) Suppose A is non-singular. Then $A\underline{x} = \underline{b}$ has a unique solution for all $\underline{b} \in \mathbb{R}^n$ by Theorem 1.1. Let

$$\underline{e}_1 = (1, 0, \dots, 0)^T, \quad \underline{e}_2 = (0, 1, 0, \dots, 0), \dots, \underline{e}_n = (0, \dots, 0, 1)$$

and define $\underline{u}_j \in \mathbb{R}^n$ to be the unique column vector such that $A\underline{u}_j = \underline{e}_j$. Let $U = [\underline{u}_1, \dots, \underline{u}_n]$ be the $n \times n$ matrix whose columns are $\underline{u}_1, \dots, \underline{u}_n$. Then

$$AU = [A\underline{u}_1, \dots, A\underline{u}_n] = [\underline{e}_1, \dots, \underline{e}_n] = I.$$

We will show that U is the inverse of A but we do not compute UA to do this!

First we note that U is non-singular because if $U\underline{x} = 0$, then

$$\underline{x} = I\underline{x} = (AU)\underline{x} = A(U\underline{x}) = A.0 = 0.$$

Because U is non-singular we may apply the argument in the previous paragraph to deduce the existence of a matrix V such that $UV = I$. (The previous paragraph showed that if a matrix is non-singular one can multiply it on the right by some matrix to obtain the identity matrix.) Now

$$V = IV = (AU)V = A(UV) = AI = A$$

so $AU = UA = I$, proving that $U = A^{-1}$. $\square$

We isolate an important part of the proof. After finding U and showing $AU = I$ we were not allowed to say U is the inverse of A and stop the proof because the definition of the inverse (read it carefully, now) says that we need to show that $UA = I$ too before we are allowed to say U is the inverse of A. It is not obvious that $AU = I$ implies $UA = I$ because there is no obvious reason for A and U to commute. That is why we need the last paragraph of the proof.

COROLLARY 5.3. *Let A be an $n \times n$ matrix. If $AU = I$, then $UA = I$, i.e., if $AU = I$, then U is the inverse of A.*

COROLLARY 5.4. *Let A be an $n \times n$ matrix. If $VA = I$, then $AV = I$, i.e., if $VA = I$, then V is the inverse of A.*

Proof. Apply Corollary 5.3 with V playing the role that A played in Corollary 5.3 and A playing the role that U played in Corollary 5.3. $\square$

THEOREM 5.5. *The following conditions on an $n \times n$ matrix A are equivalent:*

(1) *A is non-singular;*
(2) *A is invertible;*
(3) $\text{rank}(A) = n$*;*
(4) $\underline{\text{rref}}(A) = I$*, the identity matrix;*
(5) *$A\underline{x} = \underline{b}$ has a unique solution for all $\underline{b} \in \mathbb{R}^n$;*
(6) *the columns of A are linearly independent;*

6. If A is non-singular how do we find A^{-1}?

We use the idea in the proof of Theorem 5.2:

> the j^{th} column of A^{-1} is the solution to the equation $A\underline{x} = \underline{e}_j$ so we may form the augmented matrix $(A \,|\, \underline{e}_j)$ and perform row operations to get A in row-reduced echelon form.

We can carry out this procedure in one great big military operation. If we want to find the inverse of the matrix

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 3 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

we perform elementary row operations on the augmented matrix

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right)$$

so we get the identity matrix on the left hand side. The matrix on the right-hand side is then A^{-1}. Check it out!

CHAPTER 10

Bases, coordinates, and dimension

1. Definitions

A basis for a subspace W is a linearly independent subset of W that spans it.

The dimension of a subspace is the number of elements in a basis for it.

To make this idea effective we must show every subspace has a basis and that all bases for a subspace have the same number of elements.

Before doing that, let us take note of the fact that $\{\underline{e}_1, \ldots, \underline{e}_n\}$ is a basis for $\mathbb{R}^n$, the standard basis. We made the trivial observation that these vectors span $\mathbb{R}^n$ in section 3, and the equally trivial observation that these vectors are linearly independent in chapter 8. Combining these two facts we see that $\{\underline{e}_1, \ldots, \underline{e}_n\}$ is a basis for $\mathbb{R}^n$. Therefore

$$\dim \mathbb{R}^n = n.$$

Strictly speaking, we can't say this until we have proved that every basis for $\mathbb{R}^n$ has exactly n elements but we will prove that in Corollary 2.5 below.

Theorem 1.1. *Suppose $\underline{v}_1, \ldots, \underline{v}_d$ is a basis for W. If $\underline{w} \in W$, then there are unique scalars $a_1, \ldots, a_d$ such that $\underline{w} = a_1\underline{v}_1 + \cdots + a_d\underline{v}_d$.*

Proof. This theorem is a reformulation of Theorem 2.3. □

If $\underline{v}_1, \ldots, \underline{v}_d$ is a basis for W and $\underline{w} = a_1\underline{v}_1 + \cdots + a_d\underline{v}_d$ we call $(a_1, \ldots, a_d)$ the coordinates of $\underline{w}$ with respect to the basis $\underline{v}_1, \ldots, \underline{v}_d$. In this situation we can think of $(a_1, \ldots, a_d)$ as a point in $\mathbb{R}^d$.

2. A subspace of dimension d is just like $\mathbb{R}^d$

The function

$$T : \mathbb{R}^d \to W, \qquad T(a_1, \ldots, a_d) := a_1\underline{v}_1 + \cdots + a_d\underline{v}_d$$

is bijective (meaning injective and surjective, i.e., one-to-one and onto). It also satisfies the following properties:

1. $T(0) = 0$;
2. if $\underline{x}, \underline{y} \in \mathbb{R}^d$, then $T(\underline{x} + \underline{y}) = T(\underline{x}) + T(\underline{y})$;
3. if $\underline{x} \in \mathbb{R}^d$ and $\lambda \in \mathbb{R}$, then $T(\lambda\underline{x}) = \lambda T(\underline{x})$.

These properties are all special cases of the following property:

$$T(\lambda_1\underline{x}_1 + \cdots + \lambda_s\underline{x}_s) = \lambda_1 T(\underline{x}_1) + \cdots + \lambda_s T(\underline{x}_s) \tag{2-1}$$

for all $\underline{x}_1, \dots, \underline{x}_s \in \mathbb{R}^d$ and all $\lambda_1, \dots, \lambda_s \in \mathbb{R}$.

The function T is an example of a *linear transformation.*

It is the existence of the bijective function T having these properties that justifies my repeated remark that *a d-dimensional subspace looks exactly like* $\mathbb{R}^d$. That is the way you should think of a d-dimensional subspace of $\mathbb{R}^n$. It is a copy of $\mathbb{R}^d$ sitting inside $\mathbb{R}^n$. For example, all planes in $\mathbb{R}^3$ are copies of $\mathbb{R}^2$ sitting inside $\mathbb{R}^3$. Likewise, all lines in $\mathbb{R}^3$ are copies of $\mathbb{R}^1 = \mathbb{R}$ sitting inside $\mathbb{R}^3$.

3. All bases for W have the same number of elements

4. Every subspace has a basis

Our next goal, Theorem 4.2, is to show that every subspace has a basis. First we need a lemma.

By Theorem 2.6, every subset of $\mathbb{R}^n$ having $\geq n+1$ elements is linearly dependent. The lemma isolates the idea of building up a basis for a subspace one element at a time, i.e., by getting larger and larger linearly independent subsets of the subspace, a process that must eventually stop.

LEMMA 4.1. *Let $\{\underline{w}_1, \dots, \underline{w}_r\}$ be a linearly independent subset of $\mathbb{R}^n$. Let $\underline{v}$ be an element in $\mathbb{R}^n$ that does not belong to* $\mathrm{Sp}(\underline{w}_1, \dots, \underline{w}_r)$. *Then $\{\underline{v}\} \cup \{\underline{w}_1, \dots, \underline{w}_r\}$ is linearly independent.*

Proof. Suppose
$$\lambda \underline{v} + a_1 \underline{w}_1 + \cdots + a_n \underline{w}_n = 0$$
for some $\lambda, a_1, \dots, a_n \in \mathbb{R}$. If λ is non-zero, then
$$\underline{v} = (-\lambda^{-1} a_1) \underline{w}_1 + \cdots + (-\lambda^{-1} a_n) \underline{w}_n$$
which contradicts the hypothesis that $\underline{v}$ is not in $\mathrm{Sp}(\underline{w}_1, \dots, \underline{w}_r)$. Hence $\lambda = 0$. Now $a_1 \underline{w}_1 + \cdots + a_n \underline{w}_n = 0$. Because $\{\underline{w}_1, \dots, \underline{w}_r\}$ is linearly independent $a_1 = \cdots = a_n = 0$. Hence $\{\underline{v}, \underline{w}_1, \dots, \underline{w}_r\}$ is linearly independent. $\square$

THEOREM 4.2. *Every subspace of $\mathbb{R}^n$ has a basis.*

Proof. Let W be a subspace of $\mathbb{R}^n$. We adopt the standard convention that the empty set is a basis for the subspace $\{0\}$ so we may assume that $W \neq 0$. This ensures there is an element $\underline{w} \in W$ such that $\{\underline{w}\}$ is linearly independent.

Pick d as large as possible such that W contains a linearly independent subset having d elements. There *is* a largest such d because every subset of $\mathbb{R}^n$ having $\geq n+1$ elements is linearly dependent (Theorem 2.6). Suppose $\{\underline{w}_1, \dots, \underline{w}_d\}$ is a linearly independent subset of W. It is a basis for W if it spans W. However, if $\mathrm{Sp}(\underline{w}_1, \dots, \underline{w}_d) \neq W$ there is a $\underline{v}$ in W that is not in $\mathrm{Sp}(\underline{w}_1, \dots, \underline{w}_d)$. By Lemma 4.1, $\{\underline{w}_1, \dots, \underline{w}_d, \underline{v}\}$ is linearly independent, thus contradicting the maximality of d. We conclude that no such $\underline{v}$ can exist; i.e., $\mathrm{Sp}(\underline{w}_1, \dots, \underline{w}_d) = W$. Hence $\{\underline{w}_1, \dots, \underline{w}_d\}$ is a basis for W. $\square$

5. Properties of bases and spanning sets

The following is a useful way to think of $d = \dim W$; W has a linearly independent set having d elements and every subset of W having $> d$ elements is linearly dependent.

COROLLARY 5.1. *Let W be a subspace of $\mathbb{R}^n$. Then $\dim W$ is the largest number d such that W contains d linearly independent vectors.*

Proof. This is a consequence of the proof of Theorem 4.2. $\square$

COROLLARY 5.2. *Let V and W be subspaces of $\mathbb{R}^n$ and suppose $V \subseteq W$. Then*

(1) $\dim V < \dim W$ *if and only if* $V \neq W$*;*
(2) $\dim V = \dim W$ *if and only if* $V = W$*.*

Proof. Let $\{\underline{v}_1, \ldots, \underline{v}_c\}$ be a basis for V and $\{\underline{w}_1, \ldots, \underline{w}_d\}$ a basis for W. Since $\{\underline{v}_1, \ldots, \underline{v}_c\}$ is a linearly independent subset of V, and hence of W, $c \leq d$.

(1) ($\Rightarrow$) Suppose $c < d$. Since all bases for W have d elements, $\{\underline{v}_1, \ldots, \underline{v}_c\}$ can't be a basis for W. Hence $V \neq W$.

($\Leftarrow$) Suppose $V \neq W$. Then there is an element $\underline{w} \in W$ that is not in V, i.e., not in $\mathsf{span}\{\underline{v}_1, \ldots, \underline{v}_c\}$. By Lemma 4.1, $\{\underline{v}_1, \ldots, \underline{v}_c, \underline{w}\}$ is linearly independent. It is also a subset of W and contains $c+1$ elements so $c+1 \leq d$. In particular, $c < d$.

(2) This is the contrapositive of (1). $\square$

COROLLARY 5.3. *Let $W = \mathsf{span}\{\underline{v}_1, \ldots, \underline{v}_t\}$. Some subset of $\{\underline{v}_1, \ldots, \underline{v}_t\}$ is a basis for W.*

Proof. If $\{\underline{v}_1, \ldots, \underline{v}_t\}$ is linearly independent it is a basis for W and there is nothing more to prove.

If $\{\underline{v}_1, \ldots, \underline{v}_t\}$ is linearly dependent, some $\underline{v}_i$ is a linear combination of the other $\underline{v}_j$s so we can remove that $\underline{v}_i$ without changing the linear span and so get a set of $t-1$ vectors that spans W. By repeating this process we eventually get a linearly independent subset of $\{\underline{v}_1, \ldots, \underline{v}_t\}$ that spans W and is therefore a basis for W. $\square$

THEOREM 5.4. *Let W be a d-dimensional subspace of $\mathbb{R}^n$ and let $\mathcal{S} = \{\underline{w}_1, \ldots, \underline{w}_p\}$ be a subset of W.*

(1) *If $p \geq d+1$, then $\mathcal{S}$ is linearly dependent;*
(2) *If $p < d$, then $\mathcal{S}$ does not span W.*
(3) *If $p = d$, the following are equivalent:*
  (a) *$\mathcal{S}$ is linearly independent;*
  (b) *$\mathcal{S}$ spans W;*
  (c) *$\mathcal{S}$ is a basis for W.*

Proof. Let V be the subspace spanned by $\mathcal{S}$. Because $\mathcal{S} \subseteq W$, $V \subseteq W$. By Corollary 5.3, some subset of $\mathcal{S}$ is a basis for V. Hence $\dim V \le p$.

(1) is a restatement of Corollary 5.1.

(2) If $p < d$, then $\dim V < \dim W$ so $V \ne W$.

(3) Certainly, (c) implies both (a) and (b).

(a) $\Rightarrow$ (b) If $\mathcal{S}$ is linearly independent it is a basis for V so $\dim V = p = d = \dim W$. Hence $V = W$.

(b) $\Rightarrow$ (c) If $\mathcal{S}$ spans W, then $V = W$ so $\dim V = \dim W$

□

6. How to find a basis for a subspace

When a subspace is described as the linear span of an explicit set of vectors, say $W = \mathrm{Sp}(\underline{w}_1, \ldots, \underline{w}_r)$, the given vectors are typically linearly dependent so are *not* a basis for W. One can find a basis for W in the following way:

- if the $\underline{w}_j$s are row vectors form the matrix A with rows $\underline{w}_1, \ldots, \underline{w}_r$;
  - $\mathrm{Sp}(\underline{w}_1, \ldots, \underline{w}_r)$ is equal to the row space of A;
- if the $\underline{w}_j$s are column vectors form the matrix A with the rows $\underline{w}_1^T, \ldots, \underline{w}_r^T$;
  - $\mathrm{Sp}(\underline{w}_1^T, \ldots, \underline{w}_r^T)$ is equal to the row space of A;
- perform elementary row operations on A to obtain a matrix E in echelon form (in row-reduced echelon form if you want, though it isn't necessary for this);
- by Theorem 2.1, the non-zero rows of E are linearly independent;
- the non-zero rows of E are therefore a basis for the row space of E;
- by Lemma 2.1, A and E have the same row space;
- the non-zero rows of E are therefore a basis for the row space of A;
  - if the $\underline{w}_j$s are row vectors the non-zero rows of E are a basis for $\mathrm{Sp}(\underline{w}_1, \ldots, \underline{w}_r)$;
  - if the $\underline{w}_j$s are column vectors the transposes of the non-zero rows of E are a basis for $\mathrm{Sp}(\underline{w}_1, \ldots, \underline{w}_r)$.

7. How to find a basis for the range of a matrix

Proposition 1.5 proved that the range of a matrix is the linear span of its columns. A basis for $\mathcal{R}(A)$ is therefore a basis for the column space of A. Take the transpose of A and compute $\underline{\mathsf{rref}}(A^T)$. The non-zero rows of $\underline{\mathsf{rref}}(A^T)$ are a basis for the row space of A^T. The transposes of the non-zero rows in $\underline{\mathsf{rref}}(A^T)$ are therefore a basis for the column space, and hence the range, of A.

Try an example!

8. Rank + Nullity

The <u>nullity</u> of a matrix A is the dimension of its null space.

As a consequence of the following important result we shall see that the dimension of the range of A is equal to the rank of A (Corollary 8.2). In many books the rank of a matrix is *defined* to be the dimension of its range. Accordingly, the formula in the next result is often stated as

$$\operatorname{nullity} A + \operatorname{rank}(A) = n.$$

THEOREM 8.1. *Let A be an $m \times n$ matrix. Then*

$$\dim \mathcal{N}(A) + \dim \mathcal{R}(A) = n.$$

Proof. Pick bases $\{\underline{u}_1, \ldots, \underline{u}_p\}$ for $\mathcal{N}(A)$ and $\{\underline{w}_1, \ldots, \underline{w}_q\}$ for $\mathcal{R}(A)$. Remember that $\mathcal{N}(A) \subseteq \mathbb{R}^n$ and $\mathcal{R}(A) \subseteq \mathbb{R}^m$.

There are vectors $\underline{v}_1, \ldots, \underline{v}_q$ in $\mathbb{R}^n$ such that $\underline{w}_i = A\underline{v}_i$ for all i. We will show that the set

$$\mathcal{B} := \{\underline{u}_1, \ldots, \underline{u}_p, \underline{v}_1, \ldots, \underline{v}_q\}$$

is a basis for $\mathbb{R}^n$.

Let $\underline{x} \in \mathbb{R}^n$. Then $A\underline{x} = a_1\underline{w}_1 + \cdots + a_q\underline{w}_q$ for some $a_1, \ldots, a_q \in \mathbb{R}$. Now

$$A\big(\underline{x} - a_1\underline{v}_1 - \cdots - a_q\underline{v}_q\big) = A\underline{x} - a_1A\underline{v}_1 - \cdots - a_qA\underline{v}_q = 0$$

so $\underline{x} - a_1\underline{v}_1 - \cdots - a_q\underline{v}_q$ is in the null space of A and therefore

$$\underline{x} - a_1\underline{v}_1 - \cdots - a_q\underline{v}_q = b_1\underline{u}_1 + \ldots + b_p\underline{u}_p$$

for some $b_1, \ldots, b_p \in \mathbb{R}$. In particular,

$$\underline{x} = a_1\underline{v}_1 + \cdots + a_q\underline{v}_q + b_1\underline{u}_1 + \ldots + b_p\underline{u}_p$$

so $\mathcal{B}$ spans $\mathbb{R}^n$.

We will now show that $\mathcal{B}$ is linearly independent. If

$$c_1\underline{v}_1 + \cdots + c_q\underline{v}_q + d_1\underline{u}_1 + \ldots + d_p\underline{u}_p = 0,$$

then

$$\begin{aligned} 0 &= A\big(c_1\underline{v}_1 + \cdots + c_q\underline{v}_q + d_1\underline{u}_1 + \ldots + d_p\underline{u}_p\big) \\ &= c_1A\underline{v}_1 + \cdots + c_qA\underline{v}_q + d_1A\underline{u}_1 + \ldots + d_pA\underline{u}_p \\ &= c_1\underline{w}_1 + \cdots + c_q\underline{w}_q + 0 + \ldots + 0. \end{aligned}$$

But $\{\underline{w}_1, \ldots, \underline{w}_q\}$ is linearly independent so

$$c_1 = \cdots = c_q = 0.$$

Therefore

$$d_1\underline{u}_1 + \ldots + d_p\underline{u}_p = 0.$$

But $\{\underline{u}_1, \ldots, \underline{u}_p\}$ is linearly independent so

$$d_1 = \cdots = d_p = 0.$$

Hence $\mathcal{B}$ is linearly independent, and therefore a basis for $\mathbb{R}^n$. But $\mathcal{B}$ has $p + q$ elements so $p + q = n$, as required. $\square$

We now give the long-promised new interpretation of $\operatorname{rank}(A)$.

COROLLARY 8.2. *Let A be an $m \times n$ matrix. Then*

$$\operatorname{rank}(A) = \dim \mathcal{R}(A).$$

Proof. In chapter 7, we defined $\operatorname{rank}(A)$ to be the number of non-zero rows in $\underline{\mathsf{rref}}(A)$, the row-reduced echelon form of A. From the discussion in that chapter we obtain

$$\begin{aligned} n - \operatorname{rank}(A) &= \text{the number of independent variables} \\ &\qquad \text{for the equation } A\underline{x} = 0 \\ &= \dim\{\underline{x} \in \mathbb{R}^n \mid A\underline{x} = 0\} \\ &= \dim \mathcal{N}(A). \end{aligned}$$

But $\dim \mathcal{N}(A) = n - \dim \mathcal{R}(A)$ by Theorem 8.1, so $\operatorname{rank}(A) = \dim \mathcal{R}(A)$. $\square$

COROLLARY 8.3. *Let A be an $m \times n$ matrix. Then*

$$\operatorname{nullity} A + \operatorname{rank}(A) = n.$$

COROLLARY 8.4. *The row space and column spaces of a matrix have the same dimension.*

Proof. Let A be an $m \times n$ matrix. By Proposition 1.5, the column space of A is equal to $\mathcal{R}(A)$. The row space of A is equal to the row space of $\underline{\mathsf{rref}}(A)$ so the dimension of the row space of A is $\operatorname{rank}(A)$. But $\operatorname{rank}(A) = \dim \mathcal{R}(A)$. The result follows. $\square$

COROLLARY 8.5. *Let A be an $m \times n$ matrix. Then*

$$\operatorname{rank}(A) = \operatorname{rank}(A^T).$$

Proof. The rank of A^T is equal to the dimension of its row space which is equal to the dimension of the column space of A which is equal to the dimension of the row space of A which is equal to the rank of A. $\square$

We will now give some examples that show how to use Theorem 8.1.

8.1. 3×3 examples. There are four possibilities for the rank and nullity of a 3×3 matrix.

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

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

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

8.2. Planes in $\mathbb{R}^4$. Let V and V' be two dimensional subspaces of $\mathbb{R}^4$. The intersection of V and V' is a subspace of $\mathbb{R}^4$ of dimension ≤ 2 so their are three possibilities: the intersection is 2-dimensional if and only if $V = V'$; if the intersection is 1-dimensional, then V and V' have a line in common; if $V \cap V' = \{\underline{0}\}$, then $V + V' = \mathbb{R}^4$.

Let P and P' be planes in $\mathbb{R}^4$, i.e., translations of 2-dimensional subspaces. We say that P and P' are parallel if they are translates of the same 2-dimensional subspace. In that case, $P \cap P' = \phi$ but that is not the only reason two planes can fail to meet.

8.3. 3-planes in $\mathbb{R}^5$. We call a 3-dimensional subspace of $\mathbb{R}^n$ a 3-plane. Let V and V' be 3-planes

8.4. Three formulas. There are many examples in mathematics where the same idea pops up in very different settings. Here is an example:

- If U and V are subspaces of $\mathbb{R}^n$, then
$$\dim(U+V) = \dim U + \dim V - \dim(U \cap V)$$
- If A and B are finite sets, then
$$|A \cup B| = |A| + |B| - |A \cap B|.$$
- Let A and B denote events; let $A \cup B$ denote the event *either A or B occurs*, and let $A \cap B$ denote the event *both A and B occur*. If $P[\text{event}]$ denotes the probability of an event, then
$$P[A \cup B] = P[A] + P[B] - P[A \cap B].$$

LEMMA 8.6. *Let W and W' be subspaces of $\mathbb{R}^n$ and suppose that $W \subseteq W'$. If $\underline{w}_1, \ldots, \underline{w}_m$ is a basis for W, then there is a basis for W' that contains $\underline{w}_1, \ldots, \underline{w}_m$.*

Proof. We argue by induction on $\dim W' - \dim W$. Suppose $\dim W' = 1 + \dim W$. Let $\underline{w}' \in W' - W$. Then $\{\underline{w}', \underline{w}_1, \ldots, \underline{w}_m\}$ is linearly independent, and hence a basis for W'. etc. □

PROPOSITION 8.7. *If U and V are subspaces of $\mathbb{R}^n$, then*
$$\dim(U+V) = \dim U + \dim V - \dim(U \cap V)$$

Proof. Let $\mathcal{B}$ be a basis for $U \cap V$. Then there is a basis $\mathcal{B} \sqcup \mathcal{B}_U$ for U and a basis $\mathcal{B} \sqcup \mathcal{B}_V$ for V. We will now show that $\mathcal{B} \sqcup \mathcal{B}_U \sqcup \mathcal{B}_V$ is a basis for $U + V$.

Hence
$$\dim(U+V) = |\mathcal{B}| + |\mathcal{B}_U| + |\mathcal{B}_V|.$$
But $|\mathcal{B}| = \dim U \cap V$, $|\mathcal{B}| + |\mathcal{B}_U| = \dim U$, and $|\mathcal{B}| + |\mathcal{B}_V| = \dim V$, so
$$|\mathcal{B}| + |\mathcal{B}_U| + |\mathcal{B}_V| = \dim U + \dim V - \dim U \cap V$$
thus proving the result. □

9. How to compute the null space and range of a matrix

Suppose you are given a matrix A and asked to compute its null space and range. What would constitute an answer to that question? One answer would be to provide a basis for its null space and a basis for its range.

By definition, the null space of A is the set of solutions to the equation $A\underline{x} = 0$ so we may use the methods in chapters 7 and 8 to find the solutions. Do elementary row operations to find $\underline{\mathsf{rref}}(A)$. Write E for $\underline{\mathsf{rref}}(A)$. Since the equations $A\underline{x} = \underline{0}$ and $E\underline{x} = \underline{0}$ have the same solutions,

$$\mathcal{N}(A) = \mathcal{N}(E).$$

It is easy to write down the null space for E. For example, suppose If

$$E = \begin{pmatrix} 1 & 0 & 2 & 0 & 0 & 3 & 4 \\ 0 & 1 & 3 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 1 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{9-1}$$

the dependent variables are x_1, x_2, x_4, and x_5. The independent variables x_3, x_6, and x_7, may take any values and then the dependent variables are determined by the equations

$$\begin{aligned} x_1 &= -2x_3 - 3x_6 - 4x_7 \\ x_2 &= -3x_3 - 4x_6 \\ x_4 &= \qquad\quad 2x_6 + x_7 \\ x_5 &= \qquad\quad -x_6 + 2x_7. \end{aligned}$$

Now set any one of the independent variables to 1 and set the others to zero. This gives solutions

$$\begin{pmatrix} -2 \\ -3 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} -3 \\ -4 \\ 0 \\ 2 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} -4 \\ 0 \\ 0 \\ 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}.$$

These are elements of the null space and are obviously linearly independent. They span the null space.

MORE TO SAY/DO...basis for null space

CHAPTER 11

Linear transformations

Linear transformations are special kinds of functions between vector spaces. Subspaces of a vector space are of crucial importance and linear transformations are precisely those functions between vector spaces that send subspaces to subspaces. More precisely, if $T : V \to W$ is a linear transformation and U is a subspace of V, then

$$\{T(\underline{u}) \mid \underline{u} \in U\}$$

is a subspace of W. That subspace is often called the image of U under T.

1. A reminder on functions

Let X and Y be any sets. A function f from X to Y, often denoted $f : X \to Y$, is a rule that associates to each element $x \in X$ a single element $f(x)$ that belongs to Y. It might be helpful to think of f as a machine: we put an element of X into f and f spits out an element of Y. We call $f(x)$ the image of x under f. We call X the domain of f and Y the codomain.

The range of f is the subset $\mathcal{R}(f) := \{f(x) \mid x \in X\} \subseteq Y$. The range of f might or might not equal Y. For example, the functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}_{\geq 0}$ given by the formulas $f(x) = x^2$ and $g(x) = x^2$ are *different functions* even though they are defined by the same formula. The range g is equal to the codomain of g. The range of f is not equal to the codomain of f.

Part of you might rebel at this level of precision and view it as pedantry for the sake of pedantry. However, as mathematics has developed it has become clear that such precision is necessary and useful. A great deal of mathematics involves formulas but those formulas are used to define functions and we add a new ingredient, the domain and codomain.

You have already met some of this. For example, the function $f(x) = \frac{1}{x}$ is not defined at 0 so is not a function from $\mathbb{R}$ to $\mathbb{R}$. It is a function from $\mathbb{R} - \{0\}$ to $\mathbb{R}$. The range of f is not $\mathbb{R}$ but $\mathbb{R} - \{0\}$. Thus the function $f : \mathbb{R} - \{0\} \to \mathbb{R} - \{0\}$ defined by the formula $f(x) = \frac{1}{x}$ has an inverse, namely itself.

At first we learn that the number 4 has two square roots, 2 and -2, but when we advance a little we define the square root function $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$. This is because we want the function $f(x) = x^2$ to have an inverse. The desire to have inverses often makes it necessary to restrict the domain or codomain. A good example is the inverse sine function. Look at the definition of $\sin^{-1}(-)$ in your calculus book, or on the web, and notice how much care is taken with the definition of the codomain.

2. First observations

Let V be a subspace of $\mathbb{R}^n$ and W a subspace of $\mathbb{R}^m$. A linear transformation from V to W is a function $F : V \to W$ such that

(1) $F(\underline{u}+\underline{v}) = F(\underline{u}) + F(\underline{v})$ for all $\underline{u}, \underline{v} \in V$, and
(2) $F(a\underline{v}) = aF(\underline{v})$ for all $a \in \mathbb{R}$ and all $\underline{v} \in V$.

It is common to combine (1) and (2) into a single condition: F is a linear transformation if and only if

$$F(a\underline{u} + b\underline{v}) = aF(\underline{u}) + bF(\underline{v})$$

for all $a, b \in \mathbb{R}$ and all $\underline{u}, \underline{v} \in V$.

2.1. Equality of linear transformations. Two linear transformations from V to W are equal if they take the same value at all points of V. This is the same way we define equality of functions: f and g are equal if they take the same values everywhere.

2.2. Linear transformations send $\underline{0}$ to $\underline{0}$. The only distinguished point in a vector space is the zero vector, $\underline{0}$. It is nice that linear transformations send $\underline{0}$ to $\underline{0}$.

LEMMA 2.1. *If $T : V \to W$ is a linear transformation, then $T(\underline{0}) = \underline{0}$.*[1]

Proof. The following calculation proves the lemma:

$$\begin{aligned} \underline{0} &= T(\underline{0}) - T(\underline{0}) \\ &= T(\underline{0}+\underline{0}) - T(\underline{0}) \\ &= T(\underline{0}) + T(\underline{0}) - T(\underline{0}) \quad \text{by property (1)} \\ &= T(\underline{0}) + \underline{0} \\ &= T(\underline{0}). \end{aligned}$$

□

This proof is among the simplest in this course. Those averse to reading proofs should look at each step in the proof, i.e., each = sign, and ask what is the justification for that step. Ask me if you don't understand it.

2.3. The linear transformations $\mathbb{R} \to \mathbb{R}$.

[1] When we write $T(\underline{0}) = \underline{0}$ we are using the same symbol $\underline{0}$ for two different things: the $\underline{0}$ in $T(\underline{0})$ is the zero in V and the other $\underline{0}$ is the zero in W. We could write $T(\underline{0}_V) = \underline{0}_W$ but that looks a little cluttered. It is also unnecessary because T is a function from V to W so the only elements we can put into $T(-)$ are elements of V, so for $T(\underline{0})$ to make sense the $\underline{0}$ in $T(\underline{0})$ *must* be the zero in V; likewise, T spits out elements of W so $T(\underline{0})$ *must* be an element of W.

2.4. T respects linear combinations. Let $T : V \to W$ be a linear transformation. If $\underline{v}_1, \underline{v}_2, \underline{v}_3 \in V$ and $a_1, a_2, a_3 \in \mathbb{R}$, then

$$\begin{aligned} T(a_1\underline{v}_1 + a_2\underline{v}_2 + a_3\underline{v}_3) &= T((a_1\underline{v}_1 + a_2\underline{v}_2) + a_3\underline{v}_3) \\ &= T(a_1\underline{v}_1 + a_2\underline{v}_2) + a_3T(\underline{v}_3) \\ &= a_1T(\underline{v}_1) + a_2T(\underline{v}_2) + a_3T(\underline{v}_3) \end{aligned}$$

An induction argument shows that if $\underline{v}_1, \ldots, \underline{v}_p \in V$ and $a_1, \ldots, a_p \in \mathbb{R}$, then

$$T(a_1\underline{v}_1 + \cdots + a_p\underline{v}_p) = a_1T(\underline{v}_1) + \cdots + a_pT(\underline{v}_p). \tag{2-1}$$

2.5. T is determined by its action on a basis. There are two ways to formalize the statement that a linear transformation is completely determined by its values on a basis.

Let $T : V \to W$ be a linear transformation and suppose $\{\underline{v}_1, \ldots, \underline{v}_p\}$ is a basis for V.

(1) If you know the values of $T(\underline{v}_1), \ldots, T(\underline{v}_p)$ you can compute its value at every point of V because if $\underline{v} \in V$ there are unique numbers $a_1, \ldots, a_p \in \mathbb{R}$ such that $\underline{v} = a_1\underline{v}_1 + \cdots + a_p\underline{v}_p$ and it now follows from (2-1) that $T(\underline{v}) = a_1T(\underline{v}_1) + \cdots + a_pT(\underline{v}_p)$.
(2) If $S : V \to W$ is another linear transformation such that $S(\underline{v}_i) = T(\underline{v}_i)$ for $i = 1, \ldots, p$, then $S = T$. To see this use (2-1) twice: once for S and once for T.

2.6. How do we tell if a function $T : V \to W$ is a linear transformation? As with all such questions, the answer is to check whether T satisfies the definition or not.

PAUL - examples,

The function $f : \mathbb{R}^2 \to \mathbb{R}^2$ given by

$$f(x, y) = \begin{cases} (x + y, x - y) & \text{if } x \geq 0 \text{ and } y \geq 0 \\ (x - y, x + y) & \text{otherwise} \end{cases}$$

is not a linear transformation because _________

2.7. The zero transformation. The function $V \to W$ that sends every $\underline{x} \in V$ to the zero vector in W is a linear transformation (check!). We call this the *zero linear transformation* and denote it by 0 if necessary.

2.8. The identity transformation. The function $V \to V$ that sends every $\underline{x} \in V$ to itself is a linear transformation (check!). We call it the *identity transformation of* V and denote it by id_V.

2.9. A composition of linear transformations is a linear transformation. If $S : V \to W$ and $T : U \to V$ are linear transformations, their *composition*, denoted by ST or $S \circ T$, is defined in the same way as the composition of any two functions, namely

$$(ST)(\underline{u}) = S(T(\underline{u})) \qquad \text{or} \qquad (S \circ T)(\underline{u}) = S(T(\underline{u})).$$

This makes sense because $T(\underline{u}) \in V$ and we can apply S to elements of V. Thus

$$ST : U \to W.$$

To see that ST is really a linear combination suppose that $\underline{u}$ and $\underline{u}'$ belong to U and that $a, a' \in \mathbb{R}$. Then

$$\begin{aligned}(ST)(a\underline{u} + a'\underline{u}') &= S(T(a\underline{u} + a'\underline{u}')) && \text{by definition of } ST \\ &= S(aT(\underline{u}) + a'T(\underline{u}')) && \text{because } T \text{ is a linear transformation} \\ &= aS(T(\underline{u})) + a'S(T(\underline{u}')) && \text{because } S \text{ is a linear transformation} \\ &= a(ST)(\underline{u}) + a'(ST)(\underline{u}') && \text{by definition of } ST\end{aligned}$$

so ST is a linear transformation.

2.10. A linear combination of linear transformations is a linear transformation. If S and T are linear transformations from U to V and $a, b \in \mathbb{R}$, we define the function $aS + bT$ by

$$(aS + bT)(\underline{x}) := aS(\underline{x}) + bT(\underline{x}).$$

It is easy to check that $aS + bT$ is a linear transformation from U to V too. We call it a linear combination of S and T. Of course the idea extends to linear combinations of larger collections of linear transformations.

3. Linear transformations and matrices

Let A be an $m \times n$ matrix and define $T : \mathbb{R}^n \to \mathbb{R}^m$ by $T(\underline{x}) := A\underline{x}$. Then T is a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$. The next theorem says that *every* linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$ is of this form.

THEOREM 3.1. *Let $T : \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Then there is a unique $m \times n$ matrix A such that $T(\underline{x}) = A\underline{x}$ for all $\underline{x} \in \mathbb{R}^n$.*

Proof. Let A be the $m \times n$ matrix whose j^{th} column is $\underline{A}_j := T(\underline{e}_j)$. If $\underline{x} = (x_1, \ldots, x_n)^T$ is an arbitrary element of $\mathbb{R}^n$, then

$$\begin{aligned}T(\underline{x}) &= T(x_1\underline{e}_1 + \cdots + x_n\underline{e}_n) \\ &= x_1T(\underline{e}_1) + \cdots + x_nT(\underline{e}_n) \\ &= x_1\underline{A}_1 + \cdots + x_n\underline{A}_n \\ &= A\underline{x}\end{aligned}$$

as required. □

In the context of the previous theorem, we sometimes say that the matrix A represents the linear transformation T.

Suppose $T : \mathbb{R}^k \to \mathbb{R}^m$ and $S : \mathbb{R}^m \to \mathbb{R}^n$ are linear transformations and A and B matrices such that $T(\underline{x}) = A\underline{x}$ for all $\underline{x} \in \mathbb{R}^k$ and $S(\underline{y}) = B\underline{y}$ for all $\underline{y} \in \mathbb{R}^m$, then $(S \circ T)(\underline{x}) = BA\underline{x}$ for all $\underline{x} \in \mathbb{R}^k$. Thus

multiplication of matrices corresponds to
composition of linear transformations

or

multiplication of matrices is defined so that the matrix
representing the composition of two linear transformations
is the product of the matrices representing each linear transformation.

This is of great importance. It explains why the multiplication of matrices is defined as it is. That last sentence bears repeating. The fact that matrix multiplication has real meaning, as opposed to something that was defined by a committee that just wanted to be able to "multiply" matrices, is due to the fact that matrix multiplication corresponds to that most natural of operations, composition of functions, first do one, then the other.

Mathematics is not about inventing definitions just for the heck of it and seeing what one can deduce from them. Every definition is motivated by some problem, question, or naturally occurring object or feature. Linear transformations and compositions of them are more fundamental than matrices and their product. Matrices are tools for doing calculations with linear transformations. They sometimes convey information that is concealed in other presentations of linear transformations.

We introduce you to matrices before linear transformations because they are more concrete and down to earth, not because they are more important than linear transformations.

3.1. Isomorphisms. Suppose that $S : V \to U$ and $T : U \to V$ are linear transformations. Then $ST : U \to U$ and $TS : V \to V$. If $ST = \mathrm{id}_U$ and $TS = \mathrm{id}_V$ we say that S and T are inverses to one another. We also say that S and T are isomorphisms and that U and V are isomorphic vector spaces.

THEOREM 3.2. *Let V be a subspace of $\mathbb{R}^n$. If $\dim V = d$, then V is isomorphic to $\mathbb{R}^d$.*

Proof. Let $\underline{v}_1, \ldots, \underline{v}_d$ be a basis for V. Define $T : \mathbb{R}^d \to V$ by

$$T(a_1, \ldots, a_d) := a_1\underline{v}_1 + \cdots + a_d\underline{v}_d.$$

MORE TO DO

$S : V \to \mathbb{R}^d$ by □

4. How to find the matrix representing a linear transformation

The solution to this problem can be seen from the proof of Theorem 3.1. There, the matrix A such that $T(\underline{x}) = A\underline{x}$ for all $\underline{x} \in \mathbb{R}^n$ is constructed one column at a time: the i^{th} column of A is $T(\underline{e}_i)$.

PAUL–explicit example.

5. Invertible matrices and invertible linear transformations

6. How to find the formula for a linear transformation

First, what do we mean by a formula for a linear transformation? We mean the same thing as when we speak of a formula for one of the functions you met in calculus—the only difference is the appearance of the formula. For example, in calculus $f(x) = x \sin x$ is a formula for the function f; similarly, $g(x) = |x|$ is a formula for the function g; we can also give the formula for g by

$$g(x) = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x \leq 0. \end{cases}$$

The expression

$$T\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 2a-b \\ a \\ a+b+c \\ 3c-2b \end{pmatrix}$$

is a formula for a linear transformation $T : \mathbb{R}^3 \to \mathbb{R}^4$.

Although a linear transformation may not be given by an explicit formula, we might want one in order to do calculations. For example, rotation about the origin in the clockwise direction by an angle of $45°$ is a linear transformation, but that description is not a formula for it. A formula for it is given by

$$T\begin{pmatrix} a \\ b \end{pmatrix} = \tfrac{1}{\sqrt{2}}\begin{pmatrix} a+b \\ b-a \end{pmatrix} = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}.$$

Let $T : \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Suppose $\{\underline{v}_1, \ldots, \underline{v}_n\}$ is a basis for $\mathbb{R}^n$ and you are told the values of $T(\underline{v}_1), \ldots, T(\underline{v}_n)$. There is a simple procedure to find the $m \times n$ matrix A such that $T(\underline{x}) = A\underline{x}$ for all $\underline{x} \in \mathbb{R}^n$. The idea is buried in the proof of Theorem 3.1.

MORE TO DO

7. Rotations in the plane

Among the more important linear transformations $\mathbb{R}^2 \to \mathbb{R}^2$ are the rotations. Given an angle θ we write T_θ for the linear transformation that rotates a point by an angle of θ radians in the counterclockwise direction.

Before we obtain a formula for T_θ some things should be clear. First, $T_\theta T_\psi = T_{\theta+\psi}$. Second, $T_0 = 0$. Third, $T_{2n\pi} = \mathrm{id}_{\mathbb{R}^2}$ and $T_{(2n+1)\pi} = -\mathrm{id}_{\mathbb{R}^2}$ for all $n \in \mathbb{Z}$. Fourth, rotation in the counterclockwise direction by an angle of $-\theta$ is the same as rotation in the *clockwise* direction by an angle of θ so T_θ has an inverse, namely $T_{-\theta}$.

Let's write A_θ for the unique 2×2 matrix such that $T_\theta\underline{x} = A_\theta\underline{x}$ for all $\underline{x} \in \mathbb{R}^2$. The first column of A_θ is given by $T_\theta(\underline{e}_1)$ and the second column of A_θ is given by $T_\theta(\underline{e}_2)$. Elementary trigonometry (draw the diagrams and check!) then gives

$$A_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}. \tag{7-1}$$

There are many interesting aspects to this:

- if you have forgotten your formulas for $\sin(\theta+\psi)$ and $\cos(\theta+\psi)$ you can recover them by using the fact that $A_\theta A_\psi = A_{\theta+\psi}$ and computing the product on the left;
- the determinant of A_θ is 1 because $\cos^2\theta + \sin^2\theta = 1$;
- $A_\theta^{-1} = A_{-\theta}$ and using the formula for the inverse of a 2×2 matrix in Theorem 5.1 you can recover the formulae for $\sin(-\theta)$ and $\cos(-\theta)$ if you have forgotten them.

8. Reflections in $\mathbb{R}^2$

Let L be the line in $\mathbb{R}^2$ through the origin and a non-zero point $\begin{pmatrix} a \\ b \end{pmatrix}$. The reflection in L is the linear transformation that sends $\begin{pmatrix} a \\ b \end{pmatrix}$ to itself, i.e., it fixes every point on L, and sends the point $\begin{pmatrix} -b \\ a \end{pmatrix}$, which is orthogonal to L, to $\begin{pmatrix} b \\ -a \end{pmatrix}$.[2] Let A be the matrix implementing this linear transformation.

Since

$$\underline{e}_1 = \frac{1}{a^2+b^2}\left(a\begin{pmatrix} a \\ b \end{pmatrix} - b\begin{pmatrix} -b \\ a \end{pmatrix}\right)$$

and

$$\underline{e}_2 = \frac{1}{a^2+b^2}\left(b\begin{pmatrix} a \\ b \end{pmatrix} + a\begin{pmatrix} -b \\ a \end{pmatrix}\right)$$

we get

$$A\underline{e}_1 = \frac{1}{a^2+b^2}\left(a\begin{pmatrix} a \\ b \end{pmatrix} - b\begin{pmatrix} b \\ -a \end{pmatrix}\right) = \frac{1}{a^2+b^2}\begin{pmatrix} a^2-b^2 \\ 2ab \end{pmatrix}$$

and

$$A\underline{e}_2 = \frac{1}{a^2+b^2}\left(b\begin{pmatrix} a \\ b \end{pmatrix} + a\begin{pmatrix} b \\ -a \end{pmatrix}\right) = \frac{1}{a^2+b^2}\begin{pmatrix} 2ab \\ b^2-a^2 \end{pmatrix}$$

so

$$A = \frac{1}{a^2+b^2}\begin{pmatrix} a^2-b^2 & 2ab \\ 2ab & b^2-a^2 \end{pmatrix}$$

In summary, if $\underline{x} \in \mathbb{R}^2$, then $A\underline{x}$ is the reflection of $\underline{x}$ in the line $ay = bx$.

[2]Draw a picture to convince yourself that this does what you expect the reflection in L to do.

You might exercise your muscles by showing that all reflections are similar to one another. Why does it suffics to show each is similar to the reflection

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}?$$

8.1. Reflections in higher dimensions. Let $T : \mathbb{R}^n \to \mathbb{R}^n$. We call T a reflection if $T^2 = I$ and the 1-eigenspace of T has dimension $n - 1$.

9. Invariant subspaces

10. The one-to-one and onto properties

For a few moments forget linear algebra. The adjectives *one-to-one* and *onto* can be used with any kinds of functions, not just those that arise in linear algebra.

Let $f : X \to Y$ be a function between any two sets X and Y.

- We say that f is one-to-one if $f(x) = f(x')$ only when $x = x'$. Equivalently, f is one-to-one if it sends different elements of X to different elements of Y, i.e., $f(x) \neq f(x')$ if $x \neq x'$.
- The range of f, which we denote by $\mathcal{R}(f)$, is the set of all values it takes, i.e.,
$$\mathcal{R}(f) := \{f(x) \mid x \in X\}.$$
I like this definition because it is short but some prefer the equivalent definition
$$\mathcal{R}(f) := \{y \in Y \mid y = f(x) \text{ for some } \ x \in X\}.$$
- We say that f is onto if $\mathcal{R}(f) = Y$. Equivalently, f is onto if every element of Y is $f(x)$ for some $x \in X$.

10.1. The sine function $\sin : \mathbb{R} \to \mathbb{R}$ is not one-to-one because $\sin \pi = \sin 2\pi$. It is not onto because its range is $[-1, 1] = \{y \mid -1 \leq y \leq 1\}$. However, if we consider sin as a function from $\mathbb{R}$ to $[-1, 1]$ it is becomes onto, though it is still not one-to-one.

The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is not one-to-one because $f(2) = f(-2)$ for example, and is not onto because its range is $\mathbb{R}_{\geq 0} := \{y \in \mathbb{R} \mid ly \geq 0\}$. However, the function

$$f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, \qquad f(x) = x^2,$$

is both one-to-one and onto.

11. Two-to-two

One-to-one is a lousy choice of name. Two-to-two would be much better because a one-to-one function $f : X \to Y$ is a function having the property that it always sends two different elements x and x' in X to two two different elements $f(x)$ and $f(x')$ in Y. Of course, once one sees this, it follows that a one-to-one function is not only two-to-two but three-to-three, four-to-four, and so on; i.e., if $f : X \to Y$ is one-to-one and x_1, x_2, x_3, x_4 are four different elements of X, then $f(x_1), f(x_2), f(x_3), f(x_4)$ are four different elements of X

11.1. We can and do apply these ideas in the context of linear algebra. If T is a linear transformation we can ask whether T is one-to-one or onto.

For example, the linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ given by

$$T\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$$

is both one-to-one and onto.

The linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^3$ given by

$$T\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \\ x_1 + x_2 \end{pmatrix}$$

is one-to-one but not onto because $(0, 0, 1)^T$ is not in the range. Of course, since the range of T is a plane in $\mathbb{R}^3$ there are lots of other elements of $\mathbb{R}^3$ not in the range of T.

Proposition 11.1. *A linear transformation is one-to-one if and only if its null space is zero.*

Proof. Let T be a linear transformation. By definition, $\mathcal{N}(T) = \{\underline{x} \mid T(\underline{x}) = 0\}$. If T is one-to-one the only $\underline{x}$ with the property that $T(\underline{x}) = T(\underline{0})$ is $\underline{x} = \underline{0}$, so $\mathcal{N}(T) = \{\underline{0}\}$.

Conversely, suppose that $\mathcal{N}(T) = \{\underline{0}\}$. If $T(\underline{x}) = T(\underline{x}')$, then $T(\underline{x} - \underline{x}') = T(\underline{x}) - T(\underline{x}') = \underline{0}$ so $\underline{x} - \underline{x}' \in \mathcal{N}(T)$, whence $\underline{x} = \underline{x}'$ thus showing that T is one-to-one. □

Another way of saying this is that a linear transformation is one-to-one if and only if its nullity is zero.

12. Gazing into the distance: differential operators as linear transformations

You do not *need* to read this chapter. It is only for those who are curious enough to raise their eyes from the road we have been traveling to pause, refresh themselves, and gaze about in order to see more of the land we are entering. Linear algebra is a *big* subject that permeates and provides a framework for almost all areas of mathematics. So far we have seen only a small piece of this vast land.

We mentioned earlier that the set $\mathbb{R}[x]$ of all polynomials in x is a vector space with basis $1, x, x^2, \ldots$. Differentiation is a linear transformation

$$\frac{d}{dx} : \mathbb{R}[x] \to \mathbb{R}[x]$$

because

$$\frac{d}{dx}(af(x) + bg(x)) = a\frac{df}{dx} + b\frac{dg}{dx}.$$

If we write d/dx as a matrix with respect to the basis $1, x, x^2, \ldots$, then

$$\frac{d}{dx} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 2 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 3 & 0 & 0 & \cdots \\ \vdots & & & & & & \vdots \end{pmatrix}$$

because $\frac{d}{dx}(x^n) = nx^{n-1}$.

The null space of $\frac{d}{dx}$ is the set of constant functions, the subspace $\mathbb{R}.1$. The range of $\frac{d}{dx}$ is all of $\mathbb{R}[x]$: every polynomial is a derivative of another polynomial.

Another linear transformation from $\mathbb{R}[x]$ to itself is "multiplication by x", i.e., $T(f) = xf$. The composition of two linear transformations is a linear transformation. In particular, we can compose x and $\frac{d}{dx}$ to obtain another linear transformation. There are two compositions, one in each order. It is interesting to compute the difference of these two compositions. Let's do that

Write $T : \mathbb{R}[x] \to \mathbb{R}[x]$ for the linear transformation $T(f) = xf$ and $D : \mathbb{R}[x] \to \mathbb{R}[x]$ for the linear transformation $D(f) = f'$, the derivative of f with respect to x. Then, applying the product rule to compute the derivative of the product xf, we have

$$(DT - TD)(f) = D(xf) - xf' = f + xf' - xf' = f.$$

Thus $DT - TD = I$, the identity transformation.

MORE to say, Heisenberg's Uncertainty Principle.

12.1. Higher-order matrix equations. This course is all about solving equations in matrices. At high school you learned something about solving equations in which the solution is a number, i.e., a 1×1 matrix. In this course you are learning about solving equations in which the solution is a column vector, an $n \times 1$ matrix. An obvious next step is to consider equations in which the solutions are matrices.

For example, at high school solving the two equations $x^2 + y^2 = 1$ and $x - y = \frac{1}{2}$ amounts to finding the two points where the circle meets the line. The solutions are 1×2 matrices. However, you could also consider the problem of finding all 2×2 matrices x and y such that $x^2 + y^2 = 1$ and $x - y = \frac{1}{2}$.

MORE to say

Find all $n \times n$ matrices E, F, H, such that

$$\begin{aligned} HE - EH &= 2E \\ EF - FE &= H \\ HF - FH &= -2F. \end{aligned}$$

Because of the equivalence between matrices and linear transformations, which we discussed in chapter 3, this problem is equivalent to finding all linear transformations E, F, and H, from $\mathbb{R}^n$ to itself that simultaneously satisfy the three equations.

Let $\mathbb{R}[x,y]_n$ denote the $(n+1)$-dimensional vector space consisting of all homogeneous polynomials in two variables having degree n. A basis for this vector space is the set

$$x^n,\ x^{n-1}y,\ x^{n-2}y^2,\ \dots,\ xy^{n-1},\ y^n.$$

Thus the elements of $\mathbb{R}[x,y]_n$ consists of all linear combinations

$$a_nx^n + a_{n-1}x^{n-1}y + \cdots + a_1xy^{n-1} + a_0y^n.$$

Let ∂_x and ∂_y denote the partial derivatives with respect to x and y, respectively. These are linear transformations $\mathbb{R}[x,y]_n \to \mathbb{R}[x,y]_{n-1}$. We will write f_x for $\partial_x(f)$ and f_y for $\partial_y(f)$. Multiplication by x and multiplication by y are linear transformations $\mathbb{R}[x,y]_n \to \mathbb{R}[x,y]_{n+1}$. Therefore

$$E := x\partial_y, \quad H := x\partial_x - y\partial_y, \quad F := y\partial_x$$

are linear transformations $\mathbb{R}[x,y]_n \to \mathbb{R}[x,y]_n$ for every n. The action of $EF - FE$ on a polynomial f is

$$\begin{aligned}
(EF - FE)(f) &= \big(x\partial_y y\partial_x - y\partial_x x\partial_y\big)(f)\\
&= x\partial_y(yf_x) - y\partial_x(xf_y)\\
&= x(f_x + yf_{xy}) - y(f_y + xf_{yx})\\
&= xf_x + xyf_{xy} - yf_y - yxf_{yx}\\
&= xf_x - yf_y\\
&= \big(x\partial_x - y\partial_y\big)(f)\\
&= H(f).
\end{aligned}$$

Since the transformations $EF - FE$ and H act in the same way on every function f, they are equal; i.e., $EF - FE = H$. We also have

$$\begin{aligned}
(HE - EH)(f) &= \Big(\big(x\partial_x - y\partial_y\big)\big(x\partial_y\big) - \big(x\partial_y\big)\big(x\partial_x - y\partial_y\big)\Big)(f)\\
&= \big(x\partial_x - y\partial_y\big)(xf_y) - \big(x\partial_y\big)(xf_x - yf_y)\\
&= x(f_y + xf_{yx}) - yxf_{yy} - x^2f_{xy} + x(f_y + yf_{yy})\big)\\
&= 2xf_y\\
&= 2\big(x\partial_y\big)(f)\\
&= 2E(f).
\end{aligned}$$

Therefore $HE - EH = 2E$. I leave you to check that $HF - FH = -2F$.

This example illuminates several topics we have discussed. The null space of E is $\mathbb{R}x^n$. The null space of F is $\mathbb{R}y^n$. Each $x^{n-i}y^i$ is an eigenvector for H having eigenvalue $n - 2i$. Thus H has $n + 1$ distinct eigenvalues $n, n-2, n-4, \dots, 2-n, -n$ and, as we prove in greater generality in Theorem 1.2, these eigenvectors are linearly independent.

MORE to say – spectral lines....

CHAPTER 12

Determinants

The determinant of an $n \times n$ matrix A, which is denoted $\det(A)$, is a number computed from the entries of A having the wonderful property that:

A is invertible if and only if $\det(A) \neq 0$.

We will prove this in Theorem 3.1 below.

Sometimes, for brevity, we denote the determinant of A by $|A|$.

1. The definition

We met the determinant of a 2×2 matrix in Theorem 5.1:

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc.$$

The formula for the determinant of an $n \times n$ matrix is more complicated. It is defined inductively by which I mean that the formula for the determinant of an $n \times n$ matrix involves the formula for the determinant of an $(n-1) \times (n-1)$ matrix.

1.1. The 3×3 case. The determinant $\det(A) = \det(a_{ij})$ of a 3×3 matrix is the number

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

$$= a_{11}\left(a_{22}a_{33} - a_{23}a_{32}\right) - a_{12}\left(a_{21}a_{33} - a_{23}a_{31}\right) + a_{13}\left(a_{21}a_{32} - a_{22}a_{31}\right)$$

The coefficients a_{11}, a_{12}, and a_{13}, on the right-hand side of the formula are the entries in the top row of A and they appear with alternating signs $+1$ and -1; each a_{1j} is then multiplied by the determinant of the 2×2 matrix obtained by deleting the row and column that contain a_{1j}, i.e., deleting the top row and the j^{th} column of A.

In the second line of the expression for $\det(A)$ has $3 \times 2 = 6 = 3!$ terms. Each term is a product of three entries and those three entries are distributed so that each row of A contains exactly one of them and each column of A contains exactly one of them. In other words, each term is a product $a_{1p}a_{2q}a_{3r}$ where $\{p, q, r\} = \{1, 2, 3\}$.

1.2. The 4×4 case. The determinant $\det(A) = \det(a_{ij})$ of a 4×4 matrix is the number

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{34} \\ a_{42} & a_{43} & a_{44} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} & a_{24} \\ a_{31} & a_{33} & a_{34} \\ a_{41} & a_{43} & a_{44} \end{vmatrix}$$
$$+ a_{13} \begin{vmatrix} a_{21} & a_{22} & a_{24} \\ a_{31} & a_{32} & a_{34} \\ a_{41} & a_{42} & a_{44} \end{vmatrix} - a_{14} \begin{vmatrix} a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \end{vmatrix}.$$

Look at the similarities with the 3×3 case. Each entry in the top row of A appears as a coefficient with alternating signs $+1$ and -1 in the formula on the right. Each a_{1j} is then multiplied by the determinant of the 3×3 matrix obtained by deleting the row and column that contain a_{1j}, i.e., deleting the top row and the j^{th} column of A. Multiplying out the formula on the right yields a total of $4 \times 6 = 24 = 4!$ terms. Each term is a product of four entries and those four entries are distributed so that each row of A contains exactly one of them and each column of A contains one of them. In other words, each term is a product $a_{1p}a_{2q}a_{3r}a_{4s}$ where $\{p, q, r, s\} = \{1, 2, 3, 4\}$.

1.3. The $n \times n$ case. Let A be an $n \times n$ matrix. For each i and j between 1 and n we define the $(n-1) \times (n-1)$ matrix A^{ij} to be that obtained by deleting row i and column j from A. We then define

$$\det(A) := a_{11}|A^{11}| - a_{12}|A^{12}| + a_{13}|A^{13}| - \cdots + (-1)^{n-1}a_{1n}|A^{1n}|. \tag{1-1}$$

Each $|A^{ij}|$ is called the ij^{th} minor of A.

The expression (1-1) is said to be obtained by expanding A along its first column. There are similar expressions for the determinant of A that are obtained by expanding A along any row or column.

There are a number of observations to make about the formula (1-1). When the right-hand side is multiplied out one gets a total of $n!$ terms each of which looks like

$$\pm a_{1j_1}a_{2j_2}\cdots a_{nj_n} \tag{1-2}$$

where $\{j_1, \dots, j_n\} = \{1, \dots, n\}$. In particular, each row and each column contains exactly one of the factors $a_{1j_1}, a_{2j_2}, \dots, a_{nj_n}$.

PROPOSITION 1.1. *If A has a column of zeros, then* $\det(A) = 0$.

Proof. Suppose column j consists entirely if zeroes, i.e., $a_{1j} = a_{2j} = \cdots = a_{nj} = 0$. Consider one of the $n!$ terms in $\det(A)$, say $a_{1j_1}, a_{2j_2}, \dots, a_{nj_n}$. Because $\{j_1, \dots, j_n\} = \{1, \dots, n\}$, one of the factors a_{pj_p} in the product $a_{1j_1}, a_{2j_2}, \dots, a_{nj_n}$ belongs to column j, so is zero; hence $a_{1j_1}, a_{2j_2}, \dots, a_{nj_n} = 0$. Thus, every one of the $n!$ terms in $\det(A)$ is zero. Hence $\det(A) = 0$. □

A similar argument shows that $\det(A) = 0$ if one of the rows of A consists entirely of zeroes.

By Theorem **??**, A is not invertible if its columns are linearly dependent. Certainly, if one of the columns of A consists entirely of zeroes its columns are linearly dependent. As just explained, this implies that $\det(A) = 0$. This is consistent with the statement (not yet proved) at the beginning of this chapter that A is invertible if and only if $\det(A) \neq 0$.

1.4. The signs. The signs ± 1 are important. First let's just note that the coefficient of $a_{11}a_{22}\ldots a_{nn}$ is $+1$. This can be proved by induction: we have

$$\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & \ldots & a_{2n} \\ \vdots & & \vdots \\ a_{n2} & \ldots & a_{nn} \end{vmatrix} + \text{ other terms}$$

but a_{11} does not appear in any of the other terms. The coefficient of $a_{11}a_{22}\ldots a_{nn}$ in $\det(A)$ is therefore the same as the coefficient of $a_{22}\ldots a_{nn}$ in

$$\begin{vmatrix} a_{22} & \ldots & a_{2n} \\ \vdots & & \vdots \\ a_{n2} & \ldots & a_{nn} \end{vmatrix}$$

However, by an induction argument we can assume that the coefficient of $a_{22}\ldots a_{nn}$ in this smaller determinant is $+1$. Hence the coefficient of $a_{11}a_{22}\ldots a_{nn}$ in $\det(A)$ is $+1$.

In general, the sign in front of $a_{1j_1}a_{2j_2}\cdots a_{nj_n}$ is determined according to the following recipe: it is $+1$ if one can change the sequence $j_1, j_2, \ldots, j_n$ to $1, 2, \ldots, n$ by an *even* number of switches of adjacent numbers, and is -1 otherwise. For example, the coefficient of $a_{12}a_{23}a_{34}a_{45}a_{51}$ in the expression for the determinant of a 5×5 matrix is $+1$ because we need 4 switches

$$23451 \to 23415 \to 23145 \to 21345 \to 12345.$$

On the other hand, the coefficient of $a_{13}a_{24}a_{35}a_{42}a_{51}$ is -1 because we need 7 switches

$$34521 \to 34251 \to 34215 \to 32415 \to 32145 \to 23145 \to 21345 \to 12345.$$

1.5. The upper triangular case. An $n\times n$ matrix A is <u>upper triangular</u> if every entry below the main diagonal is zero; more precisely, if $a_{ij} = 0$ for all $i > j$. The next result shows that it is easy to compute the determinant of an upper triangular matrix: it is just the product of the diagonal entries.

THEOREM 1.2.

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{1n} \end{pmatrix} = a_{11}a_{22}\ldots a_{nn}.$$

Proof. The determinant is a sum of terms of the form

$$\pm a_{1j_1} a_{2j_2} \cdots a_{nj_n}$$

where $\{j_1, \ldots, j_n\} = \{1, \ldots, n\}$. For an upper triangular matrix this term can only be non-zero if $j_1 \geq 1$, and $j_2 \geq 2$, and $\ldots$, and $j_n \geq n$. But this can only happen if $j_1 = 1$, $j_2 = 2$, $\ldots$, and $j_n = n$. Hence the only non-zero term is $a_{11} a_{22} \ldots a_{nn}$ which, as we noted earlier, has coefficient $+1$. □

Thus, for example,

$$\det(I) = 1.$$

There is an analogue of Theorem 1.2 for lower triangular matrices.

2. Elementary row operations and determinants

Computing the determinant of a matrix directly from the definition is tedious and prone to arithmetic error. However, given A we can perform elementary row operations to get a far simpler matrix, say A', perhaps upper triangular, compute $\det(A')$ and, through repeated us of the next result, then determine $\det(A)$.

The row reduced echelon form of a square matrix is always upper triangular.

Proposition 2.1. *If B is obtained from A by the following elementary row operation the determinants are related in the following way:*

(2-1)

Elementary row operation	
• *switch two rows*	$\det(B) = -\det(A)$
• *multiply a row by $c \in \mathbb{R} - \{0\}$*	$\det(B) = c\det(A)$
• *replace row i by (row i + row k) with $i \neq k$*	$\det(B) = \det(A)$

In particular, $\det(A) = 0$ *if and only if* $\det(B) = 0$.

Proof. The second of these statements is obvious. Suppose we multiply row p by the number c. Each term $a_{1j_1} a_{2j_2} \cdots a_{nj_n}$ in $\det(A)$ contains exactly one factor from row p so each term in $\det(B)$ is c times the corresponding term in $\det(A)$. Hence $\det(B)$ is c times $\det(A)$.

We now prove the other two statements in the 2×2 case.

Switching two rows changes the sign because

$$\det \begin{pmatrix} c & d \\ a & b \end{pmatrix} = cb - ad = -(ad - bc) = -\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Adding one row to another doesn't change the sign because

$$\det \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = (a+c)b - (b+d)c = ad - bc = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

and

$$\det \begin{pmatrix} a & b \\ c+a & d+b \end{pmatrix} = a(d+b) - b(c+a) = -ad - bc = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{2-2}$$

Hence all three statements are true for a 2×2 matrix.

We now turn to the $n \times n$ case and argue by induction on n, i.e., we assume the result is true for $(n-1) \times (n-1)$ matrices and prove the result for the an $n \times n$ matrix.

Actually, the induction argument is best understood by looking at how the truth of the result for 2×2 matrices implies its truth for 3×3 matrices. Consider switching rows 2 and 3 in a 3×3 matrix. Since

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} \tag{2-3}$$

it follows that

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{31} & a_{32} & a_{33} \\ a_{21} & a_{22} & a_{23} \end{vmatrix} = a_{11} \begin{vmatrix} a_{32} & a_{33} \\ a_{22} & a_{23} \end{vmatrix} - a_{12} \begin{vmatrix} a_{31} & a_{33} \\ a_{21} & a_{23} \end{vmatrix} + a_{13} \begin{vmatrix} a_{31} & a_{32} \\ a_{21} & a_{22} \end{vmatrix}. \tag{2-4}$$

But the determinants of the three 2×2 matrices in this sum are the negatives of the three 2×2 determinants in (2-3). Hence the determinant of the 3×3 matrix in (2-4) is the negative of the determinant of the 3×3 matrix in (2-3). This "proves" that $\det(B) = -\det(A)$ if B is obtained from A by switching two rows.

Now consider replacing the third row of the 3×3 matrix A in (2-3) by the sum of rows 2 and 3 to produce B. Then $\det(B)$ is

$$\begin{aligned} \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{21}+a_{31} & a_{22}+a_{32} & a_{23}+a_{33} \end{vmatrix} = \; & a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{22}+a_{32} & a_{23}+a_{33} \end{vmatrix} \\ & - \; a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{21}+a_{31} & a_{23}+a_{33} \end{vmatrix} \\ & + \; a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{21}+a_{31} & a_{22}+a_{32} \end{vmatrix}. \end{aligned}$$

However, by the calculation in (2-2), this is equal to

$$a_{11} \begin{vmatrix} a_{32} & a_{33} \\ a_{22} & a_{23} \end{vmatrix} - a_{12} \begin{vmatrix} a_{31} & a_{33} \\ a_{21} & a_{23} \end{vmatrix} + a_{13} \begin{vmatrix} a_{31} & a_{32} \\ a_{21} & a_{22} \end{vmatrix}$$

i.e., $\det(B) = \det(A)$.

PAUL ... didn't cover the case of an ERO that involves row 1. □

PROPOSITION 2.2. *If A is an $n \times n$ matrix and E is an elementary matrix, then* $\det(EA) = \det(E)\det(A)$.

Proof. □

PROPOSITION 2.3. *Let A and A' be row equivalent $n \times n$ matrices. Then* $\det(A) = 0$ *if and only if* $\det(A') = 0$.

Proof. By hypothesis, A' is obtained from A by a sequence of elementary row operations. By Proposition 2.1, a single elementary row operation does not change whether the determinant of a matrix is zero or not. Therefore a sequence of elementary row operations does not change whether the determinant of a matrix is zero or not. □

3. The determinant and invertibility

THEOREM 3.1. *A square matrix is invertible if and only if its determinant is non-zero.*

Proof. Suppose A is an $n \times n$ matrix and let $E = \underline{\mathsf{rref}}(A)$. Then A and E have the same rank.

By Proposition 5.2, $E = I$ if $\operatorname{rank} E = n$, and E has a row of zeroes if $\operatorname{rank} E < n$. Since A is invertible if and only if $\operatorname{rank}(A) = n$, it follows that $\det(E) = 1$ if A is invertible and $\det(E) = 0$ if A is not invertible. The result now follows from Proposition 2.3. □

4. Properties

THEOREM 4.1. $\det(AB) = (\det A)(\det B)$.

Proof. We break the proof into two separate cases.

Suppose A and B are invertible. Then $A = E_1 \dots E_m$ and $B = E_{m+1} \dots E_n$ where each E_j is an elementary matrix. By repeated application of Proposition 2.2,

$$\begin{aligned} \det(A) &= \det(E_1 \dots E_m) \\ &= \det(E_1)\det(E_2 \dots E_m) \\ &= \cdots \\ &= \det(E_1)\det(E_2)\cdots\det(E_m). \end{aligned}$$

Applying the same argument to $\det(B)$ and $\det(AB)$ we see that $\det(AB) = (\det A)(\det B)$.

Suppose that either A or B is not invertible. Then AB is not invertible, so $\det(AB) = 0$ by Theorem 3.1. By the same theorem, either $\det(A)$ or $\det(B)$ is zero. Hence $\det(AB) = (\det A)(\det B)$ in this case too. □

COROLLARY 4.2. *If A is an invertible matrix, then* $\det(A^{-1}) = (\det A)^{-1}$.

Proof. It is clear that the determinant of the identity matrix is 1, so the result follows from Theorem 4.1 and the fact that $AA^{-1} = I$. □

$\det(A) = 0$ if two rows (or columns) of A are the same.
$\det(A^T) = \det(A)$.

5. Elementary column operations and determinants

As you might imagine, one can define elementary column operations in a way that is analogous to our definition of elementary row operations and the effect on the determinant of those operations on the determinant of a matrix parallels that on the effect of the elementary row operations.

5.1. Amusement. Here is an amusing use of the observation about the effect of the elementary column operations on the determinant.

The numbers 132, 144, and 156, are all divisible by 12. Then the determinant of

$$\begin{pmatrix} 1 & 3 & 2 \\ 1 & 4 & 4 \\ 1 & 5 & 6 \end{pmatrix}$$

is divisible by 12 because it is not changed by adding 100 times the 1st column and 10 times the second column to the third column whence

$$\det\begin{pmatrix} 1 & 3 & 2 \\ 1 & 4 & 4 \\ 1 & 5 & 6 \end{pmatrix} = \det\begin{pmatrix} 1 & 3 & 132 \\ 1 & 4 & 144 \\ 1 & 5 & 156 \end{pmatrix} = 12 \times \det\begin{pmatrix} 1 & 3 & 11 \\ 1 & 4 & 12 \\ 1 & 5 & 13 \end{pmatrix}.$$

Similarly, the numbers 289, 391, and 867, are all divisible by 17 so

$$\det\begin{pmatrix} 2 & 8 & 9 \\ 3 & 9 & 1 \\ 8 & 6 & 7 \end{pmatrix} = \det\begin{pmatrix} 2 & 8 & 289 \\ 3 & 9 & 391 \\ 8 & 6 & 867 \end{pmatrix} = 17 \times \det\begin{pmatrix} 2 & 8 & 17 \\ 3 & 9 & 23 \\ 8 & 6 & 51 \end{pmatrix}.$$

is divisible by 17.

Amuse your friends at parties.

5.2. A nice example. If the matrix

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

has rank ≤ 2, then

(1) $\underline{\mathsf{rref}}(A)$ has ≤ 2 non-zero rows so
(2) the row space of A has dimension ≤ 2 so
(3) any three rows of A are linearly dependent
(4) so $\det(\text{any 3 rows of } A) = 0$.

For example,

$$\begin{aligned} 0 = \det &\begin{pmatrix} b & c & d \\ a & -d & c \\ d & a & -b \end{pmatrix} \\ =& b(db - ac) - c(-ab - cd) + d(a^2 + d^2) \\ =& d(a^2 + b^2 + c^2 + d^2) \end{aligned}$$

Similarly, taking the determinant of the other three 3×3 submatrices of A gives

$$a(a^2+b^2+c^2+d^2) = b(a^2+b^2+c^2+d^2) = c(a^2+b^2+c^2+d^2) = 0.$$

If a, b, c, d are real numbers it follows that $a = b = c = d = 0$, i.e., A must be the zero matrix. However, if a, b, c, d are complex numbers A need not be zero because there are non-zero complex numbers a, b, c, d such that $a^2 + b^2 + c^2 + d^2 = 0$.

5.3. Permutations. You have probably met the word permutation meaning *arrangement* or *rearrangement* as in the question *"How many permutations are there of the numbers* $1, 2, \ldots, n$*?"* The answer, as you know, is $n!$.

We now define a <u>permutation</u> of the set $\{1, 2, \ldots, n\}$ as a function

$$\pi : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$$

that is one-to-one (or, equivalently, onto). Thus each term in the expression for the determinant of an $n \times n$ matrix (a_{ij}) is of the form

$$\pm a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)}. \tag{5-1}$$

The condition that π is one-to-one ensures that each row and each column contains exactly *one* of the terms in (5-1).

There area total of $n!$ permutations and the determinant of (a_{ij}) is the sum of $n!$ terms (5-1), one for each permutation. *However, there remains the issue of the* $\pm$ *signs.*

Let π be a permutation of $\{1, 2, \ldots, n\}$. Write $\pi(1), \pi(2), \ldots, \pi(n)$ one after the other. A <u>transposition</u> of this string of numbers is the string of numbers obtained by switching the positions of any two adjacent numbers. For example, if we start with 4321, then each of 3421, 4231, and 4312, is a transposition of 4321. It is clear that after some number of transpositions we can get the numbers back in their correct order. For example,

$$4321 \to 4312 \to 4132 \to 1432 \to 1423 \to 1243 \to 1234$$

or

$$4321 \to 4231 \to 2431 \to 2341 \to 2314 \to 2134 \to 1234.$$

If it takes an even number of transpositions to get the numbers back into their correct order we call the permutation <u>even</u>. If it takes an odd number we call the permutation <u>odd</u>. We define the <u>sign</u> of a permutation to be the number

$$\operatorname{sgn}(\pi) := \begin{cases} +1 & \text{if } \pi \text{ is even} \\ -1 & \text{if } \pi \text{ is odd} \end{cases}$$

It is not immediately clear that the sign of a permutation is well-defined. It is, but we won't give a proof.

The significance for us is that the coefficient of the term $a_{1\pi(1)}a_{2\pi(2)}\cdots a_{n\pi(n)}$ in the expression for the determinant is $\operatorname{sgn}(\pi)$. Hence

$$\det(a_{ij}) = \sum_{\pi} \operatorname{sgn}(\pi)\, a_{1\pi(1)}a_{2\pi(2)}\cdots a_{n\pi(n)}$$

where the sum is taken over all permutations of $\{1, 2, \ldots, n\}$.

Thus, the term $a_{14}a_{23}a_{32}a_{41}$ appears in the expression for the determinant of a 4×4 matrix with coefficient $+1$ because, as we saw above, it took an even number of transpositions (six) to get 4321 back to the correct order.

CHAPTER 13

Eigenvalues

Consider a fixed $n \times n$ matrix A. Viewed as a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^n$, A will send a line through the origin to either another line through the origin or zero. Some lines might be sent back to themselves. That is a nice situation: the effect of A on the points on that line is simply to scale them by some factor, λ say. The line $\mathbb{R}\underline{x}$ is sent by A to either zero or the line $\mathbb{R}(A\underline{x})$, so A sends this line to itself if and only if $A\underline{x}$ is a multiple of $\underline{x}$. This motivates the next definition.

1. Definitions and first steps

Let A be an $n \times n$ matrix. A number $\lambda \in \mathbb{R}$ is an eigenvalue for A if there is a *non-zero* vector $\underline{x}$ such that $A\underline{x} = \lambda\underline{x}$. If λ is an eigenvalue for A we define

$$E_\lambda := \{\underline{x} \mid A\underline{x} = \lambda\underline{x}\}.$$

We call E_λ the λ-eigenspace for A and the elements in E_λ are called eigenvectors or λ-eigenvectors for A.

We can define E_λ for any $\lambda \in \mathbb{R}$ but it is non-zero if and only if λ is an eigenvalue.[1]

Since

$$A\underline{x} = \lambda\underline{x} \iff 0 = A\underline{x} - \lambda\underline{x} = A\underline{x} - \lambda I\underline{x} = (A - \lambda I)\underline{x},$$

it follows that

$$E_\lambda = \mathcal{N}(A - \lambda I).$$

We have therefore proved that E_λ is a subspace of $\mathbb{R}^n$. The following theorem also follows from the observation that $E_\lambda = \mathcal{N}(A - \lambda I)$.

THEOREM 1.1. *Let A be an $n \times n$ matrix. The following are equivalent:*
(1) *λ is an eigenvalue for A;*
(2) *$A - \lambda I$ is singular;*
(3) $\det(A - \lambda I) = 0$.

Proof. Let $\lambda \in \mathbb{R}$. Then λ is an eigenvalue for A if and only if there is a non-zero vector $\underline{v}$ such that $(A - \lambda I)\underline{v} = 0$; but such a $\underline{v}$ exists if and only

[1] *Eigen* is a German word that has a range of meanings but the connotation here is probably closest to "peculiar to", or "particular to", or "characteristic of". The eigenvalues of a matrix are important characteristics of it.

if $A - \lambda I$ is singular. This proves the equivalence of (1) and (2). Theorem 3.1 tells us that (2) and (3) are equivalent statements. $\square$

THEOREM 1.2. *Let A be an $n \times n$ matrix and $\lambda_1, \ldots, \lambda_r$ distinct eigenvalues for A. If $\underline{v}_1, \ldots, \underline{v}_r$ are non-zero vectors such that $A\underline{v}_i = \lambda_i \underline{v}_i$ for each i, then $\{\underline{v}_1, \ldots, \underline{v}_r\}$ is linearly independent.*

Proof. Suppose the theorem is false. Let $m \geq 1$ be the smallest number such that $\{\underline{v}_1, \ldots, \underline{v}_m\}$ is linearly independent but $\{\underline{v}_1, \ldots, \underline{v}_m, \underline{v}_{m+1}\}$ is linearly dependent. Such an m exists because $\{\underline{v}_1\}$ is a linearly independent set.

There are numbers $a_1, \ldots, a_m$ such that $\underline{v}_{m+1} = a_1\underline{v}_1 + \cdots + a_r\underline{v}_m$. It follows that

$$\begin{aligned}
\lambda_{m+1}a_1\underline{v}_1 + \cdots + \lambda_{m+1}a_r\underline{v}_m &= \lambda_{m+1}\underline{v}_{m+1} \\
&= A\underline{v}_{m+1} \\
&= a_1A\underline{v}_1 + \cdots + a_rA\underline{v}_m \\
&= a_1\lambda_1\underline{v}_1 + \cdots + a_r\lambda_m\underline{v}_m.
\end{aligned}$$

Therefore

$$a_1(\lambda_{m+1} - \lambda_1)\underline{v}_1 + \cdots + a_r(\lambda_{m+1} - \lambda_m)\underline{v}_m = \underline{0}.$$

But $\{\underline{v}_1, \ldots, \underline{v}_m\}$ is linearly independent so

$$a_1(\lambda_{m+1} - \lambda_1) = \cdots = a_r(\lambda_{m+1} - \lambda_m) = 0.$$

By hypothesis, $\lambda_{m+1} \neq \lambda_i$ for any $i = 1, \ldots, m$ so

$$a_1 = a_2 = \cdots = a_m = 0.$$

But this implies $\underline{v}_{m+1} = \underline{0}$ contradicting the hypothesis that $\underline{v}_{m+1}$ is non-zero. We therefore conclude that the theorem is true. $\square$

2. Reflections in $\mathbb{R}^2$, revisited

A simple example to consider is reflection in a line lying in $\mathbb{R}^2$, the situation we considered in chapter 8. There we examined a pair of orthogonal lines, L spanned by $\begin{pmatrix} a \\ b \end{pmatrix}$, and L' spanned by $\begin{pmatrix} b \\ -a \end{pmatrix}$. We determined the matrix A that fixed the points on L and sent other points to their reflections in L. In particular, A sent $\begin{pmatrix} b \\ -a \end{pmatrix}$ to its negative. We found that

$$A = \frac{1}{a^2 + b^2}\begin{pmatrix} a^2 - b^2 & 2ab \\ 2ab & b^2 - a^2 \end{pmatrix}.$$

The matrix A has eigenvectors $\begin{pmatrix} a \\ b \end{pmatrix}$ and $\begin{pmatrix} b \\ -a \end{pmatrix}$ with eigenvalues, $+1$ and -1, and the corresponding eigenspaces are L and L'.

The point of this example is that the matrix A does not initially appear to have any special geometric meaning but by finding its eigenvalues and eigenspaces the geometric meaning of A becomes clear.

3. The 2×2 case

THEOREM 3.1. *The eigenvalues of* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *are the solutions of the quadratic polynomial equation*

$$\lambda^2 - (a+d)\lambda + ad - bc = 0. \tag{3-1}$$

Proof. We have already noted that λ is an eigenvalue for A if and only if $A - \lambda I$ is singular, i.e., if and only if $\det(A - \lambda I) = 0$. But

$$\begin{aligned} \det(A - \lambda I) &= \det \begin{pmatrix} a - \lambda & b \\ c & d - \lambda \end{pmatrix} \\ &= (a-\lambda)(d-\lambda) - bc \\ &= \lambda^2 - (a+d)\lambda + ad - bc, \end{aligned}$$

so the result follows. □

A quadratic polynomial with real coefficients can have either zero, one, or two roots. It follows that a 2×2 matrix with real entries can have either zero, one, or two eigenvalues. (Later we will see that an $n \times n$ matrix with real entries can have can have anywhere from zero to n eigenvalues.)

3.1. The polynomial $x^2 + 1$ has no real zeroes, so the matrix

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

has no eigenvalues. You might be happy to observe that this is the matrix that rotates the plane through an angle of 90° in the counterclockwise direction. It is clear that such a linear transformation will not send any line to itself: rotating by 90° moves every line.

Of course, it is apparent that rotating by any angle that is not an integer multiple of π will have the same property: it will move every line, so will have no eigenvalues. You should check this by using the formula for A_θ in(7-1) and then applying the quadratic formula to the equation (2x2.eigenvals).

3.2. The polynomial $x^2 - 4x + 4$ has one zero, namely 2, because it is a square, so the matrix

$$A = \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}$$

has exactly one eigenvalue, namely 2. The 2-eigenspace is

$$E_2 = \mathcal{N}(A - 2I) = \mathcal{N} \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} = \mathbb{R} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

You should check that A times $\begin{pmatrix}1\\1\end{pmatrix}$ is $2\begin{pmatrix}1\\1\end{pmatrix}$. We know that $\dim E_2 = 1$ because the rank of $A - 2I$ is 1 and hence its nullity is 1.

3.3. The polynomial $x^2 - x - 2$ has two zeroes, namely -1 and 2, so the matrix

$$B = \begin{pmatrix}-2 & -2\\ 2 & 3\end{pmatrix}$$

has two eigenvalues, -1 and 2. The 2-eigenspace is

$$E_2 = \mathcal{N}(B - 2I) = \mathcal{N}\begin{pmatrix}-4 & -2\\ 2 & 1\end{pmatrix} = \mathbb{R}\begin{pmatrix}1\\-2\end{pmatrix}.$$

The (-1)-eigenspace is

$$E_{-1} = \mathcal{N}(B + I) = \mathcal{N}\begin{pmatrix}-1 & -2\\ 2 & 4\end{pmatrix} = \mathbb{R}\begin{pmatrix}2\\-1\end{pmatrix}.$$

3.4. The examples we have just done should not mislead you into thinking that eigenvalues must be integers! For example, $\left(\begin{smallmatrix}1 & 2\\ 1 & 1\end{smallmatrix}\right)$ has two eigenvalues, neither of which is an integer. It would be sensible to try computing those and the associated eigenspaces.

4. The equation $A^2 + I$

You already know there is no real number x such that $x^2 + 1 = 0$. Since a number is a 1×1 matrix it is not unreasonable to ask whether there is a 2×2 matrix A such that $A^2 + I = 0$. I will leave you to tackle that question. You can attack the question in a naive way by taking a 2×2 matrix

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

squaring it, setting the square equal to

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

and asking whether the system of four quadratic equations in a, b, c, d so obtained have a solution. Not pretty, but why not try it and find out what happens.

As a cute illustration of the use of eigenvalues I will now show there is no 3×3 matrix A such that $A^2 + I = 0$. I will prove this by contradiction; i.e., I will assume A is a 3×3 matrix such that $A^2 + I = 0$ and deduce something false from that, thereby showing there can be no such A.

So, let's get started by assuming A is a 3×3 matrix such that $A^2 + I = 0$.

As a preliminary step I will show that A has no eigenvalues. If $\lambda \in \mathbb{R}$ were an eigenvalue and $\underline{v}$ a non-zero vector such that $A\underline{v} = \lambda\underline{v}$, then

$$-\underline{v} = -I\underline{v} = A^2\underline{v} = A(A\underline{v}) = A(\lambda\underline{v}) = \lambda A\underline{v} = \lambda^2\underline{v}.$$

But $\underline{v} \neq 0$ so the equality $-\underline{v} = \lambda^2\underline{v}$ implies $-1 = \lambda^2$. But this can not be true: there is no real number whose square is -1 so I conclude that A can not have an eigenvector. (Notice this argument did not use anything about the size of the matrix A. If A is any square matrix with real entries such that $A^2 + I = 0$, then A does not have an eigenvalue. We should really say "A does not have a *real* eigenvalue".

With that preliminary step out of the way let's proceed to prove the result we want. Let $\underline{v}$ be any non-zero vector in $\mathbb{R}^3$ and let $V = \mathrm{Sp}(\underline{v}, A\underline{v})$. Then V is an A-*invariant subspace* by which I mean if $\underline{w} \in V$, then $A\underline{w} \in V$. More colloquially, A sends elements of V to elements of V. Moreover, $\dim V = 2$ because the fact that A has no eigenvectors implies that $A\underline{v}$ is *not* a multiple of $\underline{v}$; i.e., $\{\underline{v}, A\underline{v}\}$ is linearly independent.

Since V is a 2-dimensional subspace of $\mathbb{R}^3$ there is a non-zero vector $\underline{w} \in \mathbb{R}^3$ that is not in V. By the same argument, the subspace $W := \mathrm{Sp}(\underline{w}, A\underline{w})$ is A-invariant and has dimension 2. Since $\underline{w} \notin V$, $V + W = \mathbb{R}^3$. From the formula

$$\dim(V + W) = \dim V + \dim W - \dim(V \cap W)$$

we deduce that $\dim(V \cap W) = 1$. Since V and W are A-invariant, so is $V \cap W$. However, $V \cap W = \mathbb{R}\underline{u}$ for some $\underline{u}$ and the fact that $\mathbb{R}\underline{u}$ is A-invariant implies that $A\underline{u}$ is a scalar multiple of $\underline{u}$; i.e., $\underline{u}$ is an eigenvector for A. But that is false: we have already proved A has no eigenvectors. Thus we are forced to conclude that there is no 3×3 matrix A such that $A^2 + I = 0$.

4.1. Why did I just prove that? A recent midterm contained the following question: if A is a 3×3 matrix such that $A^3 + A = 0$, is A invertible. The answer is "no", but the question is a *very bad question* because the "proof" I had in mind is flawed. Let me explain my false reasoning: if $A^3 + A = 0$, then $A(A^2 + I) = 0$ so A is not invertible because, as we observed in chapter 4.4, if $AB = 0$ for some non-zero matrix B, then A is not invertible. However, I can not apply the observation in chapter 4.4 unless I know that $A^2 + I$ is non-zero, and it is not easy to show that $A^2 + I$ is not zero. The argument above is the simplest argument I know, and it isn't so simple.

There is a shorter argument using determinants but at the time of the midterm I had not introduced either determinants or eigenvalues.

5. The characteristic polynomial

The characteristic polynomial of an $n \times n$ matrix A is the degree n polynomial

$$\det(A - tI).$$

You should convince yourself that $\det(A - tI)$ really is a polynomial in t of degree n. Let's denote that polynomial by $p(t)$. If we substitute a number λ for t, then

$$p(\lambda) = \det(A - \lambda I).$$

The following result is an immediate consequence of this.

Proposition 5.1. *Let A be an $n \times n$ matrix, and let $\lambda \in \mathbb{R}$. Then λ is an eigenvalue of A if and only if it is a zero of the characteristic polynomial of A.*

Proof. Theorem 1.1 says that λ is an eigenvalue for A if and only $\det(A - \lambda I) = 0$. □

A polynomial of degree n has at most n roots. The next result follows from this fact.

Corollary 5.2. *An $n \times n$ matrix has at most n eigenvalues.*

The characteristic polynomial of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is

$$t^2 - (a+d)t + ad - bc.$$

6. How to find eigenvalues and eigenvectors

Finding eigenvalues and eigenvectors is often important. Here we will discuss the head-on, blunt, full frontal method. Like breaking into a bank, that is not always the most effective way, but it is certainly one thing to try. But keep in mind that a given matrix might have some special features that can be exploited to allow an easier method. Similarly, when breaking into a bank, there might be some special features that might suggest an alternative to the guns-ablazing method.

Let A be an $n \times n$ matrix. By Proposition 5.1, λ is an eigenvalue if and only if $\det(A - \lambda I) = 0$, i.e., if and only if λ is a root/zero of the characteristic polynomial. So, the first step is to compute the characteristic polynomial. Don't forget to use elementary row operations before computing $\det(A - tI)$ if it looks like that will help—remember, the more zeroes in the matrix the easier it is to compute its determinant . The second step is to find the roots of the characteristic polynomial.

Once you have found an eigenvalue, λ say, remember that the λ-eigenspace is the null space of $A - \lambda I$. The third step is to compute that null space, i.e., find the solutions to the equation $(A - \lambda I)\underline{x} = 0$, by using the methods developed earlier in these notes. For example, put $A - \lambda I$ in row-reduced echelon form, find the independent variables and proceed from there.

6.1. An example. In order to compute the eigenvalues of the matrix

$$B := \begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$$

we perform some elementary row operations on $B - tI$ before computing its determinant: subtracting the bottom row of $B - tI$ from each of the other rows does not change the determinant, so $\det(B - tI)$ is equal to

$$\det\begin{pmatrix} 1-t & -1 & -1 & -1 \\ -1 & 1-t & -1 & -1 \\ -1 & -1 & 1-t & -1 \\ -1 & -1 & -1 & 1-t \end{pmatrix} = \det\begin{pmatrix} 2-t & 0 & 0 & t-2 \\ 0 & 2-t & 0 & t-2 \\ 0 & 0 & 2-t & t-2 \\ -1 & -1 & -1 & 1-t \end{pmatrix}.$$

If we replace a row by c times that row we change the determinant by a factor of c, so

$$\det(B - tI) = (2-t)^3 \det\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ -1 & -1 & -1 & 1-t \end{pmatrix}.$$

The determinant does not change if we add each of the first three rows to the last row so

$$\det(B - tI) = (2-t)^3 \det\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -2-t \end{pmatrix} = (t-2)^3(t+2).$$

The eigenvalues are ± 2. Now

$$E_2 = \mathcal{N}(B - 2I) = \mathcal{N}\begin{pmatrix} -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{pmatrix}.$$

The rank of $B - 2I$, i.e., the dimension of the linear span of its columns, is 1, and its nullity is therefore 3. Therefore $\dim E_2 = 3$. It is easy to find three linearly independent vectors $\underline{x}$ such that $(B - 2I)\underline{x} = 0$ and so compute

$$E_2 = \mathbb{R}\begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} + \mathbb{R}\begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} + \mathbb{R}\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}.$$

Finally,

$$E_{-2} = \mathcal{N}(B + 2I) = \mathcal{N}\begin{pmatrix} 3 & -1 & -1 & -1 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ -1 & -1 & -1 & 3 \end{pmatrix} = \mathbb{R}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

6.2. Another example. Let

$$A := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

The characteristic polynomial of A is

$$x^2(x^3 - 5x^2 + 2x - 1).$$

The x^2 factor implies that the 0-eigenspace, i.e., the null space of A, has dimension two. It is easy to see that

$$\mathcal{N}(A) = \mathbb{R}\begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \mathbb{R}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ -1 \end{pmatrix}.$$

We don't need to know the zeroes of the cubic factor $f(x) = x^3 - 5x^2 + 2x - 1$ just yet. However, a computation gives

$$f(0) = -1, \qquad f\left(\tfrac{2}{3}\right) > 0, \qquad f(1) = -3, \qquad f(10) > 0,$$

so the graph $y = f(x)$ crosses the x-axis at points in the open intervals

$$\left(0, \tfrac{2}{3}\right), \qquad \left(\tfrac{2}{3}, 1\right), \qquad \text{and} \qquad (1, 10).$$

Hence $f(x)$ has three real zeroes, and A has three distinct non-zero eigenvalues. Because A has a 2-dimensional 0-eigenspace it follows that $\mathbb{R}^5$ has a basis consisting of eigenvectors for A.

<u>Claim:</u> If λ is a non-zero eigenvalue for A, then

$$\begin{pmatrix} 1 - \lambda^{-1} - \lambda \\ 1 - \lambda^{-1} - \lambda \\ 4\lambda - 1 - \lambda^2 \\ -3 \\ 2\lambda^{-1} + 1 - \lambda \end{pmatrix}$$

is a λ-eigenvector for A.

<u>Proof of Claim:</u> We must show that $A\underline{x} = \lambda\underline{x}$. Since λ is an eigenvalue it is a zero of the characteristic polynomial; since $\lambda \neq 0$, $f(\lambda) = 0$, i.e., $\lambda^3 - 5\lambda^2 + 2\lambda - 1 = 0$. The calculation

$$A\underline{x} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 - \lambda^{-1} - \lambda \\ 1 - \lambda^{-1} - \lambda \\ 4\lambda - 1 - \lambda^2 \\ -3 \\ 2\lambda^{-1} + 1 - \lambda \end{pmatrix} = \begin{pmatrix} \lambda - 1 - \lambda^2 \\ \lambda - 1 - \lambda^2 \\ \lambda - 1 - \lambda^2 \\ -3\lambda \\ 2 + \lambda - \lambda^2 \end{pmatrix} = \lambda\underline{x}$$

shows that the Claim is true, <u>*however*</u> please, please, please, notice we used the fact that λ is a solution to the equation $x^3 - 5x^2 + 2x - 1 = 0$ in the calculation in the following way: because $\lambda^3 - 5\lambda^2 + 2\lambda - 1 = 0$ it follows that $\lambda - 1 - \lambda^2 = \lambda(4\lambda - 1 - \lambda^2)$, so the third entry in $A\underline{x}$ is λ times the third entry in $\underline{x}$, thus justifying the final equality in the calculation. $\Diamond$

Notice we did not need to compute the eigenvalues in order to find the eigenspaces. If one wants more explicit information one needs to determine the roots of the cubic equation $x^3 - 5x^2 + 2x - 1 = 0$.

6.3. How did I find the eigenvector in the previous example? That is the real problem! If someone hands you a matrix A and a vector $\underline{v}$ and claims that $\underline{v}$ is an eigenvector one can test the truth of the claim by computing $A\underline{v}$ and checking whether $A\underline{v}$ is a multiple of $\underline{v}$.

To find the eigenvector I followed the proceedure described in the first paragraph of section 6. By definition, the λ-eigenspace is the space of solutions to the homogeneous equation $(A-\lambda I)\underline{x}=0$. To find those solutions we must put

$$\begin{pmatrix} 1-\lambda & 1 & 1 & 1 & 1 \\ 1 & 1-\lambda & 1 & 1 & 1 \\ 1 & 1 & 1-\lambda & 1 & 1 \\ 1 & 1 & 0 & 1-\lambda & 1 \\ 1 & 1 & 1 & 0 & 1-\lambda \end{pmatrix}$$

in row-reduced echelon form. To do this first subtract the top row from each of the other rows to obtain

$$\begin{pmatrix} 1-\lambda & 1 & 1 & 1 & 1 \\ \lambda & -\lambda & 0 & 0 & 0 \\ \lambda & 0 & -\lambda & 0 & 0 \\ \lambda & 0 & -1 & -\lambda & 0 \\ \lambda & 0 & 0 & -1 & -\lambda \end{pmatrix}.$$

Now add the bottom row to the top row and subtract the bottom row from each of the middle three rows, then move the bottom row to the top to get

$$\begin{pmatrix} \lambda & 0 & 0 & -1 & -\lambda \\ 1 & 1 & 1 & 0 & 1-\lambda \\ 0 & -\lambda & 0 & 1 & \lambda \\ 0 & 0 & -\lambda & 1 & \lambda \\ 0 & 0 & -1 & 1-\lambda & \lambda \end{pmatrix}.$$

Write $\nu=\lambda^{-1}$ (this is allowed since $\lambda\neq 0$) and multiply the first, third, and fourth rows by ν to get

$$\begin{pmatrix} 1 & 0 & 0 & -\nu & -1 \\ 1 & 1 & 1 & 0 & 1-\lambda \\ 0 & -1 & 0 & \nu & 1 \\ 0 & 0 & -1 & \nu & 1 \\ 0 & 0 & -1 & 1-\lambda & \lambda \end{pmatrix}.$$

Replace the second row by the second row minus the first row plus the third row to get

$$\begin{pmatrix} 1 & 0 & 0 & -\nu & -1 \\ 0 & 0 & 1 & 2\nu & 3-\lambda \\ 0 & -1 & 0 & \nu & 1 \\ 0 & 0 & -1 & \nu & 1 \\ 0 & 0 & -1 & 1-\lambda & \lambda \end{pmatrix}.$$

Now multiply the third row by -1, add the bottom row to the second row, and subtract the bottom row from the fourth row, then multiply the bottom row by -1, to get

$$B := \begin{pmatrix} 1 & 0 & 0 & -\nu & -1 \\ 0 & 0 & 0 & 2\nu+1-\lambda & 3 \\ 0 & 1 & 0 & -\nu & -1 \\ 0 & 0 & 0 & \nu-1+\lambda & 1-\lambda \\ 0 & 0 & 1 & -1+\lambda & -\lambda \end{pmatrix}.$$

There is no need to do more calculation to get A in row-reduced echelon form because it is quite easy to write down the solutions to the system $B\underline{x} = 0$ *which is equivalent to the system* $(A - \lambda I)\underline{x} = 0$. Write $\underline{x} = (x_1, x_2, x_3, x_4, x_5)^T$. From the second row of B we see that we should take

$$x_4 = -3 \qquad \text{and} \qquad x_5 = 2\nu + 1 - \lambda.$$

From the other rows of B we see that we must have

$$\begin{aligned} x_1 &= \nu x_4 + x_5 && = -3\nu + (2\nu + 1 - \lambda) \\ x_2 &= \nu x_4 + x_5 && = -3\nu + (2\nu + 1 - \lambda) \\ x_3 &= (1-\lambda)x_4 + \lambda x_5 && = 3(\lambda - 1) + \lambda(2\nu + 1 - \lambda). \end{aligned}$$

Thus

$$\underline{x} = \begin{pmatrix} 1-\nu-\lambda \\ 1-\nu-\lambda \\ 4\lambda - 1 - \lambda^2 \\ -3 \\ 2\nu+1-\lambda \end{pmatrix}.$$

This is the matrix in the statement of the claim we made on page 120.

6.4. It ain't easy. Before finding the eigenvector in the claim I made many miscalculations, a sign here, a sign there, and pretty soon I was doomed and had to start over. So, take heart: all you need is perseverance, care, and courage, when dealing with a 5×5 matrix by hand. Fortunately, there are computer packages to do this for you. The main thing is to understand the principle for finding the eigenvectors. The computer programs simply implement the principle.

7. The utility of eigenvectors

Let A be an $n \times n$ matrix, and suppose we are in the following good situation:

- $\mathbb{R}^n$ has a basis consisting of eigenvectors for A;
- given $\underline{v} \in \mathbb{R}^n$ we have an effective means of writing $\underline{v}$ as a linear combination of the eigenvectors for A.

Then, as the next result says, it is easy to compute $A\underline{v}$.

PROPOSITION 7.1. *Suppose that A is an $n \times n$ matrix such that $\mathbb{R}^n$ has a basis consisting of eigenvectors for A. Explicitly, suppose that $\{\underline{v}_1, \ldots, \underline{v}_n\}$ is a basis for $\mathbb{R}^n$ and that each $\underline{v}_i$ is an eigenvector for A with eigenvalue λ_i. If $\underline{v} = a_1\underline{v}_1 + \cdots + a_n\underline{v}_n$, then*

$$A\underline{v} = a_1\lambda_1\underline{v}_1 + \cdots + a_n\lambda_n\underline{v}_n.$$

CHAPTER 14

Complex vector spaces and complex eigenvalues

1. The complex numbers

The set of complex numbers is denoted by $\mathbb{C}$. I assume you have already met complex numbers but will give a short refresher course in chapter 2 below.

The complex numbers were introduced to provide roots for polynomials that might have no real roots. The simplest example is the polynomial $x^2 + 1$. It has no real roots because the square of a real number is *never* equal to -1.

Complex numbers play a similar role in linear algebra: a matrix with real entries might have no real eigenvalues but it will always have at least one complex eigenvalue (unless it is a 1×1 matrix, i.e., a number.

For example, the matrix

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

representing counterclockwise rotation by 90° moves every 1-dimensional subspace of $\mathbb{R}^2$ so has no eigenvectors and therefore no eigenvalues, at least no *real* eigenvalues. I like that geometric argument but one can also see it has no real eigenvalues because its characteristic polynomial $x^2 + 1$ has no real roots. However, $x^2 + 1$ has two complex roots, $\pm i$, and the matrix has these as complex eigenvalues and has two corresponding eigenvectors in $\mathbb{C}^2$. Explicitly,

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} -i \\ 1 \end{pmatrix} = -i \begin{pmatrix} 1 \\ i \end{pmatrix}$$

and

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -i \end{pmatrix} = \begin{pmatrix} i \\ 1 \end{pmatrix} = i \begin{pmatrix} 1 \\ -i \end{pmatrix}.$$

As this calculation suggests, all the matrix algebra and linear algebra we have done so far extends with essentially no change from $\mathbb{R}$ to $\mathbb{C}$. We simply allow matrices to have entries that are complex numbers and instead of working with $\mathbb{R}^n$ we work with $\mathbb{C}^n$, $n \times 1$ column matrices, or vectors, whose entries are complex numbers.

2. The complex numbers

This interlude is to remind you of some basic facts about complex numbers.

The set of complex numbers is an enlargement of the set of real numbers created by adjoining a square root of -1, denoted by i, and then making the minimal enlargement required to permit addition, subtraction and multiplication of all the numbers created by this process. Thus $\mathbb{C}$ contains $\mathbb{R}$ and because we want to add and multiply complex numbers we define

$$\mathbb{C} := \{a + ib \mid a, b \in \mathbb{R}\}.$$

Notice that $\mathbb{C}$ contains $\mathbb{R}$. The real numbers are just those complex numbers $a + ib$ for which $b = 0$. Of course we don't bother to write $a + i0$; we just write a.

We often think of the elements of $\mathbb{R}$ as lying on a line. It is common to think of $\mathbb{C}$ as a plane, a 2-dimensional vector space over $\mathbb{R}$, the linear span of 1 and i.

Every complex number can be written in a unique way as $a + ib$ for suitable real numbers a and b, We add by

$$(a + ib) + (c + id) = (a + c) + i(b + d).$$

and multiply by

$$(a + ib)(c + id) = ac + iad + ibc + i^2bd = (ac - bd) + i(ad + bc).$$

If $b = d = 0$ we get the usual addition and multiplication of real numbers.

An important property enjoyed by both real and complex numbers is that non-zero numbers have inverses. If $a + ib \neq 0$, then

$$\frac{a - ib}{a^2 + b^2} = \frac{1}{a + ib}.$$

You should check this by multiplying the left-hand term by $a+ib$ and noting that the answer is 1.

2.1. Reassurance. If you haven't met the complex numbers before don't be afraid. You have done something very similar before and survived that so you will survive this. Once upon a time your knowledge of numbers was limited to fractions, i.e., all you knew was $\mathbb{Q}$. Imagine yourself in that situation again. I now come to you saying I have a new number that I will denote by the symbol $\bowtie$ and I wish to enlarge the number system $\mathbb{Q}$ to a new number system that I will denote by $\mathbb{Q}(\bowtie)$. I propose that in my new number system the product of $\bowtie$ with itself is 2, i.e., $\bowtie^2 = 2$, and I further propose that $\mathbb{Q}(\bowtie)$ consists of all expressions

$$a + b \bowtie$$

with the addition and multiplication in $\mathbb{Q}(\bowtie)$ defined by

$$(a + b \bowtie) + (c + d \bowtie) := (a + c) + (b + d) \bowtie$$

and

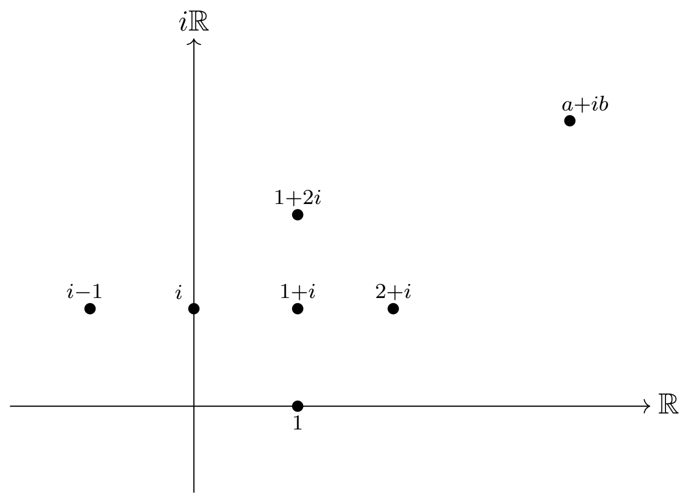
$$(a + b \bowtie)(c + d \bowtie) := (ac + 2bd) + (ad + bc) \bowtie .$$

It might be a little tedious to check that the multiplication is associative, that the distributive law holds, and that every non-zero number in $\mathbb{Q}(\bowtie)$ has an inverse that also belongs to $\mathbb{Q}(\bowtie)$. The number system $\mathbb{Q}(\bowtie)$ might also seem a little mysterious until I tell you that a copy of $\mathbb{Q}(\bowtie)$ can already be found inside $\mathbb{R}$. In fact, $\bowtie$ is just a new symbol for $\sqrt{2}$. The number $a + b \bowtie$ is really just $a + b\sqrt{2}$.

Now re-read the previous paragraph with this additional information.

2.2. The complex plane. As mentioned above, it is useful to picture the set of real numbers as the points on a line, the real line, and equally useful to picture the set of complex numbers as the points on a plane. The horizontal axis is just the real line, sometimes called the real axis, and the vertical axis, sometimes called the imaginary axis, is all real multiples of i. We denote it by $i\mathbb{R}$.

The complex plane $\mathbb{C}$



2.3. Complex conjugation. Let $z = a + ib \in \mathbb{C}$. The conjugate of z, denoted $\bar{z}$, is defined to be

$$\bar{z} := a - ib.$$

You can picture complex conjugation as reflection in the real axis. The important points are these

- $z\bar{z} = a^2 + b^2$ is a real number;
- $z\bar{z} \geq 0$;
- $z\bar{z} = 0$ if and only if $z = 0$;
- $\sqrt{z\bar{z}}$ is the distance from zero to z;
- $\overline{wz} = \bar{w}\bar{z}$;
- $\overline{w+z} = \bar{w} + \bar{z}$;
- $\bar{z} = z$ if and only if $z \in \mathbb{R}$.

It is common to call $\sqrt{z\bar{z}}$ the absolute value of z and denote it by $|z|$. It is also common to call $\sqrt{z\bar{z}}$ the norm of z and denote it by $\|z\|$.

Performing the conjugate twice gets us back where we started: $\bar{\bar{z}} = z$. The geometric interpretation of this is that the conjugate of a complex number is its relection in the real axis and $\overline{\overline{z}} = z$ because reflecting twice in the real axis is the same as doing nothing.

2.4. Roots of polynomials. Complex numbers were invented to provide solutions to quadratic polynomials that had no real solution. The ur-example is $x^2 + 1 = 0$ which has no solutions in $\mathbb{R}$ but solutions $\pm i$ in $\mathbb{C}$. This is the context in which you meet complex numbers at high school. You make the observation there that the solutions of $ax^2 + bx + c = 0$ are given by

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

provided $a \neq 0$ and the equation has no real solutions when $b^2 - 4ac < 0$ but has two complex zeroes,

$$\lambda = -\frac{b}{2a} + i\,\frac{\sqrt{4ac - b^2}}{2a} \qquad \text{and} \qquad \bar{\lambda} = -\frac{b}{2a} - i\,\frac{\sqrt{4ac - b^2}}{2a}.$$

Notice that the zeroes λ and $\bar{\lambda}$ are complex conjugates of each other.

It is a remarkable fact that although the complex numbers were invented with no larger purpose than providing solutions to *quadratic* polynomials, they provide all solutions to polynomials of *all* degrees.

THEOREM 2.1. *Let $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$ be a polynomial with coefficients $a_1, \ldots, a_n$ belonging to $\mathbb{R}$. Then there are complex numbers $r_1, \ldots, r_n$ such that*

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n).$$

Just as for quadratic polynomials, the zeroes of f come in conjugate pairs because if $f(\lambda) = 0$, then, using the properties of conjugation mentioned at the end of chapter 2.3,

$$\begin{aligned} f(\bar{\lambda}) &= \bar{\lambda}^n + a_1\bar{\lambda}^{n-1} + a_2\bar{\lambda}^{n-2} + \cdots + a_{n-1}\bar{\lambda} + a_n \\ &= \overline{\lambda^n} + a_1\overline{\lambda^{n-1}} + a_2\overline{\lambda^{n-2}} + \cdots + a_{n-1}\overline{\lambda} + a_n \\ &= \overline{\lambda^n + a_1\lambda^{n-1} + a_2\lambda^{n-2} + \cdots + a_{n-1}\lambda + a_n} \\ &= \overline{f(\lambda)} \\ &= 0. \end{aligned}$$

2.5. Application to the characteristic polynomial of a real matrix. Let A be an $n \times n$ matrix whose entries are real numbers. Then $\det(A - tI)$ is a polynomial with real coefficients. If $\lambda \in \mathbb{C}$ is a zero of $\det(A - tI)$ so is $\bar{\lambda}$.

Recall that the eigenvalues of A are exactly (the real numbers that are) the zeroes of $\det(A - tI)$. We wish to view the complex zeroes of $\det(A - tI)$ as eigenvalues of A but to do that we have to extend our framework for linear algebra from $\mathbb{R}^n$ to $\mathbb{C}^n$.

3. Linear algebra over $\mathbb{C}$

We now allow matrices to have entries that are complex numbers. Because $\mathbb{R}$ is contained in $\mathbb{C}$ linear algebra over $\mathbb{C}$ includes linear algebra over $\mathbb{R}$, i.e., every matrix with real entries is a matrix with complex entries by virtue of the fact that every real number is a complex number.

Hence, left multiplication by an $m \times n$ matrix with real entries can be viewed as a linear transformation $\mathbb{C}^n \to \mathbb{C}^m$ in addition to being viewed as a linear transformation $\mathbb{R}^n \to \mathbb{R}^m$.

We extend the operation of complex conjugation to matrices. If $A = (a_{ij})$ is a matrix with entries $a_{ij} \in \mathbb{C}$, we define the conjugate of A to be

$$\bar{A} := (\overline{a_{ij}}),$$

i.e., the matrix obtained by replacing every entry of A by its complex conjugate.

It is straightforward to verify that $\overline{AB} = \bar{A}\bar{B}$ and $\overline{A+B} = \bar{A} + \bar{B}$.

PROPOSITION 3.1. *Let A be an $n \times n$ matrix with real entries. If $\lambda \in \mathbb{C}$ is an eigenvalue for A so is $\bar{\lambda}$. Furthermore, if $\underline{x}$ is a λ-eigenvector for A, then $\bar{x}$ is a $\bar{\lambda}$ eigenvector for A.*

Proof. This is a simple calculation. If $A\underline{x} = \lambda\underline{x}$, then

$$A\bar{x} = \bar{A}\bar{x} = \overline{A\underline{x}} = \overline{\lambda\underline{x}} = \bar{\lambda}\bar{x}$$

as claimed. $\square$

The first half of Proposition 3.1 is a consequence of the fact that if λ is a zero of a polynomial with real coefficients so is $\bar{\lambda}$.

3.1. The conjugate transpose.

For complex matrices, i.e., entries having complex entries, one often combines the operations of taking the transpose and taking the conjugate. Notice that these operations commute, i.e., it doesn't matter which order one performs them: in symbols

$$\left(\overline{A}\right)^{\mathsf{T}} = \overline{A^{\mathsf{T}}}.$$

We often write

$$A^* := \overline{A}^{\mathsf{T}}$$

and call this the conjugate transpose of A.

4. The complex norm

Let $z \in \mathbb{C}$. The norm of z is the number

$$\|z\| = \sqrt{z\bar{z}}.$$

If $z \neq 0$,

$$z^{-1} = \bar{z}/\|z\|.$$

Check this.

We can extend the notion of norm, or "size", from complex numbers to vectors in $\mathbb{C}^n$.

One important difference between complex and real linear algebra involves the definition of the norm of a vector. Actually, this change already begins when dealing with complex numbers. The distance of a real number x from zero is given by its absolute value $|x|$. The distance of a point $x = (x_1, x_2) \in \mathbb{R}^2$ from zero is $\sqrt{x_1^2 + x_2^2}$. Picturing the complex plane as $\mathbb{R}^2$, the distance of $z = a + ib$ from 0 is

$$\sqrt{a^2 + b^2} = \sqrt{z\bar{z}}.$$

If $\mathbb{R}^n$, the distance of a point $\underline{x} = (x_1, \ldots, x_n)^\mathsf{T}$ from the origin is given by taking the square root of its dot product with itself:

$$\|\underline{x}\| = \sqrt{x_1^2 + \cdots + x_n^2} = \sqrt{\underline{x} \cdot \underline{x}} = \sqrt{\underline{x}^\mathsf{T}\underline{x}}.$$

Part of the reason this works is that a sum of squares of real numbers is always ≥ 0 and is equal to zero only when each of those numbers is zero. This is no longer the case for complex numbers.

The norm of $x \in \mathbb{C}^n$ is

$$\|\underline{x}\| = \sqrt{\underline{x}^*\underline{x}}.$$

Since

$$\underline{x}^*\underline{x} = \sum_{j=1}^{n} \bar{x}_j x_j = \sum_{j=1} |x_j|^2$$

is a real number ≥ 0 the definition of $\|\underline{x}\|$ makes sense—it is the non-negative square root of the real number $\underline{x}^*\underline{x}$.

4.1. Real symmetric matrices have real eigenvalues. The next result is proved by a nice application of the complex norm.

THEOREM 4.1. *All the eigenvalues of a symmetric matrix with real entries are real.*

Proof. Let A be real symmetric $n \times n$ matrix and λ an eigenvalue for A. We will show λ is a real number by proving that $\lambda = \bar{\lambda}$. Because λ is an eigenvalue, there is a non-zero vector $\underline{x} \in \mathbb{C}^n$ such that $A\underline{x} = \lambda\underline{x}$. Then

$$\lambda\|\underline{x}\|^2 = \lambda\underline{x}^*\underline{x} = \underline{x}^*\lambda\underline{x} = \underline{x}^*A\underline{x} = (A^\mathsf{T}\bar{x})^\mathsf{T}\underline{x} = (A\bar{x})^\mathsf{T}\underline{x}$$

where the last equality follows from the fact that A is symmetric. Continuing this string of equalities, we obtain

$$(A\bar{x})^\mathsf{T}\underline{x} = (\bar{\lambda}\bar{x})^\mathsf{T}\underline{x} = \bar{\lambda}\underline{x}^*\underline{x} = \bar{\lambda}\|\underline{x}\|^2.$$

We have shown that

$$\lambda\|\underline{x}\|^2 = \bar{\lambda}\|\underline{x}\|^2$$

from which we deduce that $\lambda = \bar{\lambda}$ because $\|\underline{x}\|^2 \neq 0$. Hence $\lambda \in \mathbb{R}$. $\square$

This is a clever proof. Let's see how to prove the 2×2 case in a less clever way. Consider the symmetric matrix

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

where a, b, d are real numbers. The characteristic polynomial of A is

$$t^2 - (a+d)t + ad - b^2 = 0$$

and your high school quadratic formula tells you that the roots of this polynomial are

$$\pm\tfrac{1}{2}\Big(a + d \pm \sqrt{(a+d)^2 - 4(ad - b^2)}$$

However,

$$(a+d)^2 - 4(ad - b^2) = (a-d)^2 + 4b^2$$

which is ≥ 0 because it is a sum of squares. Hence $\sqrt{(a+d)^2 - 4(ad - b^2)}$ is a real number and we conclude that the roots of the characteristic polynomial, i.e., the eigenvalues of A, are real.

It might be fun for you to try to prove the 3×3 case by a similar elementary argument.

5. An extended exercise

Let

$$A = \begin{pmatrix} 2 & -1 & -1 & -1 \\ 1 & -1 & -1 & 0 \\ 1 & 0 & -1 & -1 \\ 1 & -1 & 0 & -1 \end{pmatrix}.$$

Compute the characteristic polynomial of A and factor it as much as you can. Remember to use elementary row operations before computing $\det(A - xI)$. Can you write the characteristic polynomial of A as a product of 4 linear terms, i.e., as $(x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$ with $\alpha, \beta, \gamma, \delta \in \mathbb{C}$?

What are the eigenvalues and corresponding eigenspaces for A in $\mathbb{C}^4$?

Show that $A^6 = I$ and that no lower power of A is the identity.

Suppose that λ is a complex eigenvalue for A, i.e., there is a non-zero vector $\underline{x} \in \mathbb{C}^4$ such that $A\underline{x} = \lambda\underline{x}$. Show that $\lambda^6 = I$.

Let $\omega = e^{2\pi i/3}$. Thus $\omega^3 = 1$. Show that $(t-1)(t-\omega)(t-\omega^2) = 0$.

Show that

$$\{\pm 1, \pm\omega, \pm\omega^2\} \;=\; \{\lambda \in \mathbb{C} \mid \lambda^6 = 1\}.$$

Compute $A\underline{v}_1$, $A\underline{v}_2$, $A\underline{v}_3$, and $A\underline{v}_4$, where

$$\underline{v}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad \underline{v}_2 = \begin{pmatrix} 3 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad \underline{v}_3 = \begin{pmatrix} 0 \\ 1 \\ \omega \\ \omega^2 \end{pmatrix}, \quad \underline{v}_4 = \begin{pmatrix} 0 \\ 1 \\ \omega^2 \\ \omega \end{pmatrix}.$$

CHAPTER 15

Orthogonality

The word *orthogonal* is synonymous with *perpendicular*.

1. Geometry

In earlier chapters I often used the word *geometry* and spoke of the importance of have a geometric view of $\mathbb{R}^n$ and the sets of solutions to systems of linear equations. However, geometry really involves lengths and angles which have been absent from our discussion so far. The word *geometry* is derived from the Greek word *geometrein* which means to measure the land: cf. $\gamma\eta$ or $\gamma\alpha\iota\alpha$ meaning *earth* and metron or $\mu\varepsilon\tau\rho o\nu$ meaning *an instrument to measure*—metronome, metre, geography, etc.

In order to introduce angles and length in the context of vector spaces we use the dot product.

2. The dot product

The dot product of vectors $\underline{u} = (u_1, \ldots, u_n)$ and $\underline{v} = (v_1, \ldots, v_n)$ in $\mathbb{R}^n$ is the number

$$\underline{u} \cdot \underline{v} := u_1 v_1 + \cdots + u_n v_n.$$

The norm or length of $\underline{u}$ is

$$\|\underline{u}\| := \sqrt{\underline{u} \cdot \underline{u}}.$$

The justification for calling this the length is Pythagoras's Theorem.

Notice that

- $\underline{u} \cdot \underline{u} = 0$ if and only if $\underline{u} = \underline{0}$—this makes sense: the only vector having length zero is the zero vector.
- If $\underline{u}$ and $\underline{v}$ are column vectors of the same size, then $\underline{u} \cdot \underline{v} = \underline{u}^T \underline{v} = \underline{v}^T \underline{u}$.

2.1. Angles. We define the angle between two non-zero vectors $\underline{u}$ and $\underline{v}$ in $\mathbb{R}^n$ to be the unique angle $\theta \in [0, \pi]$ such that

$$\cos(\theta) := \frac{\underline{u} \cdot \underline{v}}{\|\underline{u}\| \, \|\underline{v}\|}.$$

Since $\cos(\frac{\pi}{2}) = 0$, the angle between $\underline{u}$ and $\underline{v}$ is $\frac{\pi}{2} = 90^\circ$ if and only if $\underline{u} \cdot \underline{v} = 0$.

Before accepting this definition as reasonable we should check that it gives the correct answer for the plane.

Suppose $\underline{u}, \underline{v} \in \mathbb{R}^2$. If $\underline{u}$ or $\underline{v}$ is a multiple of the other, then the angle between them is zero and this agrees with the formula because $\cos(0) = 1$.

Now assume $\underline{u} \neq \underline{v}$. The cosine rule applied to the triangle with sides $\underline{u}$, $\underline{v}$, and $\underline{u} - \underline{v}$, gives

$$\|\underline{u} - \underline{v}\|^2 = \|\underline{u}\|^2 + \|\underline{v}\|^2 - 2\|\underline{u}\| \, \|\underline{v}\| \cos(\theta).$$

The left-hand side of this expression is $\|\underline{u}\|^2 - 2(\underline{u} \cdot \underline{v}) + \|\underline{v}\|^2$. The result now follows.

General case done by reducing to the $\mathbb{R}^2$ case using the fact that every pair of vectors in $\mathbb{R}^n$ lies in a plane.

3. Orthogonal vectors

Two non-zero vectors $\underline{u}$ and $\underline{v}$ are said to be orthogonal if $\underline{u} \cdot \underline{v} = 0$.

The following result is a cute observation.

Proposition 3.1. *Let A be a symmetric $n \times n$ matrix and suppose λ and μ are different eigenvalues of A. If $\underline{u} \in E_\lambda$ and $\underline{v} \in E_\mu$, then $\underline{u}$ is orthogonal to $\underline{v}$.*

Proof. The calculation

$$\lambda \underline{u}^T \underline{v} = (\lambda \underline{u})^T \underline{v} = (A\underline{u})^T \underline{v} = \underline{u}^T A^T \underline{v} = \underline{u}^T A \underline{v} = \mu \underline{u}^T \underline{v}$$

shows that $(\lambda - \mu)\underline{u}^T \underline{v} = 0$. But $\lambda - \mu \neq 0$ so $\underline{u}^T \underline{v} = 0$. □

Let S be a non-empty subset of $\mathbb{R}^n$. We define

$$S^\perp := \{\underline{w} \in \mathbb{R}^n \mid \underline{w} \cdot \underline{v} = 0 \text{ for all } \underline{v} \in S\},$$

i.e., $S^\perp$ consists of those vectors that are perpendicular to every vector in S. We call $S^\perp$ the orthogonal to S and usually say "*S perp*" or "*S orthogonal*" when we read $S^\perp$.

Lemma 3.2. *If S is a non-empty subset of $\mathbb{R}^n$, then $S^\perp$ is a subspace of $\mathbb{R}^n$.*

Proof. Certainly $\underline{0} \in S^\perp$. If $\underline{w}_1$ and $\underline{w}_2$ are in $S^\perp$ so is $\underline{w}_1 + \underline{w}_2$ because if $\underline{u} \in S$, then

$$(\underline{w}_1 + \underline{w}_2) \cdot \underline{u} = \underline{w}_1 \cdot \underline{u} + \underline{w}_2 \cdot \underline{u} = 0 + 0 = 0.$$

If $\underline{w} \in S^\perp$ and $\lambda \in \mathbb{R}$, then $\lambda\underline{w} \in S^\perp$ because if $\underline{u} \in S$, then $(\lambda\underline{w}) \cdot \underline{u} = \lambda(\underline{w} \cdot \underline{u}) = \lambda \times 0 = 0$. □

Lemma 3.3. *If V is a subspace of $\mathbb{R}^n$, then $V \cap V^\perp = \{\underline{0}\}$.*

Proof. If $\underline{v}$ is in $V \cap V^\perp$, then $\underline{v} \cdot \underline{v} = 0$, whence $\underline{v} = 0$. □

4. Classical orthogonal polynomials

In chapter **??** we introduced the infinite dimensional vector space $\mathbb{R}[x]$ consisting of all polynomials with real coefficients. You are used to writing polynomials with respect to the basis $1, x, x^2, \ldots$. However, there are many other bases some of which are extremely useful.

Suppose we define a "dot product" on $\mathbb{R}[x]$ by declaring that

$$f \cdot g := \int_{-1}^{1} \frac{f(x)g(x)}{\sqrt{1-x^2}} dx.$$

It is easy to see that $f \cdot g = g \cdot f$, that $f \cdot (g+h) = f \cdot g + f \cdot g$, and $(\lambda f) \cdot g = \lambda(f \cdot g)$ for all $\lambda \in \mathbb{R}$.

It is common practice to call this dot product the inner product and write it as (f, g) rather than $f \cdot g$. We will do this.

The Chebyshev polynomials are defined to be

$$\begin{aligned} T_0(x) &:= 1 \\ T_1(x) &:= x \qquad \text{and} \\ T_n(x) = 2xT_n(x) - T_{n-1}(x) &\quad \text{for all } n \geq 2. \end{aligned}$$

THEOREM 4.1. *The set of Chebyshev polynomials are orthogonal to one another with respect to the inner product*

$$\int_{-1}^{1} \frac{T_m(x)T_n(x)}{\sqrt{1-x^2}} dx = \begin{cases} 0 & \text{if } m \neq n \\ \pi & \text{if } m = n = 0 \\ \pi/2 & \text{if } m = n \geq 1 \end{cases}$$

Proof. Use a change of variables $x = \cos(\theta)$ and use an induction argument to prove that $T_n(\cos(\theta)) = \cos(n\theta)$. □

5. Orthogonal and orthonormal bases

A set of non-zero vectors $\{\underline{v}_1, \ldots, \underline{v}_d\}$ is said to be orthogonal if $\underline{v}_i$ is orthogonal to $\underline{v}_j$ whenever $i \neq j$. A set consisting of a single non-zero vector is declared to be an orthogonal set.

LEMMA 5.1. *An orthogonal set of vectors is linearly independent.*

Proof. Let $\{\underline{v}_1, \ldots, \underline{v}_d\}$ be an orthogonal set of vectors and suppose that $a_1\underline{v}_1 + \cdots + a_d\underline{v}_d = 0$. Then

$$0 = \underline{v}_i \cdot (a_1\underline{v}_1 + \cdots + a_d\underline{v}_d).$$

However, when we multiply this out all but one term will vanish because $\underline{v}_i \cdot \underline{v}_j = 0$ when $j \neq i$. The non-vanishing term is $a_i\underline{v}_i$, so $a_i\underline{v}_i = 0$. But $\underline{v}_i \neq 0$, so $a_i = 0$. Thus all the a_is are zero and we conclude that $\{\underline{v}_1, \ldots, \underline{v}_d\}$ is linearly independent. □

An orthogonal basis is just that, a basis consisting of vectors that are orthogonal to one another. If in addition each vector has length one we call it an orthonormal basis.

The standard basis $\{\underline{e}_1, \ldots, \underline{e}_n\}$ for $\mathbb{R}^n$ is an orthonormal basis.

It is usually a tedious chore to express an element $\underline{w}$ in a subspace W as an *explicit* linear combination of a given basis $\{\underline{v}_1, \ldots, \underline{v}_d\}$ for W. To find the numbers $a_1, \ldots, a_d$ such that $\underline{w} = a_1\underline{v}_1 + \cdots + a_d\underline{v}_d$ usually involves solving a system of linear equations. However, if $\{\underline{v}_1, \ldots, \underline{v}_d\}$ is an orthonormal basis for W it is trivial to find the a_is. That's one reason we like orthogonal bases.

PROPOSITION 5.2. *Suppose $\{\underline{v}_1, \ldots, \underline{v}_d\}$ is an orthonormal basis for W. If $\underline{w} \in W$, then*

$$\underline{w} = (\underline{w} \cdot \underline{v}_1)\underline{v}_1 + \cdots + (\underline{w} \cdot \underline{v}_d)\underline{v}_d.$$

Proof. Notice first that each $(\underline{w} \cdot \underline{v}_i)$ *is* a number!

We know there are numbers $a_1, \ldots, a_d$ such that $\underline{w} = a_1\underline{v}_1 + \cdots + a_d\underline{v}_d$. It follows that

$$\begin{aligned} \underline{w} \cdot \underline{v}_i &= (a_1\underline{v}_1 + \cdots + a_d\underline{v}_d) \cdot \underline{v}_i \\ &= a_1(\underline{v}_1 \cdot \underline{v}_i) + \cdots + a_d(\underline{v}_d \cdot \underline{v}_i). \end{aligned}$$

Because $\{\underline{v}_1, \ldots, \underline{v}_d\}$ is an orthonormal set of vectors $\underline{v}_j \cdot \underline{v}_i = 0$ when $j \neq i$ and $\underline{v}_i \cdot \underline{v}_i = 1$. Hence

$$\underline{w}^T\underline{v}_i = a_1(\underline{v}_1 \cdot \underline{v}_i) + \cdots + a_d(\underline{v}_d \cdot \underline{v}_i) = a_i.$$

The result now follows. □

That is the great virtue of orthonormal bases. Unfortunately, one is not always fortunate enough to be presented with an orthonormal basis. However, there is a standard mechanism, the Gram-Schmidt process, that will take any basis for W and produce from it an orthonormal basis for W. That is the subject of the next chapter.

6. The Gram-Schmidt process

Suppose $\mathcal{B} = \{\underline{v}_1, \ldots, \underline{v}_s\}$ is a basis for a subspace W. The Gram-Schmidt process is a method for constructing from $\mathcal{B}$ an *orthogonal* basis $\{\underline{u}_1, \ldots, \underline{u}_s\}$ for W.

THEOREM 6.1. *Every subspace of $\mathbb{R}^n$ has an orthogonal basis.*

Proof. Let $\mathcal{B} = \{\underline{v}_1, \ldots, \underline{v}_s\}$ be a basis for W. Define $\underline{u}_1, \underline{u}_2, \underline{u}_3, \ldots$ by

$$\begin{aligned} \underline{u}_1 &:= \underline{v}_1 \\ \underline{u}_2 &:= \underline{v}_2 - \frac{\underline{u}_1 \cdot \underline{v}_2}{\|\underline{u}_1\|^2}\,\underline{u}_1 \\ \underline{u}_3 &:= \underline{v}_3 - \frac{\underline{u}_1 \cdot \underline{v}_3}{\|\underline{u}_1\|^2}\,\underline{u}_1 - \frac{\underline{u}_2 \cdot \underline{v}_3}{\|\underline{u}_2\|^2}\,\underline{u}_2 \\ &\textit{etc.} \end{aligned}$$

We will prove the theorem by showing that $\underline{u}_i \cdot \underline{u}_j = 0$ when $i \neq j$.

The first case is $i = 2$ and $j = 1$. We get

$$\underline{u}_2 \cdot \underline{u}_1 = \underline{v}_2 \cdot \underline{u}_1 - \frac{\underline{u}_1 \cdot \underline{v}_2}{\|\underline{u}_1\|^2}\, \underline{u}_1 \cdot \underline{u}_1.$$

But $\underline{u}_1 \cdot \underline{u}_1 = \|\underline{u}_1\|^2$ so those factors cancel in the second term to leave

$$\underline{u}_2 \cdot \underline{u}_1 = \underline{v}_2 \cdot \underline{u}_1 - \underline{u}_1 \cdot \underline{v}_2$$

which is zero because $\underline{u} \cdot \underline{v} = \underline{v} \cdot \underline{u}$. Hence $\underline{u}_2$ is orthogonal to $\underline{u}_1$.

The next case is $i = 3$ and $j = 1$. We get

$$\underline{u}_3 \cdot \underline{u}_1 = \underline{v}_3 \cdot \underline{u}_1 - \frac{\underline{u}_1 \cdot \underline{v}_3}{\|\underline{u}_1\|^2}\, \underline{u}_1 \cdot \underline{u}_1 - \frac{\underline{u}_2 \cdot \underline{v}_3}{\|\underline{u}_2\|^2}\, \underline{u}_2 \cdot \underline{u}_1. \tag{6-1}$$

The right-most term in (6-1) is zero because $\underline{u}_2 \cdot \underline{u}_1 = 0$. Arguing as in the previous paragraph shows that the two terms immediately to the right of the $=$ sign in (6-2) cancel so we get $\underline{u}_3 \cdot \underline{u}_1 = 0$.

Carry on like this to get $\underline{u}_i \cdot \underline{u}_1$ for all $i \geq 2$.

The next case is to take $i = 3$ and $j = 2$. We get

$$\underline{u}_3 \cdot \underline{u}_2 = \underline{v}_3 \cdot \underline{u}_2 - \frac{\underline{u}_1 \cdot \underline{v}_3}{\|\underline{u}_1\|^2}\underline{u}_1 \cdot \underline{u}_2 - \frac{\underline{u}_2 \cdot \underline{v}_3}{\|\underline{u}_2\|^2}\underline{u}_2 \cdot \underline{u}_2. \tag{6-2}$$

The second term on the right-hand-side is zero because $\underline{u}_1 \cdot \underline{u}_2 = 0$; in the third term, $\underline{u}_2 \cdot \underline{u}_2 = \|\underline{u}_2\|^2$ so those factors cancel to leave

$$\underline{u}_3 \cdot \underline{u}_2 = \underline{v}_3 \cdot \underline{u}_2 - \underline{u}_2 \cdot \underline{v}_3$$

which is zero. Hence $\underline{u}_3$ is orthogonal to $\underline{u}_2$.

Now do the case $i = 4$ and $j = 2$, and carry on like this to get $\underline{u}_i \cdot \underline{u}_2 = 0$ for all $i \geq 3$. Then start again with $i = 4$ and $j = 3$, et cetera, et cetera! Eventually, we prove that $\underline{u}_i \cdot \underline{u}_j = 0$ for all $i \neq j$.

We still need to prove that $\{\underline{u}_1, \ldots, \underline{u}_s\}$ is a basis for W. Because the $\underline{u}_i$s are an orthogonal set they are linearly independent. Their linear span is therefore a vector space of dimension s. By definition, each $\underline{u}_i$ is in $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_s)$ which equals W. Thus $\mathrm{Sp}(\underline{u}_1, \ldots, \underline{u}_s)$ is an s-dimensional subspace of the s-dimensional vector space W, and therefore equal to it by Corollary 5.2.[1] □

Corollary 6.2. *Every subspace of $\mathbb{R}^n$ has an orthonormal basis.*

[1]Alternative proof that the $\underline{u}_i$s span W. Rewrite the definition of $\underline{u}_i$ by putting $\underline{v}_i$ on one side and so obtain

$$\underline{v}_i = \underline{u}_i + \text{a linear combination of } \underline{u}_1, \ldots, \underline{u}_{i-1}.$$

Hence $\underline{v}_i \in \mathrm{Sp}(\underline{u}_1, \ldots, \underline{u}_s)$. Hence $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_s) \subseteq \mathrm{Sp}(\underline{u}_1, \ldots, \underline{u}_s)$; but $\mathrm{Sp}(\underline{u}_1, \ldots, \underline{u}_s) \subseteq \mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_s)$ too so the two linear spans are equal. Since $\mathrm{Sp}(\underline{v}_1, \ldots, \underline{v}_s) = W$ we conclude that $\mathrm{Sp}(\underline{u}_1, \ldots, \underline{u}_s) = W$.

Proof. Let W be a subspace of $\mathbb{R}^n$. By Theorem 6.1, W has an orthogonal basis. Let $\{\underline{u}_1, \dots, \underline{u}_s\}$ be an orthogonal basis for W. If we divide each $\underline{u}_i$ by its length we obtain a set of orthogonal vectors

$$\frac{\underline{u}_1}{\|\underline{u}_1\|}, \ \frac{\underline{u}_2}{\|\underline{u}_2\|}, \ \dots, \ \frac{\underline{u}_s}{\|\underline{u}_s\|}$$

each of which has length one; i.e., we obtain an orthonormal basis for W. □

Theorem 6.3. *Let A be an $n \times n$ symmetric matrix. Then $\mathbb{R}^n$ has an orthonormal basis consisting of eigenvectors for A.*

Proof. By Theorem 4.1, all A's eigenvalues are real. □

7. Orthogonal matrices

A matrix A is <u>orthogonal</u> if $A^T = A^{-1}$. By definition, an orthogonal matrix has an inverse so must be a square matrix.

An <u>orthogonal linear transformation</u> is a linear transformation implemented by an orthogonal matrix, i.e., if $T(\underline{x}) = A\underline{x}$ and A is an orthogonal matrix we call T an orthogonal linear transformation.

Theorem 7.1. *The following conditions on an $n \times n$ matrix Q are equivalent:*

(1) *Q is an orthogonal matrix;*
(2) *$Q\underline{x} \cdot Q\underline{y} = \underline{x} \cdot \underline{y}$ for all $\underline{x}, \underline{y} \in \mathbb{R}^n$;*
(3) *$\|Q\underline{x}\| = \|\underline{x}\|$ for all $\underline{x} \in \mathbb{R}^n$;*
(4) *the columns of Q, $\{\underline{Q}_1, \dots, \underline{Q}_n\}$, form an orthonormal basis for $\mathbb{R}^n$.*

Proof. We start by pulling a rabbit out of a hat. Let $\underline{x}, \underline{y} \in \mathbb{R}^n$. Then

$$\begin{aligned}\tfrac{1}{4}\big(\|\underline{x}+\underline{y}\|^2 - \|\underline{x}-\underline{y}\|^2\big) &= \tfrac{1}{4}\big(\underline{x}\cdot\underline{x} + 2\underline{x}\cdot\underline{y} + \underline{y}\cdot\underline{y}\big) - \tfrac{1}{4}\big(\underline{x}\cdot\underline{x} - 2\underline{x}\cdot\underline{y} + \underline{y}\cdot\underline{y}\big)\\ &= \underline{x}\cdot\underline{y}.\end{aligned}$$

We will use the fact that $\frac{1}{4}\big(\|\underline{x}+\underline{y}\|^2 - \|\underline{x}-\underline{y}\|^2\big)$ later in the proof.

(1) ⇒ (2) If Q is orthogonal, then $Q^TQ = I$ so

$$(Q\underline{x}) \cdot (Q\underline{y}) = (Q\underline{x})^T(Q\underline{y}) = \underline{x}^TQ^TQ\underline{y} = \underline{x}^T\underline{y} = \underline{x}\cdot\underline{y}.$$

(2) ⇒ (3) because (3) is a special case of (2), the case $\underline{x} = \underline{y}$.

(3) ⇒ (4) By using the hypothesis in (3) and the rabbit we obtain

$$\begin{aligned}\underline{x}\cdot\underline{y} &= \tfrac{1}{4}\big(\|\underline{x}+\underline{y}\|^2 - \|\underline{x}-\underline{y}\|^2\big)\\ &= \tfrac{1}{4}\big(\|Q(\underline{x}+\underline{y})\|^2 - \|Q(\underline{x}-\underline{y})\|^2\big)\\ &= \tfrac{1}{4}\big(\|Q\underline{x}+Q\underline{y}\|^2 - \|Q\underline{x}-Q\underline{y}\|^2\big)\\ &= (Q\underline{x})\cdot(Q\underline{y}).\end{aligned}$$

(We have just shown that (3) implies (2).) In particular, if $\{\underline{e}_1, \dots, \underline{e}_n\}$ is the standard basis for $\mathbb{R}^n$, then

$$\underline{e}_i \cdot \underline{e}_j = (Q\underline{e}_i)\cdot(Q\underline{e}_j) = \underline{Q}_i \cdot \underline{Q}_j.$$

But $\underline{e}_i \cdot \underline{e}_j = 0$ if $i \neq j$ and $= 1$ if $i = j$ so the columns of Q form an orthonormal set and therefore an orthonormal basis for $\mathbb{R}^n$.

(4) $\Rightarrow$ (1) The ij^{th} entry in Q^TQ is equal to the i^{th} row of Q^T times the i^{th} column of Q, i.e., to $\underline{Q}_i^T \underline{Q}_j = \underline{Q}_i \cdot \underline{Q}_j$ which is 1 when $i = j$ and 0 when $i \neq j$ so $Q^TQ = I$. □

7.1. Orthogonal linear transformations are of great practical importance because they do not change the lengths of vectors or, as a consequence of that, the angles between vectors. For this reason we often call the linear transformations given by orthogonal matrices "rigid motions". Moving a rigid object, by which we mean some some kind of physical structure, a submarine, a rocket, a spacecraft, or piece of machinery, in space does not change the lengths of its pieces or the angles between them.

7.2. The orthogonal groups. You should check the following facts: the identity matrix is orthogonal; a product of orthogonal matrices is an orthogonal matrix; the inverse of an orthogonal matrix is orthogonal. The set of all $n \times n$ orthogonal matrices is called the $n \times n$ orthogonal group and is denoted by $O(n)$. The orthogonal groups are fundamental objects in mathematics.

7.3. Rigid motions in $\mathbb{R}^2$. We have met two kinds of rigid motions in $\mathbb{R}^2$, rotations and reflections. Let's check that both are orthogonal transformations. If A_θ denotes the matrix representing the rotation by an angle θ in the counterclockwise direction, then

$$A_\theta (A_\theta)^T = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Hence A_θ is an orthogonal matrix.

On the other hand, reflection in the line L through the origin and a non-zero point $\begin{pmatrix} a \\ b \end{pmatrix}$ is given by the matrix

$$A = \frac{1}{a^2+b^2} \begin{pmatrix} a^2-b^2 & 2ab \\ 2ab & b^2-a^2 \end{pmatrix}.$$

This is an orthogonal linear transformation because

$$A^TA = A^2 = \frac{1}{(a^2+b^2)^2} \begin{pmatrix} a^4+2a^2b^2+b^4 & 0 \\ 0 & a^4+2a^2b^2+b^4 \end{pmatrix} = I.$$

Notice an important difference between rotations and reflections: the determinant of a rotation is $+1$ but the determinant of a reflection is -1.

PROPOSITION 7.2. *Every rigid motion in $\mathbb{R}^2$ is a composition of a rotation and a reflection.*

Proof. Let A be an orthogonal 2×2 matrix. □

7.4. The standard basis vectors $\underline{e}_1, \ldots, \underline{e}_n$ are orthogonal to one another. We said that an orthogonal matrix preserves the angles between vectors so, if that is correct, an orthogonal matrix A will have the property that the vectors $A\underline{e}_j$ are orthogonal to one another. But $A\underline{e}_j$ is the j^{th} column of A. Thus, the next result confirms what we have been saying.

THEOREM 7.3. *Let A be a symmetric matrix with real entries. Then there is an orthogonal matrix Q such that $Q^{-1}AQ$ is diagonal.*

Proof. ☐

THEOREM 7.4. *Let A be a diagonal matrix with real entries. For every orthogonal matrix Q, $Q^{-1}AQ$ is symmetric.*

Proof. A matrix is symmetric if it is equal to its transpose. We have

$$\left(Q^{-1}AQ\right)^T = Q^T A^T \left(Q^{-1}\right)^T = Q^{-1}A^T \left(Q^T\right)^T = Q^{-1}AQ$$

so $Q^{-1}AQ$ is symmetric. ☐

8. Orthogonal projections

Let V be a subspace of $\mathbb{R}^n$. Let $\{\underline{u}_1, \ldots, \underline{u}_k\}$ be an orthonormal basis for V.

The function $P_V : \mathbb{R}^n \to \mathbb{R}^n$ defined by the formula

$$P_V(\underline{v}) := (\underline{v} \cdot \underline{u}_1)\underline{u}_1 + \cdots + (\underline{v} \cdot \underline{u}_k)\underline{u}_k \tag{8-1}$$

is called the orthogonal projection of $\mathbb{R}^n$ onto V.

We are not yet justified in calling P_V *the* orthogonal projection of $\mathbb{R}^n$ onto V because the definition of P_V depends on the basis and every subspace of $\mathbb{R}^n$ of dimension ≥ 2 has *infinitely many* orthogonal bases. For example, if $a^2 + b^2 = 1$, then $\{(a, b), (b, -a)\}$ is an orthonormal basis for $\mathbb{R}^2$. In §**??** we will show that P_V does not depend on the choice of orthonormal basis; that will justify our use of the word *"the"*.[2]

PROPOSITION 8.1. *Let $\{\underline{u}_1, \ldots, \underline{u}_k\}$ be an orthonormal basis for V. The orthogonal projection $P_V : \mathbb{R}^n \to \mathbb{R}^n$ has the following properties:*

1. *it is a linear transformation;*
2. *$P_V(\underline{v}) = \underline{v}$ for all $\underline{v} \in V$;*
3. *$\mathcal{R}(P_V) = V$;*
4. *$\ker(P_V) = V^{\perp}$;*
5. *$P_V \circ P_V = P_V$.*[3]

---

[2]Thus, although the formula on the right-hand side of (8-1) depends on the choice of orthonormal basis the value $P_V(\underline{v})$ is independent of how it is computed.

[3]We usually abbreviate this by writing $P_V^2 = P_V$.

Proof. We will write P for P_V in this proof.

(1) To show that P is a linear transformation we must show that $P(a\underline{v}+b\underline{w}) = aP(\underline{v})+bP(\underline{w})$ for all $a, b \in \mathbb{R}$ and all $\underline{v}, \underline{w} \in \mathbb{R}^n$. To do this we simply calculate:

$$\begin{aligned} P(a\underline{v}+b\underline{w}) &= \big((a\underline{v}+b\underline{w})\cdot\underline{u}_1\big)\underline{u}_1 + \big((a\underline{v}+b\underline{w})\cdot\underline{u}_2\big)\underline{u}_2 + \cdots \\ &= \big(a(\underline{v}\cdot\underline{u}_1)+b(\underline{w}\cdot\underline{u}_1)\big)\underline{u}_1 + \big(a(\underline{v}\cdot\underline{u}_2)+b(\underline{w}\cdot\underline{u}_2)\big)\underline{u}_2 + \cdots \\ &= a(\underline{v}\cdot\underline{u}_1)\underline{u}_1 + b(\underline{w}\cdot\underline{u}_1)\underline{u}_1 + a(\underline{v}\cdot\underline{u}_2)\underline{u}_2 + b(\underline{w}\cdot\underline{u}_2)\underline{u}_2 + \cdots \\ &= a(\underline{v}\cdot\underline{u}_1)\underline{u}_1 + a(\underline{v}\cdot\underline{u}_2)\underline{u}_2 + \cdots + b(\underline{w}\cdot\underline{u}_1)\underline{u}_1 + b(\underline{w}\cdot\underline{u}_2)\underline{u}_2 + \cdots \\ &= aP(\underline{v}) + bP(\underline{w}). \end{aligned}$$

(2) Because the basis is orthonormal, $\underline{u}_i\cdot\underline{u}_i = 1$ and $\underline{u}_i\cdot\underline{u}_j = 0$ when $i \neq j$. Therefore $P(\underline{u}_i) = \underline{u}_i$ for each $i = 1, \ldots, k$.

Let $\underline{v} \in V$. Then $\underline{v} = a_1\underline{u}_1 + \cdots + a_k\underline{u}_k$ because $V = \operatorname{span}\{\underline{u}_1, \ldots, \underline{u}_k\}$. Therefore

$$\begin{aligned} P(\underline{v}) &= P(a_1\underline{u}_1 + \cdots + a_k\underline{u}_k) \\ &= a_1P(\underline{u}_1) + \cdots + a_kP(\underline{u}_k) \text{ because } P \text{ is a linear transformation} \\ &= a_1\underline{u}_1 + \cdots + a_k\underline{u}_k \\ &= \underline{v}. \end{aligned}$$

(3) Because (2) is true $V \subseteq \mathcal{R}(P)$. On the other hand, if $\underline{v}$ is any element in $\mathbb{R}^n$, then $P(\underline{v})$ is a linear combination of the $\underline{u}_i$s so belongs to V; i.e., $\mathcal{R}(P) \subseteq V$. Hence $\mathcal{R}(P) = V$.

(4) If $\underline{v} \in V^\perp$, then $\underline{v}\cdot\underline{u}_i = 0$ for all $\underline{u}_i$ so $P(\underline{v}) = 0$. Therefore $V^\perp \subseteq \ker(P)$. Conversely, if $\underline{w} \in \mathbb{R}^n$ and $P(\underline{w}) = \underline{0}$, then

$$(\underline{w}\cdot\underline{u}_1)\underline{u}_1 + \cdots + (\underline{w}\cdot\underline{u}_k)\underline{u}_k = 0;$$

but $\{\underline{u}_1, \ldots, \underline{u}_k\}$ is linearly independent so $\underline{w}\cdot\underline{u}_i = 0$ for all i. Therefore $\underline{w} \in \operatorname{Sp}\{\underline{u}_1, \ldots, \underline{u}_k\}^\perp = V^\perp$. We have shown that $\ker(P) \subseteq V^\perp$. Hence $\ker(P) = V^\perp$.

(5) Let $\underline{v} \in \mathbb{R}^n$. By (3), $P(\underline{v}) \in V$. However, $P(\underline{w}) = \underline{w}$ for all $\underline{w} \in V$ by (2). Applying this fact to $\underline{w} = P(\underline{v})$ we see that $(P \circ P)(\underline{v}) = P(P(\underline{v})) = \underline{v}$. Since this equality holds for all $\underline{v}$ in $\mathbb{R}^n$ we conclude that $P \circ P = P$. $\square$

The next result shows that $V + V^\perp = \mathbb{R}^n$, i.e., every element in $\mathbb{R}^n$ is the sum of an element in V and an element in $V^\perp$. Actually, the result shows more: there is only *one* way to write a vector $\underline{v} \in \mathbb{R}^n$ as the sum of an element in V and an element in $V^\perp$.

PROPOSITION 8.2. *Let V be a subspace of $\mathbb{R}^n$. If $\underline{v} \in \mathbb{R}^n$ there are unique elements $\underline{w} \in V$ and $\underline{w}' \in V^\perp$ such that $\underline{v} = \underline{w} + \underline{w}'$, namely $\underline{w} := P_V(\underline{v})$ and $\underline{w}' := \underline{v} - P_V(\underline{v})$.*

Proof. We write P for P_V in this proof.

We start with the trivial observation that

$$\underline{v} = P(\underline{v}) + \big(\underline{v} - P(\underline{v})\big). \tag{8-2}$$

By Proposition 8.1, $P(\underline{v})$ belongs to V. On the other hand,

$$P(\underline{v} - P(\underline{v})) = P(\underline{v}) - P(P(\underline{v})) = P(\underline{v}) - (P \circ P)(\underline{v}) = P(\underline{v}) - P(\underline{v}) = \underline{0}$$

so $\underline{v} - P(\underline{v}) \in \ker(P)$. But $\ker(P) = V^{\perp}$ by Proposition 8.1. Therefore the expression (8-2) shows that $\underline{v}$ is in $V + V^{\perp}$.

To show the uniqueness, suppose that $\underline{w}_1, \underline{w}_2 \in V$, that $\underline{x}_1, \underline{x}_2 \in V^{\perp}$, and that $\underline{w}_1 + \underline{x}_1 = \underline{w}_2 + \underline{x}_2$. Therefore $\underline{w}_1 - \underline{w}_2 = \underline{x}_2 - \underline{x}_1$; since V is a subspace $\underline{w}_1 - \underline{w}_2 \in V$; since $V^{\perp}$ is a subspace $\underline{x}_2 - \underline{x}_1 \in V^{\perp}$; but $V \cap V^{\perp} = \{\underline{0}\}$ so $\underline{w}_1 - \underline{w}_2 = \underline{x}_2 - \underline{x}_1 = 0$. Thus $\underline{w}_1 = \underline{w}_2$ and $\underline{x}_1 = \underline{x}_2$. This proves that an element of $\mathbb{R}^n$ is the sum of an element in V and an element in $V^{\perp}$ in a *unique* way. $\square$

The next result is just another way of stating Proposition 8.2.

COROLLARY 8.3. *Let V is a subspace of $\mathbb{R}^n$ and $\underline{v} \in \mathbb{R}^n$. The only point $\underline{w} \in V$ such that $\underline{v} - \underline{w} \in V^{\perp}$ is $\underline{w} = P(\underline{v})$.*

Proof. Suppose that $\underline{w} \in V$ and $\underline{v} - \underline{w} \in V^{\perp}$. The equation $\underline{v} = \underline{w} + (\underline{v} - \underline{w})$ expresses $\underline{v}$ as the sum of an element in V and an element in $V^{\perp}$. But the *only* way to express $\underline{v}$ as such a sum is $\underline{v} = P_V(\underline{v}) + (\underline{v} - P_V(\underline{v})$. Therefore $\underline{w} = P_V(\underline{v})$. $\square$

PROPOSITION 8.4. *If V is a subspace of $\mathbb{R}^n$, then*

$$\dim V + \dim V^{\perp} = n.$$

Proof. Since P_V is a linear transformation from $\mathbb{R}^n$ to itself there is a unique $n \times n$ matrix B such that $P_V(\underline{v}) = B\underline{v}$ for all $\underline{v} \in \mathbb{R}^n$. It is clear that $\mathcal{R}(P_V) = \mathcal{R}(B)$ and $\ker(P_V) = \mathcal{N}(B)$. But $\mathcal{R}(P_V) = V$ and $\ker(P_V) = V^{\perp}$ so

$$n = \operatorname{rank}(B) + \operatorname{nullity}(B) = \dim(V) + \dim(V^{\perp})$$

as claimed. $\square$

8.1. P_V is well-defined. The projection P_V was defined in terms of an orthonormal basis $\{\underline{u}_1, \ldots, \underline{u}_k\}$ for V. However, if $\dim(V) \geq 2$, then V has infinitely many orthonormal bases so why are we justified in calling P_V *the* orthogonal projection onto V? It is conceivable that if $\{\underline{w}_1, \ldots, \underline{w}_k\}$ is a different orthonormal basis for V then the linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$ defined by the formula

$$T(\underline{v}) := (\underline{v} \cdot \underline{w}_1)\underline{w}_1 + \cdots + (\underline{v} \cdot \underline{w}_k)\underline{w}_k$$

is not the same as P_V, i.e., perhaps there is a $\underline{v}$ such that $P_V(\underline{v}) \neq T(\underline{v})$.

<u>This does not happen</u> because we can use Proposition 8.2 to define

$$P_V(\underline{v}) := \begin{cases} \text{the unique } \underline{w} \in V \text{ such that} \\ \underline{v} = \underline{w} + \underline{w}' \text{ for some } \underline{w}' \in V^{\perp}. \end{cases}$$

Alternatively, using the point of view expressed by Corollary 8.3, we could define $P_V(\underline{v})$ to be the unique element of V such that $\underline{v} - P_V(\underline{v})$ belongs to $V^{\perp}$.

9. Least-squares "solutions" to inconsistent systems

A system of linear equations is inconsistent if it doesn't have a solution. Until now we have ignored inconsistent systems for what might seem sensible reasons—if $A\underline{x} = \underline{b}$ has no solutions what more is there to say? Actually, a lot!

Although there may be no solution to $A\underline{x} = \underline{b}$ we might still want to find an $\underline{x}$ such that $A\underline{x}$ is as close as possible to $\underline{b}$. For example, if $\underline{b}$ was obtained as a result of making error-prone measurements it might be that the true value is not $\underline{b}$ but some other point $\underline{b}^*$. If so, we should be seeking solutions to the equation $A\underline{x} = \underline{b}^*$ not $A\underline{x} = \underline{b}$.

The equation $A\underline{x} = \underline{b}$ has a solution if and only if $\underline{b}$ is in the range of A or, equivalently, if and only if $\underline{b}$ is a linear combination of the columns of A. Thus, if $A\underline{x} = \underline{b}$ has no solution it is sensible to replace $\underline{b}$ by the point $\underline{b}^*$ in $\mathcal{R}(A)$ closest to $\underline{b}$ and find a solution $\underline{x}^*$ to the equation $A\underline{x}^* = \underline{b}^*$; there *is* such an $\underline{x}^*$ because $\underline{b}^*$ is in the range of A.

We will now implement this idea. The first step is the next result. It says that the point in $\mathcal{R}(A)$ closest to $\underline{b}$ is $P(\underline{v})$ where $P : \mathbb{R}^n \to \mathbb{R}^n$ is the orthogonal projection onto $\mathcal{R}(A)$.[4]

Theorem 9.1 (The best approximation theorem,[5] BAT). *Let V be a subspace of $\mathbb{R}^n$ and $\underline{b}$ a point in $\mathbb{R}^n$. Then*

$$\|P_V(\underline{b}) - \underline{b}\| < \|\underline{w} - \underline{b}\|$$

for all other $\underline{w} \in V$. More precisely, the unique point in V closest to $\underline{b}$ is $P_V(\underline{b})$.[6]

Proof. To keep the notation simple let's write P for P_V.

Suppose $\underline{b} \in V$. Then $\underline{b}$ is the point in V closest to $\underline{b}$, duh! But $P(\underline{b}) = \underline{b}$ the theorem is true.

From now on we assume $\underline{b} \notin V$. Let $\underline{w} \in V$ and assume $\underline{w} \neq P(\underline{b})$.

The sides of the triangle in $\mathbb{R}^n$ with vertices $\underline{0}$, $\underline{b} - P(\underline{b})$, and $\underline{w} - P(\underline{b})$ have lengths $\|\underline{b} - \underline{w}\|$, $\|\underline{b} - P(\underline{b})\|$, and $\|\underline{w} - P(\underline{b})\|$. Notice that $\underline{b} - P(\underline{b}) \in V^\perp$, and $\underline{w} - P(\underline{b}) \in V$ because it is a difference of elements in the subspace V. It follows that the line through $\underline{0}$ and $\underline{b} - P(\underline{b})$ is perpendicular to the line

---

[4]When you read the statement of the theorem you will see that it does not *exactly* say that. The theorem states a more general result. Try to understand why the theorem implies $P(\underline{v})$ is *the* point in $\mathcal{R}(A)$ closest to $\underline{b}$. If you can't figure this out, ask.

[5]The adjective "best" applies to the word "approximation", not to the word "theorem".

[6]We use the word *unique* to emphasize the fact that there is only *one* point in V that is closest to $\underline{b}$. This fact is not obvious even though your geometric intuition might suggest otherwise. If we drop the requirement that V is a subspace there can be more than one point in V that is closest to some given point $\underline{b}$. For example, if V is the circle $x^2 + y^2 = 1$ in $\mathbb{R}^2$ and $\underline{b} = (0, 0)$, then *all* points in V have the same distance from $\underline{b}$. Likewise, if $\underline{b} = (0, 2)$ and V is the parabola $y = x^2$ in $\mathbb{R}^2$, there are two points on V that are closest to $\underline{b}$, namely $\left(\sqrt{\frac{3}{2}}, \frac{3}{2}\right)$ and $\left(-\sqrt{\frac{3}{2}}, \frac{3}{2}\right)$.

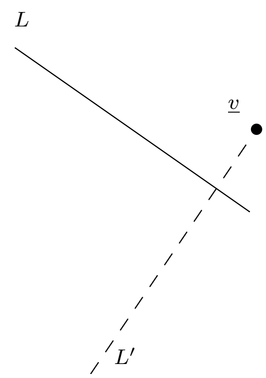
through $\underline{0}$ and $\underline{w} - P(\underline{b})$. Thus, the triangle has a right angle at the origin. The longest side of a right-angled triangle is its hypotenuse which, in this case, is the line through $\underline{b} - P(\underline{b})$, and $\underline{w} - P(\underline{b})$. That side has length

$$\|(\underline{w} - P(\underline{b})) - (\underline{b} - P(\underline{b}))\| = \|\underline{w} - \underline{b}\|.$$

Therefore $\|\underline{w} - \underline{b}\| > \|\underline{b} - P(\underline{b})\|$. □

9.1. The point in V closest to $\underline{v}$. Let V be a subspace of $\mathbb{R}^n$ and $\underline{v}$ a point in $\mathbb{R}^n$. How do we find/compute the point in V that is closest to $\underline{v}$? We will show that $P_V(\underline{v})$ is the point in V that is closest to $\underline{v}$.

We begin with a high school question. Let L be a line through the origin in $\mathbb{R}^2$ and $\underline{v}$ a point in $\mathbb{R}^2$; which point on L is closest to $\underline{v}$? Here's a picture to help you think about the question:



It is pretty obvious that one should draw a line L' through $\underline{v}$ that is perpendicular to L and the intersection point $L \cap L'$ will be the point on L closest to $\underline{v}$.

That is the idea behind the next result because the point $L \cap L'$ is $P_L(\underline{v})$.

9.2. A problem: find the line that best fits the data. Given points

$$(\alpha_1, \beta_1), \dots, (\alpha_m, \beta_m)$$

in $\mathbb{R}^2$ find the line $y = dx + c$ that best approximates those points. In general there will not be a line passing through all the points but we still want "the best line". This sort of problem is typical when gathering data to understand the relationship between two variables x and y. The data obtained might suggest a linear relationship between x and y but, especially in the social sciences, it is rare that the data gathered spells out an exact linear relationship.

We restate the question of finding the line $y = dx + c$ as a linear algebra problem. The problem of finding the line that fits the data (α_i, β_i), $1 \leq i \leq$

m is equivalent to finding d and c such that

$$\begin{aligned} \beta_1 &= d\alpha_1 + c \\ \beta_2 &= d\alpha_2 + c \\ \beta_3 &= d\alpha_3 + c \\ \vdots &\quad \vdots \\ \beta_m &= d\alpha_m + c_m \end{aligned}$$

which is, in turn, Equivalent to finding d and c such that

$$\begin{pmatrix} \alpha_1 & 1 \\ \alpha_2 & 1 \\ \alpha_3 & 1 \\ \vdots & \vdots \\ \alpha_m & 1 \end{pmatrix} \begin{pmatrix} d \\ c \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \vdots \\ \beta_m \end{pmatrix} \qquad \text{or} \qquad A \begin{pmatrix} d \\ c \end{pmatrix} = \underline{b}$$

where A is an $m \times 2$ matrix and $\underline{b} \in \mathbb{R}^m$.

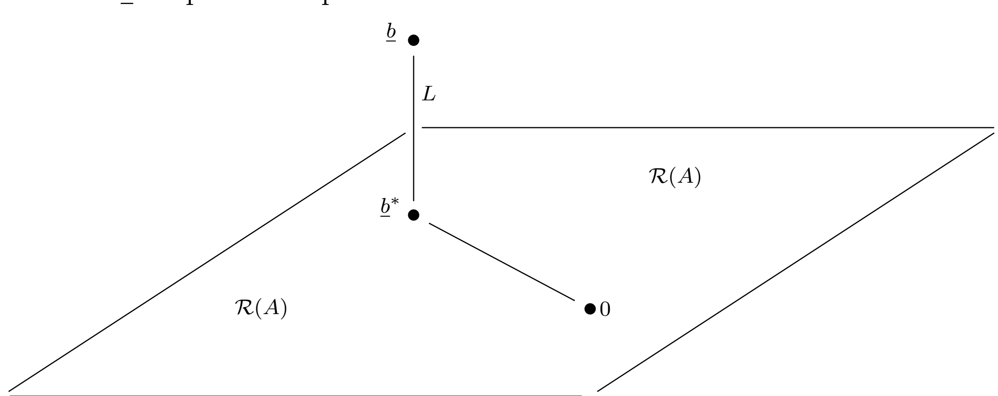
As we said, there is usually no solution $\binom{d}{c}$ to this system of linear equations but we still want to find a line that is as close as possible to the given points. The next definition makes the idea “as close as possible” precise.

Definition 9.2. *Let A be an $m \times n$ matrix and $\underline{b}$ a point in $\mathbb{R}^m$. We call $\underline{x}^*$ a* least-squares “solution” *to the equation $A\underline{x} = \underline{b}$ if $A\underline{x}^*$ is as close as possible to $\underline{b}$; i.e.,*

$$\|A\underline{x}^* - \underline{b}\| \leq \|A\underline{x} - \underline{b}\| \qquad \text{for all } \underline{x} \in \mathbb{R}^n.$$

We will now explain how to find $\underline{x}^*$

Because $A\underline{x}^*$ is in the range of A we want $A\underline{x}^*$ to be the (unique!) point in $\mathcal{R}(A)$ that is closest to $\underline{b}$. Let's write $\underline{b}^*$ for the point in $\mathcal{R}(A)$ that is closest to $\underline{b}$. A picture helps:



Lemma 9.3. *Let A be an $m \times n$ matrix and $\underline{v} \in \mathbb{R}^m$. Consider $\underline{v}$ as a column vector. Then $\underline{v} \in \mathcal{R}(A)^\perp$ if and only if $A^T\underline{v} = \underline{0}$.*

Proof. Since the range of A is the linear span of the columns of A, $\underline{v} \in \mathcal{R}(A)^\perp$ if and only if $\underline{A}_1 \cdot \underline{v} = \cdots = \underline{A}_n \cdot \underline{v} = 0$. However, $\underline{A}_j \cdot \underline{v} = \underline{A}_j^T \underline{v}$ so $\underline{v} \in \mathcal{R}(A)^\perp$ if and only if $\underline{A}_1^T \underline{v} = \cdots = \underline{A}_n^T \underline{v} = 0$. But $\underline{A}_j^T$ is the j^{th} row of A^T so $\underline{v} \in \mathcal{R}(A)^\perp$ if and only if $A^T \underline{v} = \underline{0}$. □

With reference to the picture above, $\underline{b} - \underline{b}^* \in \mathcal{R}(A)^\perp$ if and only if $A^T(\underline{b} - \underline{b}^*) = 0$.

Lemma 9.4. *Let A be an $m \times n$ matrix and let $P : \mathbb{R}^n \to \mathbb{R}^n$ be the orthogonal projection onto $\mathcal{R}(A)$. Define*

$$\underline{b}^* := P(\underline{b}).$$

Then $\underline{b}^*$ is the unique point in $\mathcal{R}(A)$

1. *that is closest to $\underline{b}$;*
2. *such that $\underline{b} - \underline{b}^* \in \mathcal{R}(A)^\perp$;*
3. *such that $A^T(\underline{b} - \underline{b}^*) = 0$.*

Proof. (1) This is what Theorem 9.1 says.
(2) This is what Corollary 8.3 says.
(3) This follows from (2) and Lemma 9.3. □

The point in $\mathcal{R}(A)$ closest to $\underline{b}$ is the unique point $\underline{b}^*$ in $\mathcal{R}(A)$ such that $A^T\underline{b} = A^T\underline{b}^*$.

Since $\underline{b}^*$ is in $\mathcal{R}(A)$, there is a vector $\underline{x}^*$ such that $A\underline{x}^* = \underline{b}^*$. It follows that

$$A^T A\underline{x}^* = A^T\underline{b}^* = A^T\underline{b}.$$

The preceding argument has proved the following result.

Theorem 9.5. *Let A be an $m \times n$ matrix and $\underline{b}$ a point in $\mathbb{R}^m$. There is a point $\underline{x}^*$ in $\mathbb{R}^n$ having the following equivalent properties:*

1. $A^T A\underline{x}^* = A^T\underline{b}$;
2. *$A\underline{x}^*$ is the point in $\mathcal{R}(A)$ that is closest to $\underline{b}$;*
3. *$\underline{x}^*$ is a least-squares solution to $A\underline{x} = \underline{b}$.*

Moreover, $\underline{x}^*$ is unique if and only if $\mathcal{N}(A) = 0$.

Theorem 9.6. *Let $A\underline{x} = \underline{b}$ be an $m \times n$ system of linear equations.*

1. *The system $A^T A\underline{x} = A^T\underline{b}$ is consistent.*
2. *The solutions to the system $A^T A\underline{x} = A^T\underline{b}$ are least-squares solutions to $A\underline{x} = \underline{b}$.*
3. *There is a unique least squares solution if and only if* $\operatorname{rank}(A) = n$.

10. Approximating data by polynomial curves

When engineers lay out the path for a new a freeway they often do so under the constraint that the curve/path is a piecewise cubic curve. Let me explain. Suppose one wants a freeway to begin at a point (a, b) in $\mathbb{R}^2$ and end at the point (a', b'). Of course, it is unreasonable to have the freeway be a straight line: there might be geographical obstacles, or important buildings and other things to be avoided, or one might want the freeway to pass close to some particular points, towns, other roads, etc. At the other extreme one doesn't want the freeway to be "too curvy" because a very curvy road is dangerous and more expensive to build. What one tends to do is break the interval $[a, a']$ into subintervals, say

$$[a, a_1],\ [a_1, a_2], \ldots, [a_n, a']$$

where $a < a_1 < \ldots < a_n < a'$ and then decide on some points $(a_1, b_1), \ldots, (a_n, b_n)$ that one would like the freeway to pass through.

Calculus tells us that a cubic curve $y = \alpha x^3 + \beta x^2 + \gamma x + \delta$ has at most two maxima and minima or, less formally, two major bends.

Let's look at

Given points

$$(\alpha_1, \beta_1), \ldots, (\alpha_m, \beta_m)$$

in $\mathbb{R}^2$ we might want to find a degree 2 polynomial $f(x)$ such that the curve $y = f(x)$ best approximate those points. In general there will not be a degree 2 curve that passes through all the points but we still want "the best curve". We could also ask for the best cubic curve, etc. All these problems are solved by using the general method in section 9. For example, if we are looking for a degree two curve we are looking for a, b, c such that $y = ax^2 + bx + c$ best fits the data. That problem reduces to solving the system

$$\begin{pmatrix} \alpha_1^2 & \alpha_1 & 1 \\ \alpha_2^2 & \alpha_2 & 1 \\ \alpha_3^2 & \alpha_3 & 1 \\ \vdots & \vdots & \vdots \\ \alpha_m^2 & \alpha_m & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \vdots \\ \beta_m \end{pmatrix} \qquad \text{or} \qquad A \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \underline{b}$$

where A is an $m \times 3$ matrix and $\underline{b} \in \mathbb{R}^m$.

So, using the ideas in chapter 9 we must solve the equation

$$A^T A \underline{x}^* = A^T \underline{b}$$

to get an a^*, b^*, and c^* that gives a parabola $y = a^* x^2 + b^* x + c^*$ that best fits the data.

10.1. Why call it least-squares? We are finding an $\underline{x}$ that minimizes $\|A\underline{x} - \underline{b}\|$ and hence $\|A\underline{x} - \underline{b}\|^2$ But

$$\|A\underline{x} - \underline{b}\|^2 = (A\underline{x} - \underline{b}) \cdot (A\underline{x} - \underline{b}) = \text{a sum of squares.}$$

11. Gazing into the distance: Fourier series

12. Infinite sequences

CHAPTER 16

Similar matrices

1. Definition

Similar matrices are just that, similar, very similar, in a sense so alike as to be indistinguishable in their essential properties. Although a precise definition is required, and will be given shortly, it should be apparent that the matrices

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

are, in the everyday sense of the word, "similar". Multiplication by A and multiplication by B are linear transformations from $\mathbb{R}^2$ to $\mathbb{R}^2$; A sends $\underline{e}_1$ to itself and kills $\underline{e}_2$; B sends $\underline{e}_2$ to itself and kills $\underline{e}_1$. Pretty similar behavior, huh!?

2. Definition and first properties

.

Let A and B be $n \times n$ matrices. We say that A is <u>similar</u> to B and write $A \sim B$ if there is an invertible matrix S such that

$$A = SBS^{-1}.$$

Similarity of matrices is an equivalence relation meaning that

(1) $A \sim A$ because $A = IAI^{-1}$;
(2) if $A \sim B$, then $B \sim A$ because $A = SBS^{-1}$ implies $S^{-1}AS = S^{-1}(SBS^{-1})S = (S^{-1}S)B(S^{-1}S) = IBI = B$;
(3) if $A \sim B$ and $B \sim C$, then $A \sim C$ because $A = SBS^{-1}$ and $B = TCT^{-1}$ implies $A = SBS^{-1} = S(TCT^{-1})S^{-1} = (ST)C(T^{-1}S^{-1}) = (ST)C(ST)^{-1}$.

Thus, the word "similar" behaves as it does in its everyday use:

(1) a thing is similar to itself;
(2) if one thing is similar to another thing, then the other thing is similar to the first thing;
(3) if a thing is similar to a second thing and the second thing is similar to a third thing, then the first thing is similar to the third thing.

3. Example

Let's return to the example in chapter 1. The only difference between A and B is the choice of labeling: which order do we choose to write

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

or, if you prefer, which is labelled $\underline{e}_1$ and which is labelled $\underline{e}_2$.

There is a linear transformation from $\mathbb{R}^2$ to $\mathbb{R}^2$ that interchanges $\underline{e}_1$ and $\underline{e}_2$, namely

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \qquad S\underline{e}_1 = \underline{e}_2 \quad \text{and} \quad S\underline{e}_2 = \underline{e}_1.$$

Since $S^2 = I$, $S^{-1} = S$ and

$$SBS^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = A.$$

The calculation shows that $A = SBS^{-1}$; i.e., A is similar to B in the technical sense of the definition in chapter 2.

4

We now show that similar matrices have some of the same properties.

THEOREM 4.1. *Similar matrices have the same*

(1) *determinant;*
(2) *characteristic polynomial;*
(3) *eigenvalues.*

Proof. Suppose A and B are similar. Then $A = SBS^{-1}$ for some invertible matrix S.

(1) Since $\det(S^{-1}) = (\det S)^{-1}$, we have

$$\det(A) = (\det S)(\det B)(\det S^{-1}) = (\det S)(\det B)(\det S)^{-1} = \det(B).$$

We used the fact that the determinant of a matrix is a number.

(2) Since $S(tI)S^{-1} = tI$, $A - tI = S(B - tI)S^{-1}$; i.e., $A - tI$ and $B - tI$ are similar. (2) now follows from (1) because the characteristic polynomial of A is $\det(A - tI)$.

(3) The eigenvalues of a matrix are the roots of its characteristic polynomial. Since A and B have the same characteristic polynomial they have the same eigenvalues. □

4.1. Warning: Although they have the same eigenvalues similar matrices do *not* usually have the same eigenvectors or eigenspaces. Nevertheless, there is a precise relationship between the eigenspaces of similar matrices. We prove that in Proposition 4.2

4.2. Notation: If A is an $n \times n$ matrix and X a subset of $\mathbb{R}^n$, we use the notation

$$AX := \{A\underline{x} \mid \underline{x} \in \mathbb{R}^n\}.$$

This shorthand is similar to the notation $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ for the even numbers.

To check whether you understand this notation try the following problems.

(1) Show that AX is a subspace if X is.
(2) Show that $A(BX) = (AB)X$ if A and B are $n \times n$ matrices.
(3) Show that $IX = X$.
(4) If S is an invertible matrix and $Y = SX$, show that $X = S^{-1}Y$.
(5) If S is an invertible matrix and X is a subspace of $\mathbb{R}^n$ show that $\dim SX = \dim X$ by proving the following claim: if $\{\underline{v}_1, \ldots, \underline{v}_d\}$ is a basis for X, then $\{S\underline{v}_1, \ldots, S\underline{v}_d\}$ is a basis for SX.

PROPOSITION 4.2. *Suppose $A = SBS^{-1}$. Let $E_\lambda(A)$ be the λ-eigenspace for A and $E_\lambda(B)$ the λ-eigenspace for B. Then $E_\lambda(B) = S^{-1}E_\lambda(A)$, i.e.,*

$$E_\lambda(B) = \{S^{-1}\underline{x} \mid \underline{x} \in E_\lambda(A)\}.$$

In particular, the dimensions of the λ-eigenspaces for A and B are the same.

Proof. If $\underline{x} \in E_\lambda(A)$, then $\lambda\underline{x} = A\underline{x} = SBS^{-1}\underline{x}$ so

$$B(S^{-1}\underline{x}) = S^{-1}\lambda\underline{x} = \lambda(S^{-1}\underline{x});$$

i.e., $S^{-1}\underline{x}$ is a λ-eigenvector for B or, equivalently,

$$S^{-1}E_\lambda(A) \subseteq E_\lambda(B).$$

Starting from the fact that $B = S^{-1}AS$, the same sort of argument shows that $SE_\lambda(B) \subseteq E_\lambda(A)$.

Therefore

$$E_\lambda(B) = I.E_\lambda(B) = S^{-1}S.E_\lambda(B) \subseteq S^{-1}.E_\lambda(A) \subseteq E_\lambda(B).$$

In particular, $E_\lambda(B) \subseteq S^{-1}.E_\lambda(A) \subseteq E_\lambda(B)$ so these three sets are equal, i.e., $E_\lambda(B) = S^{-1}.E_\lambda(A) = \{S^{-1}\underline{x} \mid \underline{x} \in E_\lambda(A)\}$.

That $\dim E_\lambda(A) = \dim E_\lambda(B)$ is proved by method suggested in exercise 5 just prior to the statement of this proposition. $\square$

If A and B are similar and $A^r = 0$, then $B^r = 0$. To see this one uses the marvelous cancellation trick, $S^{-1}S = I$.

COROLLARY 4.3. *Similar matrices have there same rank and the same nullity.*

Proof. Suppose A and B are similar matrices. By definition, the nullity of A is the dimension of its null space. But $\mathcal{N}(A) = E_0(A)$, the 0-eigenspace of A. By the last sentence in the statement of Proposition 4.2, $E_0(A)$ and $E_0(B)$ have the same dimension. Hence A and B have the same nullity. Since rank +nullity $= n$, A and B also have the same rank. $\square$

4.3. Intrinsic and extrinsic properties of matrices. It is not unreasonable to ask whether a matrix that is similar to a symmetric matrix is symmetric. Suppose A is symmetric and S is invertible. Then $(SAS^{-1})^T = (S^{-1})^T A^T S^T = (S^T)^{-1} A S^T$ and there is no obvious reason which this should be the same as SAS^{-1}. The explicit example

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 8 & 11 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 8 & -5 \\ 3 & -2 \end{pmatrix}$$

shows that a matrix similar to a symmetric matrix need not be symmetric.

PAUL - More to say.

5. Diagonalizable matrices

5.1. Diagonal matrices. A square matrix $D = (d_{ij})$ is <u>diagonal</u> if $d_{ij} = 0$ for all $i \neq j$. In other words,

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_{n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

for some $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$. We sometimes use the abbreviation

$$\operatorname{diag}(\lambda_1, \ldots, \lambda_n) = \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_{n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_n \end{pmatrix}.$$

The identity matrix and the zero matrix are diagonal matrices.

Let $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$. The following facts are obvious:

(1) the λ_is are the eigenvalues of D;
(2) $\det(D) = \lambda_1 \lambda_2 \cdots \lambda_n$;
(3) the characteristic polynomial of D is $(\lambda_1 - t)(\lambda_2 - t)\cdots(\lambda_n - t)$;
(4) $D\underline{e}_j = \lambda_j \underline{e}_j$, i.e., the standard basis vectors $\underline{e}_j$ are eigenvectors for D.

Warning: Although the axis $\mathbb{R}\underline{e}_j$ is contained in λ_j-eigenspace for D its λ_j-eigenspace might be bigger. For example, if $\lambda_i = \lambda_j$, then the E_{λ_i} contains the plane $\mathbb{R}\underline{e}_i + \mathbb{R}\underline{e}_j$.

5.2. Definition. An $n \times n$ matrix A is <u>diagonalizable</u> if it is similar to a diagonal matrix, i.e., if $S^{-1}AS$ is diagonal for some S.

A diagonal matrix is diagonalizable: if D is diagonal, then $I^{-1}DI$ is diagonal!

Since similar matrices have the same characteristic polynomials, the characteristic polynomial of a diagonalizable matrix is a product of n linear terms. See "obvious fact" (3) above.

5.3. Example. If

$$A = \begin{pmatrix} 5 & -6 \\ 3 & -4 \end{pmatrix} \qquad \text{and} \qquad S = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},$$

then

$$S^{-1}AS = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 5 & -6 \\ 3 & -4 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}$$

so A is diagonalizable.

5.4. The obvious questions are *how do we determine whether A is diagonalizable or not* and if A is diagonalizable *how do we find an S such that $S^{-1}AS$ is diagonal.* The next theorem and its corollary answer these questions.

THEOREM 5.1. *An $n \times n$ matrix A is diagonalizable if and only if it has n linearly independent eigenvectors.*

Proof. We will use the following fact. If B is a $p \times q$ matrix and C a $q \times r$ matrix, then the columns of BC are obtained by multiplying each column of C by B; explicitly,

$$BC = [B\underline{C}_1, \ldots, B\underline{C}_r]$$

where $\underline{C}_j$ is the j^{th} column of C.

($\Leftarrow$) Let $\{\underline{u}_1, \ldots, \underline{u}_n\}$ be linearly independent eigenvectors for A with $A\underline{u}_j = \lambda_j \underline{u}_j$ for each j. Define

$$S := [\underline{u}_1, \ldots, \underline{u}_n],$$

i.e., the j^{th} column of S is $\underline{u}_j$. The columns of S are linearly independent so S is invertible. Since

$$I = S^{-1}S = S^{-1}[\underline{u}_1, \ldots, \underline{u}_n] = [S^{-1}\underline{u}_1, \ldots, S^{-1}\underline{u}_n],$$

$S^{-1}\underline{u}_j = \underline{e}_j$, the j^{th} standard basis vector.

Now

$$\begin{aligned}
S^{-1}AS &= S^{-1}A[\underline{u}_1, \dots, \underline{u}_n] \\
&= S^{-1}[A\underline{u}_1, \dots, A\underline{u}_n] \\
&= S^{-1}[\lambda_1\underline{u}_1, \dots, \lambda_n\underline{u}_n] \\
&= [\lambda_1 S^{-1}\underline{u}_1, \dots, \lambda_n S^{-1}\underline{u}_n] \\
&= [\lambda_1\underline{e}_1, \dots, \lambda_n\underline{e}_n] \\
&= \begin{pmatrix}
\lambda_1 & 0 & 0 & \cdots & 0 & 0 \\
0 & \lambda_2 & 0 & \cdots & 0 & 0 \\
0 & 0 & \lambda_3 & \cdots & 0 & 0 \\
\vdots & & & \ddots & & \vdots \\
0 & 0 & 0 & \cdots & \lambda_{n-1} & 0 \\
0 & 0 & 0 & \cdots & 0 & \lambda_n
\end{pmatrix}.
\end{aligned}$$

Thus A is diagonalizable.

($\Rightarrow$) Now suppose A is diagonalizable, i.e.,

$$S^{-1}AS = D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$$

for some invertible S. Now

$$\begin{aligned}
[A\underline{S}_1, \dots, A\underline{S}_n] &= AS \\
&= SD \\
&= S[\lambda_1\underline{e}_1, \dots, \lambda_n\underline{e}_n] \\
&= [\lambda_1 S\underline{e}_1, \dots, \lambda_n S\underline{e}_n] \\
&= [\lambda_1\underline{S}_1, \dots, \lambda_n\underline{S}_n]
\end{aligned}$$

so $A\underline{S}_j = \lambda_j\underline{S}_j$ for all j. But the columns of S are linearly independent so A has n linearly independent eigenvectors for A. □

The proof of Theorem 5.1 established the truth of the following corollary.

COROLLARY 5.2. *If A is a diagonalizable $n \times n$ matrix and $\underline{u}_1, \dots, \underline{u}_n$ are linearly independent eigenvectors for A and $S = [\underline{u}_1, \dots, \underline{u}_n]$, then $S^{-1}AS$ is diagonal.*

COROLLARY 5.3. *If an $n \times n$ matrix has n distinct eigenvalues it is diagonalizable.*

Proof. Suppose $\lambda_1, \dots, \lambda_n$ are the distinct eigenvalues for A and for each i let $\underline{v}_i$ be a non-zero vector such that $A\underline{v}_i = \lambda_i\underline{v}_i$. By Theorem 1.2, $\{\underline{v}_1, \dots, \underline{v}_n\}$ is a linearly independent set. It now follows from Theorem 5.1 that $A$is diagonalizable. □

5.5. Previous example revisited. We showed above that

$$A = \begin{pmatrix} 5 & -6 \\ 3 & -4 \end{pmatrix}$$

is diagonalizable. Let's suppose we did not know that and had to find out whether is was diagonalizable and, if so to find a matrix S such that $S^{-1}AS$ is diagonal. Theorem 5.1 says we must determine whether A has two linearly independent eigenvectors.

The characteristic polynomial of A is $t^2 - t(a+d) + ad - bc$, i.e.,

$$t^2 - t - 2 = (t-2)(t+1).$$

The eigenvalues for A are 2 and -1. By Corollary 5.3, A is diagonalizable. To find an S we need to find eigenvectors for A. The 2-eigenspace is

$$E_2 = \mathcal{N}(A - 2I) = \mathcal{N}\begin{pmatrix} 3 & -6 \\ 3 & -6 \end{pmatrix} = \mathbb{R}\begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

The (-1)-eigenspace is

$$E_{-1} = \mathcal{N}(A + I) = \mathcal{N}\begin{pmatrix} 6 & -6 \\ 3 & -3 \end{pmatrix} = \mathbb{R}\begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Thus S can be any matrix with one column a non-zero multiple of $(2\ 1)^T$ and the other a non-zero multiple of $(1\ 1)^T$. For example, the matrix we used before, namely

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},$$

works.

It is important to realize that S is not the only matrix that "works". For example, if

$$R = \begin{pmatrix} 3 & -2 \\ 3 & -1 \end{pmatrix}.$$

Now

$$R^{-1}AR = \frac{1}{3}\begin{pmatrix} -1 & 2 \\ -3 & 3 \end{pmatrix}\begin{pmatrix} 5 & -6 \\ 3 & -4 \end{pmatrix}\begin{pmatrix} 3 & -2 \\ 3 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 2 \end{pmatrix}.$$

Notice that $R^{-1}AR \neq S^{-1}AS$. In particular, A is similar to two different diagonal matrices.

CHAPTER 17

Words and terminology

1. The need for clarity and precision

Definitions constitute the rock on which mathematics rests. Definitions must be precise and unambiguous. The should be expressed in simple language that is easy to understand. The mathematical edifice built upon this rock consists of results, usually called Lemmas, Propositions, Theorems, and Corollaries. I won't discuss the question of which types of results should receive which of those labels. Results, like definitions, must be stated clearly, accurately, and precisely. They should be unambiguous and easy to understand.

Students taking linear algebra find it a challenge to state definitions and results with the required clarity and precision. But clarity of thought and clarity of statement go hand-in-hand. You can't have one without the other and as the clarity and precision of one increases so does that of the other. Do not confuse the requirement for clarity and precision with a pedantic adherence to the rules of grammar. The demand for clarity and precision is a demand that you truly understand what you think, write, and say.

Be clear in what you write. Put yourself in the shoes of the reader. Particularly when stating a definition or result put yourself in the shoes of a reader who has never seen that definition or result before. When I see a student's inaccurate statement of a definition or result I can guess what they *want* to say. But I am not grading you on what you *want* to say. I am grading you on the basis of what you *do* say. When I read your statement I ask myself *"is this statement good enough to appear in a textbook?"* and *"does this statement tell someone who has never before seen the statement, or a variation on it, exactly what the author wants to, or should, convey?"*

2. Some, all, each, every, and only

In your everyday life you know that a statement beginning *"Some dogs ..."* is very different from one that begins *"All dogs ..."*. The three words *"some"*, *"all"*, and *"every"*, play a crucial role in mathematics. Try to use them whenever it is appropriate to do so—there is rarely a situation in which a variation on one of those three words is better than using the word itself.

Let's consider the definition of a linear transformation.

2.1. The following definition is perfect:

> A function $T : V \to W$ between two vector spaces is a linear transformation if $T(a\underline{u} + b\underline{u}) = aT(\underline{u}) + bT(\underline{v})$ for all $\underline{u}, \underline{v} \in V$ and all $a, b \in \mathbb{R}$.

Here is a less than perfect version of that definition.

> A function $T : V \to W$ between two vector spaces is a linear transformation if $T(a\underline{u} + b\underline{u}) = aT(\underline{u}) + bT(\underline{v})$ where $\underline{u}, \underline{v} \in V$ and $a, b \in \mathbb{R}$.

The words *"for all"* have been replaced by *"where"*. The word *"where"* has many meanings (check the dictionary if you need convincing) and in this situation it does not have the clarity that *"for all"* does. When I read *"where"* I have to pause and ask myself which of its meanings is being used but when I read *"for all"* I do not have to pause and think.

Here is an incorrect version of that definition.

> A function $T : V \to W$ between two vector spaces is a linear transformation if $T(a\underline{u} + b\underline{u}) = aT(\underline{u}) + bT(\underline{v})$ for some $\underline{u}, \underline{v} \in V$ and $a, b \in \mathbb{R}$.

This is wrong because *"some"* has a different meaning than *"all"*. Consider the sentences *"Some dogs have rabies"* and *"All dogs have rabies"*.

There are mathematical statements in which the word *"where"* is appropriate. For example:

> If V is a subspace of $\mathbb{R}^n$, then every point $\underline{w} \in \mathbb{R}^n$ can be written in a unique way as $\underline{w} = \underline{v} + \underline{v}'$ where $\underline{v} \in V$ and $\underline{v}' \in V^{\perp}$.

The sentence is intended to state the fact that every point in $\mathbb{R}^n$ is the sum of a point in V and a point in $V^{\perp}$, and there is only one way in which that happens, i.e., if $\underline{u}$ and $\underline{v}$ are in V and $\underline{u}'$ and $\underline{v}'$ are in $V^{\perp}$ and $\underline{v}+\underline{v}' = \underline{u}+\underline{u}'$, then $\underline{u} = \underline{v}$ and $\underline{u}' = \underline{v}'$. I think the displayed sentence does convey that but perhaps there is a better way to convey that fact. What do you think? One alternative is this:

> If V is a subspace of $\mathbb{R}^n$ and $\underline{w} \in \mathbb{R}^n$, then there is a unique $\underline{v} \in V$ and a unique $\underline{v}' \in V^{\perp}$ such that $\underline{w} = \underline{v} + \underline{v}'$.

What do you think of the alternatives?

2.2. The following is the definition of what it means for a set of vectors to be orthogonal.

> We say that $\{\underline{v}_1, \ldots, \underline{v}_k\}$ is orthogonal if $\underline{v}_i \cdot \underline{v}_j = 0$ for all $i \neq j$.

I think it is implicit in the statement that this must be true for all pairs of different numbers between 1 and n but it is not unreasonable to argue that one should make it clearer that $\underline{v}_i \cdot \underline{v}_j = 0$ for all $i, j \in \{1, \ldots, n\}$ such that $i \neq j$. The words *"for all"* are suggesting that one is making a statement about all pairs of distinct numbers i and j in *some* collection of pairs. In any case, it seems to me that the word *"all"* should be used in this definition. The following version of the definition seems less clear:

> We say that $\{\underline{v}_1, \dots, \underline{v}_k\}$ is orthogonal if $\underline{v}_i \cdot \underline{v}_j = 0$ where $i \neq j$.

"Where" seems to need some interpretation and may be mis-interpreted. Better to use the word *"all"* because there is little possibility it can be misunderstood.

2.3. I used the word *"where"* in my definition of linear span.

> A <u>linear combination</u> of vectors $\underline{v}_1, \dots, \underline{v}_n$ in $\mathbb{R}^m$ is a vector that can be written as
>
> $$a_1\underline{v}_1 + \cdots + a_n\underline{v}_n$$
>
> for some numbers $a_1, \dots, a_n \in \mathbb{R}$.
>
> Let A be any $m \times n$ matrix and $\underline{x} \in \mathbb{R}^n$. Then $A\underline{x}$ is a linear combination of the columns of A. Explicitly,

$$A\underline{x} = x_1\underline{A}_1 + \cdots + x_n\underline{A}_n \tag{2-1}$$

> where $\underline{A}_j$ denotes the j^{th} column of A.
>
> A function $T : V \to W$ between two vector spaces is a linear transformation if $T(a\underline{u} + b\underline{u}) = aT(\underline{u}) + bT(\underline{v})$ where $\underline{u}, \underline{v} \in V$ and $a, b \in \mathbb{R}$.

2.4. Try to avoid *"where"*. I think it is a good general rule to avoid using the word *"where"* whenever possible. I don't think it is good to *never* use the word *"where"* in mathematics, but certainly it should be avoided if there is a clear alternative that conveys your meaning without making the sentence clunky.

3. Singular and plural

> A system of linear equations is consistent if it has a solution and inconsistent if it doesn't.

The subject of this sentence, *"A system"* is singular. The system may consist of many equations but the system is a single entity.

The subject of a sentence beginning *"The people of America ..."* is *plural* so it would be correct to proceed with the word *"are"*. The subject of a sentence beginning *"The population of America ..."* is *singular* so it would be correct to proceed with the word *"is"*.

4. The word *"it"*

The word *"it"* is versatile. But danger lurks in in its versatility. A writer must ensure that *"it"* refers to what it is supposed to refer to.

Examples...

In the following definition *"it"* refers to the system of linear equations, the subject of the sentence.

> A system of linear equations is consistent if it has a solution and inconsistent if it doesn't.

5. "A" and "The"

If V is a non-zero vector space it has infinitely many bases so one cannot speak of *"the basis"* for a vector space unless it is clear from the context which basis is being referred to. That is why we say *"a basis"* in the definition of dimension.

> The dimension of a vector space is the number of elements in a basis for it.

The definition

> The dimension of a vector space is the number of elements in the basis for it.

is wrong because it suggests, incorrectly, that there is only one basis for a vector space.

6. If and only if

CHAPTER 18

Applications of linear algebra and vector spaces

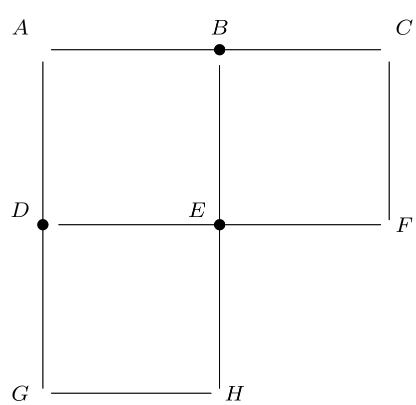
There are so many applications of linear algebra and vector spaces that many volumes are needed to do justice to the title of this chapter. Linear algebra and vector spaces are embedded deep in the heart of modern technology and the modern world.

1. Simple electrical circuits

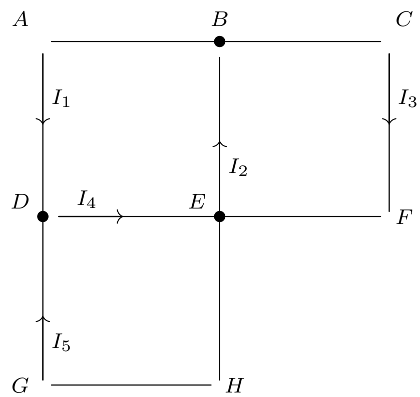
The flow of current in a simple electrical circuit consisting of batteries and resistors is governed by three laws:

- **Kirchoff's First Law** The sum of the currents flowing into a node is equal to the sum of the currents flowing out of it.
- **Kirchoff's Second Law** The sum of the voltage drops around a closed loop is equal to the total voltage in the loop.
- **Ohm's Law** The voltage drop across a resistor is the product of the current and the resistor.

To make apply these we must first draw a picture of the circuit. To simplify I will begin by leaving out the resistors and batteries. A typical circuit might look like this:



There are three loops and three nodes in this circuit. We must put arrows on each loop indicating the direction the current is flowing. It doesn't matter how we label these currents, or the direction we choose for the current flowing around each loop.



Applying Kirchoff's First Law at the nodes B, D, and E, we deduce that

$$\begin{aligned} I_1 + I_3 &= I_2 \\ I_1 + I_5 &= I_4 \\ I_2 + I_5 &= I_3 + I_4. \end{aligned}$$

I am going to refer you to the book for more on this because I can't draw the diagrams!

2. Magic squares

You have probably seen the following example of a magic square:

4	3	8
9	5	1
2	7	6

The numbers in each row, column, and diagonal add up to 15. Let's look at this from the point of view of linear algebra and learn a little about this magic square and then try to construct some larger ones.

Let's call any $n \times n$ matrix with the property that the numbers in each row, column, and diagonal add up to the same number, σ say, a σ-valued magic square. We will call σ the magic value. We will write

$$MS_n(\sigma)$$

for the set of σ-valued magic squares. If the numbers in the matrix are $1, 2, \ldots, n^2$ we will call it a classical magic square.

The sum of all integers from 1 to n^2 is $\frac{1}{2}n^2(n^2+1)$, so in a classical $n \times n$ magic square the sum of the numbers in a row is $\frac{1}{2}n(n^2+1)$. For example when $n = 3$, the magic value is 15. When $n = 4$ it is 34.

The $n \times n$ matrix with every entry equal to 1 is an n-valued magic square. We will write E_n for this matrix or just E if the n is clear. Although this will not strike you as a particularly interesting n-valued magic square it will play a useful role in showing that it an appropriate system of linear equations is consistent – it will be a solution to them—and in reducing the problem from to a system of *homogenous* linear equations.

The set of all $n \times n$ matrices forms a vector space: we can add them and multiply by scalars and the properties in Proposition **??** hold. We usually write $M_n(\mathbb{R})$ for the set of all $n \times n$ matrices. The subset of 0-valued magic squares $MS_n(0)$ is a subspace of $M_n(\mathbb{R})$. The next lemma says that

$$MS_n(\sigma) = \tfrac{\sigma}{n}E + MS_n(0);$$

i.e., the set of σ-valued magic squares is a translation of the subspace $MS_n(0)$.

LEMMA 2.1. *Let A be an $n \times n$ matrix. Then A is a σ-valued magic square if and only if $A - \frac{\sigma}{n}E$ is a 0-valued magic square.*

For example, when $n = 3$,

$$\begin{pmatrix} 4 & 3 & 8 \\ 9 & 5 & 1 \\ 2 & 7 & 6 \end{pmatrix} - 5E = \begin{pmatrix} -1 & -2 & 3 \\ 4 & 0 & -4 \\ -3 & 2 & 1 \end{pmatrix}$$

is a 0-valued magic square.

We now consider the problem of finding all 0-valued 3×3 magic squares. We will write x_{ij} for the unknown value of the ij^{th} entry. For example, the fact that sum of the top row of the matrix must be zero gives us the equation $x_{11} + x_{12} + x_{13} = 0$. And so on. Doing the obvious thing we get a total of 8 homogeneous equations in 9 unknowns—3 equations from the rows, 3 from the columns, and 2 from the diagonals. By Proposition **??** a system of homogeneous equations always has a non-trivial solution when the number of rows is strictly smaller than the number of unknowns. Hence there is a non-trivial 3×3 0-valued magic square.

Before we can write down the coefficient matrix for the system of equations we must agree on an ordering for the unknowns. We will just use the naive ordering and write them in the order

$$x_{11},\ x_{12},\ x_{13},\ x_{21},\ x_{22},\ x_{23},\ x_{31},\ x_{32},\ x_{33}.$$

The coefficient matrix is

$$\begin{array}{cc} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} & \begin{array}{c} \text{main diagonal} \\ \text{column 2} \\ \text{column 3} \\ \text{column 1} \\ \text{row 2} \\ \text{row 1} \\ \text{anti-diagonal} \\ \text{row 3} \end{array} \end{array}$$

I don't want to present all the row operations in gory detail, but we can progressively obtain the equivalent matrices

$$\begin{pmatrix}1&0&0&0&1&0&0&0&1\\0&1&0&0&1&0&0&1&0\\0&0&1&0&0&1&0&0&1\\0&0&0&1&-1&0&1&0&-1\\0&0&0&0&1&-1&1&0&-1\\0&0&0&0&0&0&0&0&0\\0&0&0&0&-2&-1&0&-1&-2\\0&0&0&0&0&0&1&1&1\end{pmatrix}\qquad\begin{array}{c}\text{MD}\\\text{C2}\\\text{C3}\\\text{C1-MD}\\\text{AD-C3}\\\text{R2+R1+R3-C1-C2-C3}\\\text{R1-MD-C2-C3}\\\text{row 3}\end{array}$$

then

$$\begin{pmatrix}1&0&0&0&1&0&0&0&1\\0&1&0&0&1&0&0&1&0\\0&0&1&0&0&1&0&0&1\\0&0&0&1&-1&0&1&0&-1\\0&0&0&0&1&-1&1&0&-1\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&-3&2&-1&-4\\0&0&0&0&0&0&1&1&1\end{pmatrix}\qquad\begin{array}{c}\text{MD}\\\text{C2}\\\text{C3}\\\text{C1-MD}\\\text{AD-C3}\\\text{R2+R1+R3-C1-C2-C3}\\\text{R1-MD-C2-3C3+2AD}\\\text{row 3}\end{array}$$

We can already see from this that x_{32} and x_{33} will be the independent variables, so let's take

$$x_{33} = 1, \quad x_{32} = 2.$$

Evaluating the dependent variables gives

$$x_{31} = -3,\ x_{23} = -4,\ x_{22} = 0,\ x_{21} = 4,\ x_{13} = 3,\ x_{12} = -2,\ x_{11} = -1,$$

which is the 0-valued magic square we obtained before.

The rank of the matrix is 8-1=7, so its nullity is 2. That is equivalent to the existence of two independent variables, so let's find another solution that together with the first will give us a basis. It is obvious though that a 3×3 matrix has various symmetries that we can exploit.

For the $n \times n$ case we get a homogeneous system of $2n + 2$ equations in n^2 variables. If $n > 2$ this system has a non-trivial solution.

CHAPTER 19

Last rites

1. A summary of notation

Sets are usually denoted by upper case letters.

$f : X \to Y$ denotes a function f from a set X to a set Y. If $f : X \to Y$ and $g : Y \to Z$ are functions, then $g \circ f$ or gf denotes the composition *first do f then do g*. Thus $gf : X \to Z$ and is defined by

$$(gf)(x) = g(f(x)).$$

This makes sense because $f(x)$ is an element of Y so g can be applied to it.

The identity function $\mathrm{id}_X : X \to X$ is defined by

$$\mathrm{id}_X(x) = x \qquad \text{for all } x \in X.$$

If $f : X \to Y$ and $g : Y \to X$ are such that $gf = \mathrm{id}_X$ and $fg = \mathrm{id}_Y$ we call g the inverse of f and denote it by f^{-1}. Of course, if $g = f^{-1}$, then $f = g^{-1}$.

We denote the range of a function $f : X \to Y$ by $\mathcal{R}(f)$. Thus, $\mathcal{R}(f) = \{f(x) \mid x \in X\}$. It is a subset of Y.

If A is an $m \times n$ matrix we often write $\underline{A}_1, \ldots, \underline{A}_n$ for the columns of A and

$$A = [\underline{A}_1, \ldots, \underline{A}_n]$$

to indicate this. This notation usually appears when we want to make use of the fact that

$$BA = B[\underline{A}_1, \ldots, \underline{A}_n] = [B\underline{A}_1, \ldots, B\underline{A}_n],$$

i.e., the j^{th} column of BA is B times the j^{th} column of A.

We write $\underline{e}_j$ for the element in $\mathbb{R}^n$ having zeroes in all positions except the j^{th} which is 1. Thus, the identity matrix is $I = [\underline{e}_1, \ldots, \underline{e}_n]$. More generally, if A is any $m \times n$ matrix, then $A\underline{e}_j = \underline{A}_j$, the j^{th} column of A. You can see this either by computation or using the fact that $AI = A$.

If $\underline{x}_1, \ldots, \underline{x}_n$ are vectors, then $\mathbb{R}\underline{x}_1 + \cdots + \mathbb{R}\underline{x}_n$ is synonymous with $\mathrm{Sp}(\underline{x}_1, \ldots, \underline{x}_n)$. It denotes the set of all linear combinations of the vectors $\underline{x}_1, \ldots, \underline{x}_n$.

The λ-eigenspace is denoted by E_λ. If it is necessary to name the matrix for which it is the eigenspace we write $E_\lambda(A)$.

2. A sermon

Learning a new part of mathematics is like learning other things: photography, cooking, riding a bike, playing chess, listening to music, playing music, tennis, tasting wine, archery, seeing different kinds of art, etc. At some point one does, or does not, make the transition to a deeper involvement where one internalizes and makes automatic the steps that are first learned by rote. At some point one does, or does not, integrate the separate discrete aspects of the activity into a whole.

You will know whether you are undergoing this transition or not. It may be happening slowly, more slowly than you want, but it is either happening or not. Be sensitive to whether it is happening. Most importantly, ask yourself whether you want it to happen and, if you do, how much work you want to do to make it happen. It will not happen without your active involvement.

Can you make fluent sentences about linear algebra? Can you formulate the questions you need to ask in order to increase your understanding? Without this internalization and integration you will feel more and more like a juggler with too many balls in the air. Each new definition, concept, idea, is one more ball to keep in the air. It soon becomes impossible unless one sees the landscape of the subject as a single entity into which the separate pieces fit together neatly and sensibly.

Linear algebra will remain a great struggle if this transition is not happening. A sense of mastery will elude you. Its opposite, a sense that the subject is beyond you, will take root—paralysis and fear will set in. That is the dark side of all areas of life that involve some degree of competence, public performance, evaluation by others, and consequences that you care about.

Very few people, perhaps none, get an A in 300- and higher-level math courses unless they can integrate the separate parts into a whole in which the individual pieces not only make sense but seem inevitable and natural.

It is you, and only you, who will determine whether you understand linear algebra. It is not easy.

Good luck!