

Intuitive Linear Algebra:

A Gateway to Bright Horizons

Kevin Powell, Ph.D.

September 20, 2024 Draft

An Introductory Text in Linear Algebra

What we see depends on how we see.

©2023 by Kevin Powell

All rights reserved. This book may only be downloaded in the digital format and reproduced for *personal* study or for an *individual instructor*'s class activities. All other reproductions, distributions, or transmissions of any portion of this book by any means without prior written permission of Kevin Powell are strictly prohibited, except in the case of brief quotations for noncommercial uses as permitted by copyright law.

Direct all inquiries to Kevin Powell by email at:

kevin.powell@snow.edu

This is the Digital Ebook Format

Paperback ISBN:

I strongly feel that Heavenly Father has guided my steps while writing this book.

My first dedication is to Him.

I also dedicate this book to my incredible wife, my loving parents, and my nine amazing children.

Contents

Preface	14
Note From the Author	17
How to Read a Math Book	18
I Matrices As Functions	19
1 Getting Ready	21
1.1 Writing Proofs	22
1.1.1 Covering All Cases and Definition Matching	22
1.1.2 Using Counterexamples	24
1.1.3 Finding Contradictions	25
1.1.4 Using Induction	26
1.1.5 Logical Equivalence	28
1.1.6 Exercises	32
1.1.7 Solutions	34
1.2 Sets, Functions, and Fibers	38
1.2.1 Sets and Subsets	38
1.2.2 Basic Set Operations	41
1.2.3 Defining Functions	43
1.2.4 Mapping Subsets to Subsets	45
1.2.5 Injectivity, Surjectivity, Bijectivity	50

1.2.6	Exercises	58
1.2.7	Solutions	61
1.3	Set Products, Compositions and Inverses	64
1.3.1	Cartesian Products	64
1.3.2	Less Important Side Notes (optional)	66
1.3.3	Composition Diagrams	66
1.3.4	Surjective Maps, the Identity Function, and Right Inverses	69
1.3.5	Injective Maps, and Left Inverses	71
1.3.6	Exercises	76
1.3.7	Solutions	78
1.4	Additive Structure on Sets and Functions	80
1.4.1	Set Addition	80
1.4.2	Groups	82
1.4.3	Additive Functions	85
1.4.4	Exercises	92
1.4.5	Solutions	94
	Chapter 1 Selected Review Questions	96
2	Linear Transformations	103
2.1	Vector Spaces and Their Subspaces	104
2.1.1	Fields of Scalars	105
2.1.2	Vector Spaces	106
2.1.3	Subspaces and Spans	108
2.1.4	Quotient Vector Spaces	114
2.1.5	Function Vector Spaces	116
2.1.6	Rings and Modules	117
2.1.7	Exercises	121
2.1.8	Solutions	124
2.2	Linear Independence and Bases	128
2.2.1	Linear Independence	128
2.2.2	More on Bases	132
2.2.3	Free Rank and Existence of a Basis	136
2.2.4	Exercises	139
2.2.5	Solutions	142
2.3	Matrix Functions: Linear Transformations	147
2.3.1	Linear Transformations	147
2.3.2	Matrices are Just Functions of Column Vectors	149
2.3.3	Matrices are Functions of Row Vectors	154
2.3.4	Matrix Multiplication From a Column Interpretation	156
2.3.5	Matrix Multiplication From a Row Interpretation	158

2.3.6	Fast Matrix Squaring	161
2.3.7	Exercises	167
2.3.8	Solutions	171
2.4	Matrix Block Multiplication	174
2.4.1	Column-Row Partition Blocks for Multiplication	174
2.4.2	Mixing Column-Row Partitions with Row-Column Partitions	177
2.4.3	Block Diagonal Matrices	182
2.4.4	The Standard Definition of Matrix Multiplication	185
2.4.5	Exercises	189
2.4.6	Solutions	193
	Chapter 2 Selected Review Questions	196
3	Linear Transformation Examples	203
3.1	Rotating and Stretching the Plane	204
3.1.1	Building Matrices for Plane Transformations	204
3.1.2	The Equation of a Transformed Graph	206
3.1.3	Exercises	209
3.1.4	Solutions	213
3.2	Derivatives as Matrices	216
3.2.1	Graphing Shifts of Linear Transformations	216
3.2.2	Derivatives	218
3.2.3	Chain Rule	225
3.2.4	Machine Learning	226
3.2.5	Exercises	231
3.2.6	Solutions	238
3.3	Recursive Sequences	243
3.3.1	Exercises	247
3.3.2	Solutions	249
3.4	Matrices for Digraphs	251
3.4.1	Adjacency Matrices	251
3.4.2	Incidence Matrices	256
3.4.3	Stochastic Matrices	259
3.4.4	Exercises	263
3.4.5	Solutions	267
	Chapter 3 Selected Review Questions	271
4	Smith Normal Form	275
4.1	Isomorphic Views of Matrices	276
4.1.1	Isomorphisms and What They Do	276
4.1.2	Some Simple Isomorphisms	280

4.1.3	Smith Normal Form	285
4.1.4	Finding Matrices for the Row and Column Isomorphisms	292
4.1.5	Using Smith Normal Form to Check Linear Independence	297
4.1.6	Exercises	303
4.1.7	Solutions	313
4.2	Reduced Row Echelon Form	325
4.2.1	Reduced Row Echelon Form and Bases	325
4.2.2	Solving Systems of Equations	331
4.2.3	Shortcut to the Kernel by Columns	336
4.2.4	Independent and Inconsistent Systems	339
4.2.5	Solving Systems with the Row Operations Matrix	341
4.2.6	Exercises	346
4.2.7	Solutions	352
4.3	Inverses	359
4.3.1	Right Inverses	359
4.3.2	Left Inverses	364
4.3.3	Inverses	367
4.3.4	Exercises	371
4.3.5	Solutions	373
4.4	Changing Bases	375
4.4.1	Different Coordinate Axes: Change of Base	375
4.4.2	Expressing a Linear Transformation in Skewed Coordinates.	379
4.4.3	Expressing a Skewed Transformation in Standard Coordinates	380
4.4.4	Writing a Transformation in Terms of Ambient (Outside) Coordinates.	382
4.4.5	Relabeling Transformations	384
4.4.6	Different Bases from Input to Output	386
4.4.7	Exercises	391
4.4.8	Solutions	400
4.5	Topology of Graphs and Surfaces	409
4.5.1	Connected Components of a Digraph	410
4.5.2	Cell Complexes and Boundaries	413
4.5.3	Interlude on Gluing Diagrams	418
4.5.4	Equivalent Paths	425
4.5.5	Exercises	436
4.5.6	Solutions	443
Chapter 4 Selected Review Questions		447

II The Symmetries of Matrices 457

5 Projections	459
5.1 Transposes, Symmetric Matrices, and Lengths	460
5.1.1 Matrix Transposes	461
5.1.2 Notation and Terminology for Row Vectors (Duals)	463
5.1.3 Symmetric Matrices	464
5.1.4 Projection Length	465
5.1.5 Orthogonality	470
5.1.6 The Laplacian Symmetric Matrix (Optional)	472
5.1.7 Exercises	479
5.1.8 Solutions	483
5.2 Projections via Right and Left Inverses	488
5.2.1 Decomposing the Domain of a Surjective Linear Transformation	488
5.2.2 Making a Left/Right Inverse Pair for Projections	493
5.2.3 Orthogonal Projections	500
5.2.4 Exercises	507
5.2.5 Solutions	512
5.3 Gram-Schmidt Orthogonalization	515
5.3.1 Orthogonal Right Inverses	515
5.3.2 Iterative Procedure using Matrices	518
5.3.3 Iterative Procedure Using Dot Product	523
5.3.4 Orthonormal Bases	525
5.3.5 QR Decomposition	526
5.3.6 LQ Decomposition	533
5.3.7 Exercises	538
5.3.8 Solutions	541
5.4 Least Squares	544
5.4.1 Orthogonal Right Inverse gives Closest Solution	544
5.4.2 Two Examples	546
5.4.3 Intuition For Best Fit Line	549
5.4.4 Fitting to other Curves	550
5.4.5 Using Calculus to Prove Minimality (Optional)	553
5.4.6 Exercises	556
5.4.7 Solutions	558
Chapter 5 Selected Review Questions	561
6 Determinants	565
6.1 Permutation Arithmetic	566
6.1.1 Pictures of Permutations	566

6.1.2	Composition of Permutations	569
6.1.3	Even and Odd Permutations	570
6.1.4	Symmetric Groups: Half Even, Half Odd	575
6.1.5	Exercises	579
6.1.6	Solutions	581
6.2	Determinants via Permutations and Sliding	582
6.2.1	Partitioning the Permutations with an Example	589
6.2.2	Generalizing to other Permutation Partitions	595
6.2.3	Using Cosets of Smaller Subgroups	597
6.2.4	Airdropping and Cofactor Techniques	602
6.2.5	Matrix Multiplication and Determinants	603
6.2.6	Diagonal Blocks and Determinants	607
6.2.7	Exercises	612
6.2.8	Solutions	618
6.3	Inverses, Cramer's Rule, and Singular Matrices	620
6.3.1	Inverses by Cofactors	620
6.3.2	Cramer's Rule	623
6.3.3	Singular and Nonsingular Matrices	625
6.3.4	Exercises	629
6.3.5	Solutions	633
6.4	Multilinear Functions	637
6.4.1	Determinants are Multilinear	638
6.4.2	Bilinear Transformations	640
6.4.3	Trilinear Transformations	642
6.4.4	Bilinear Transformations by Tensors	646
6.4.5	Fast Evaluation of Bilinear Transformations	650
6.4.6	Derivatives as Multilinear Forms	652
6.4.7	More Examples via Wedge Product	662
6.4.8	Determinants by Wedges and Properties of Wedges	664
6.4.9	Exercises	672
6.4.10	Solutions	679
6.5	Cofactor and Wedge Intuition	685
6.5.1	Area of a Parallelogram is a Linear Transformation	685
6.5.2	Intuition for the Volume of a Parallelepiped	692
6.5.3	The Cross Product	695
6.5.4	Wedge Products on Surfaces	701
6.5.5	Surface Area	704
6.5.6	Changing Coordinates	708
6.5.7	Stoke's Theorem via Wedges	713
6.5.8	Exercises	725

6.5.9	Solutions	730
Chapter 6 Selected Review Questions		734
7	Matrices as Scalars	741
7.1	Matrix Scalars and Zero Scalars	742
7.1.1	A Scalar as a Matrix	743
7.1.2	Representations of the Zero Matrix	745
7.1.3	Polynomial Scalars That Act Like Zero	747
7.1.4	Generalized Synthetic Division	750
7.1.5	Counting Paths	755
7.1.6	Recursive Sequences	757
7.1.7	Exercises	763
7.1.8	Solutions	770
7.2	Characteristic Polynomial by Central Submatrices	776
7.2.1	Finding Coefficients	776
7.2.2	Relating Characteristic Polynomials	783
7.2.3	Studying the Orthonormal Columns	791
7.2.4	An Optional Calculus Proof	796
7.2.5	Counting Spanning Trees	800
7.2.6	Trace and Similarity	806
7.2.7	An Extra Group Map Example	813
7.2.8	Conjugacy and Similarity	816
7.2.9	Exercises	821
7.2.10	Solutions	825
7.3	The Minimal Polynomial	827
7.3.1	Proof That The Minimal Polynomial Exists	828
7.3.2	Finding a Diagonal Polynomial Matrix	831
7.3.3	Polynomial Spans	834
7.3.4	Invariant Subspaces	840
7.3.5	The Minimal Polynomial from Row and Column Operations	844
7.3.6	Comparing the Minimal and Characteristic Polynomials	848
7.3.7	Just Using Column Operations	849
7.3.8	Invariant Subspaces Along the Way	850
7.3.9	Computing the Minimal Polynomial via Trial and Error	851
7.3.10	When the Characteristic and Minimal Polynomials are the Same	853
7.3.11	Technology Exploration	855
7.3.12	Nilpotents, Zero Divisors, and Idempotents	855
7.3.13	Exercises	862
7.3.14	Solutions	867
7.4	Diagonalization of Matrices	873

7.4.1	Eigenvectors Help Diagonalize	873
7.4.2	Exploring Why We Could Find Enough Eigenvectors	876
7.4.3	Eigenvectors in $\mathbb{R}[x] \cdot v$	879
7.4.4	Minimal Polynomials and Diagonalizability	882
7.4.5	Proof of Diagonalization By Ranges and Kernels	884
7.4.6	Finding Eigenvectors by Ranges	887
7.4.7	Finding Eigenvectors by Kernels	892
7.4.8	Powers of a matrix	895
7.4.9	Diagonalizing by Roots	896
7.4.10	Exercises	901
7.4.11	Solutions	905
7.5	Symmetric Matrices and Applications	910
7.5.1	Symmetric Matrices are Diagonalizable	911
7.5.2	Orthogonality Between Eigenspaces	915
7.5.3	Orthogonal Diagonalization Reveals Rotations	919
7.5.4	Positive Definite Symmetric Matrices	923
7.5.5	Optimization	926
7.5.6	Finding the Center of a Rotated Ellipse	929
7.5.7	Diagonalizing a Trilinear Form	931
7.5.8	Revisiting Least Squares with a Pseudo Inverse	934
7.5.9	Exercises	944
7.5.10	Solutions	948
7.6	Inner Products	956
7.6.1	Inner Products from Positive Definite Symmetric Matrices	957
7.6.2	Hermitian Inner Product	958
7.6.3	An Integral Inner Product	961
7.6.4	Orthonormal Bases	963
7.6.5	Introduction to Fourier Series	964
7.6.6	Fourier Series Example and π	972
7.6.7	Gram-Schmidt and Polynomials	973
7.6.8	Exercises	979
7.6.9	Solutions	983
	Chapter 7 Selected Review Questions	986

III Number Theory and Other Applications of Linear Algebra 997

8	Differential Equations and More on Rotations	999
8.1	Differential Equations	1000
8.1.1	Exercises	1009

8.1.2	Solutions	1010
8.2	Quaternion Rotations	1011
8.2.1	Introduction to Quaternions	1011
8.2.2	Rotations	1015
8.2.3	Specific Rotation Computations	1020
8.2.4	Euler's Theorem (Proof)	1024
8.2.5	Exercises	1029
8.2.6	Solutions	1030
9	Number Theory	1031
9.1	Matrices in Modular Arithmetic	1032
9.1.1	\mathbb{Z} -modules	1033
9.1.2	Chinese Remainder Theorem	1044
9.1.3	Arithmetic With Bar Notation	1057
9.1.4	Classifying \mathbb{Z} -modules	1058
9.1.5	Multiplicative Groups and Exponents	1060
9.1.6	Exercises	1071
9.1.7	Solutions	1073
9.2	Field Extensions and Galois Groups	1075
9.2.1	Algebraic Field Extensions	1077
9.2.2	Proving the Fundamental Theorem of Algebra	1092
9.2.3	Examples: Matrix Diagonalization to Compute Galois Groups	1094
9.2.4	Cyclotomic Polynomials	1105
9.2.5	A Linear Transformation that Counts what is Primitive	1108
9.2.6	Exercises	1116
9.2.7	Solutions	1117
9.3	Factorization of Integers Using Field Extensions	1118
9.3.1	A Bilinear Map and Rings of Integers.	1119
9.3.2	How to Find Factors in \mathcal{O}_K	1129
9.3.3	Factorization into Ideals	1134
9.3.4	More on Repetitions in Ideal Factorization.	1146
9.3.5	Quadratic Reciprocity	1148
9.3.6	Sums of Squares	1152
9.3.7	Using Squares in Modular Arithmetic to Factor Large Numbers	1156
9.3.8	General Number Field Sieve	1161
Bibliography	1176
Index	1178

Preface

With the only prerequisite being a first semester calculus course, this book offers an exciting approach to linear algebra and stretches the reader in ways that most such introductory texts would not even consider. Even though there are some allusions to second and third semester calculus courses, it is assumed that most readers have no familiarity with them. *Any topics that assume too much are considered as optional.*

This book is an experiment to help make matrix and linear algebra computations more intuitive. Most all of the exercises in this text are intended to be done by hand! The problems have simple numbers so that they are not an obstacle to developing the necessary intuition.

In the book I use the word "we" instead of "I" even though I am just one person. I follow this convention, however, to include the reader so that "we" refers both of us—the reader and me. I hope this small detail makes the book more inviting.

The first part of the book goes through functions, matrices, inverses, Smith normal form and solving equations. *This is the first part of a one semester introductory course in linear algebra.*



The reader will notice video links given by and SageMath activity links given by . The resources through these links and my website at <https://www.kevindowell.rf.gd/> will help the reader both better understand and explore the content in the book.

To help the reader actually read the textbook, I have a section on proof writing upfront. *How can we have proper intuition when we do not even know where something comes from nor why nor how it works?*

I show the reader that matrices are really just functions. To develop further intuition for functions, we look at what I call "fiber box diagrams." I whittle common lists of axioms down to bite-size chunks. Linear transformations are additive and scalable functions between vector spaces. Vector spaces are additive groups with an outside scalar action.

Early on, I present many applications of functions represented by matrices and how to build them. Specifically, the book looks at 2×2 rotations of matrices by considering the images of e_1 and e_2 . Also, we look at applications of matrices to graph theory, sequences, and calculus.

Instead of starting with systems of equations and discussing Gaussian elimination, I go right to Smith normal form (over \mathbb{R}). The reader comes to realize that column operations are like bijective linear transformations

(i.e. isomorphisms) applied *before* the matrix function and row operations are like isomorphisms *after* the function. We can get valuable information about the dimension of the range and the null space (i.e. kernel) of the matrix. In this book I use the word “kernel” much more often than null space. I coin the term “airdropping” to mean “add a multiple of a row to another.”

The book uses the Smith normal form process as a valuable tool for solving systems of equations. The solution is viewed as a fiber of a function which itself is a shift of the kernel. The book gives a fast column technique for determining a basis for the kernel of a matrix.

The parts of Smith Normal form can be used to find left or right matrix inverses. I keep the reader using such processes for a while to develop greater skill. In chapter 6, I introduce other techniques for finding matrix inverses. But in the mean time, the reader will learn about change of basis through the notions of “pretending” and “unpretending” matrices.

At the end of chapter 4, I give the interested reader a taste of topology with cellular complexes explored through Smith normal forms. The linear algebra learned thus far gives valuable geometric information about a surface.

Part II goes over projections, determinants, diagonalization of matrices and more. *This is the second part of a one semester introductory course in linear algebra.*

Chapter 5 takes us through different types of vector projections using things like “shadow vectors” and “light ray vectors” that we can obtain by studying a pair of functions f, g so that g is a right inverse to f . This naturally flows to a nice iterative matrix procedure for Gram Schmidt and finding least square approximations.

In chapter 6, a study of permutations leads us to determinants. In addition to standard cofactor expansions, we also look at how we can use 6 pairs of 2×2 submatrices to compute the determinant of a 4×4 matrix. The book turns to multilinear functions and fun applications of them.

In chapter 7, we think about a matrix acting in two ways: as a matrix function and as a scalar x . Assuming these actions are the same leads to a lot of fun with polynomials, generalized synthetic division, powers of matrices, and more. Diagonalization of matrices is considered in a very “polynomial way.” We study the coefficients of the characteristic polynomial and look at procedures for computing the minimal polynomial. Some applications include the optimization of multivariable functions and determining rotation angles of conics. Additionally, we dive into inner products and even look at Fourier series.

Part III is completely extra and *should not be part of a first semester of linear algebra except for additional study, reading, projects, or exploration.*

After sections on differential equations and quaternions, the book turns to number theory. This is because I think that an introduction to \mathbb{Z} -modules and field extensions can very well be done with a *linear algebra core*.

The chapter on number theory is an *experiment* to see if we can use a linear algebra focus to make topics in algebraic number theory *intuitive and understandable for more people*.

So my experiment continues! We begin with cosets inside of \mathbb{Z}^2 . Systems of congruences and the Euclidean algorithm come from the Smith normal form process. The book goes into field extensions, Galois theory, and even the General Number Field Sieve.

I hope the reader finds something enjoyable and enlightening as I have in these pages.

Note From the Author

Why do people study music? Why do people paint pictures? Why do people like to hike to the top of mountain peaks? But why do people study math? Is there any correlation between the answers to these questions. Unfortunately, there is not as much correlation as there should be.

To me, it is just as valuable to study an art or music or go exploring as it is to explore mathematics. It is a music of the soul with just as much expression as anything else has.

But how is it not generally seen this way? At the beginning, elementary school students are eager to learn about their world and every aspect of it—*including mathematics*. But how does the excitement fade as children grow older? I believe that one reason is that, in school, mathematics is taught as a means to an end. It is stream-lined and made into a hard stiff grammar. The *art* is taken out of it. It is nothing more than objectives to accomplish instead of a means of expression. We objectify it into a plain, nonliving object. Why? *Because it is so useful, we focus too much on its utility*. We demand that certain tasks should be perfected. There is no time to appreciate various ways of seeing the same thing.

Yet, the very art of mathematics is finding the perspective that captures the greatest logical beauty just like a photographer searches for the best angle from which to snap a picture. The irony is that *more is accomplished* by exploring various perspectives than just trying to take lots of snap shots as a book tells us to do. Yet in math that is what we do—we follow the rules delineated in a book instead of just getting out into the open and enjoying and appreciating what we see from various angles.

More is accomplished, more is understood, more is appreciated and we can do more *in applications too* than we could by trying to go through a list of objective tasks.

In this book, I hope to open the reader's eyes a little more to some of the angles from which they can view both things they may have seen before and things they may have never seen before. What we see, including how to solve a challenging problem, is often a result of the perspective we take. *What we see depends on how we see it.*

“How can I keep from singing?”

—American Folk Song

How to Read a Math Book

The best way to read a mathematics book is to *treat it* as art. That is, try to catch the vision of what is happening and then close your eyes and feel it—*recreate it in your own way*. Feel the music. Do not waste time trying to follow all of the details that I write. Rather, find the thoughts and details that you *do* understand. Then, ask yourself: “how would *I* fill in the gaps?” or “what would I need to know in order to fill in the details?” If it is hard to answer these, you can do two things: go forward or go backward. Just do not stay put. Often by reading a little further, the right connection is made that allows you to see how the gap could be filled. Sometimes just pondering on something already read, experimenting with it and viewing it from various angles can help too. But whatever you, *do not get stuck! Keep moving in some direction.*

A healthy dose of confusion is good. Don’t be deterred. It is a compelling force that leads us to action: “what part of this is making me confused? I would not be confused on this point if I saw or understood what? What do I understand already about this? Is there any way this can relate to what I already understand? What clues do I have? What are some various ways I can look at and view those clues?” Keep going. By allowing a little confusion, we allow ourselves to familiarize ourselves with *the art of mathematics: the art of looking at things in different ways*. It compels us to press forward right into the exploration of various ideas and perspectives.

Sometimes crystal clear presentations such as those that can be found at our finger tips on our very informative technological devices can be mind numbing. We are not allowing our minds to explore. We are scared of anything that will require us to press through confusion. *Yet our ability to press through confusion is called intelligence.* By spoon feeding their students in just the way they like, teachers can inhibit some of their intellectual growth. Just because it is not popular, does not mean that it is not good. Do not be afraid to take a little time to ponder. *You will become more adept at the art—not just the information of mathematics.*

Part I

Matrices As Functions

Getting Ready

1

Writing Proofs

1.1

1.1.1 Covering All Cases and Definition Matching	22
1.1.2 Using Counterexamples	24
1.1.3 Finding Contradictions	25
1.1.4 Using Induction	26
1.1.5 Logical Equivalence	28
1.1.6 Exercises	32
1.1.7 Solutions	34

Questions to Guide Your Study:

- *What does it mean to write a proof?*
- *What do we need to be careful of when trying to prove something by looking at examples?*
- *What is definition matching and how does it relate to writing a proof?*
- *When is writing down a simple, single example considered a proof?*
- *What does it mean to prove something by contradiction?*
- *What is proof by induction and how does it work?*

Linear algebra is a wonderful network of ideas that fit together logically so well. In order to master these ideas, we need to master how we link them together. In other words, we need to be able to write proofs.

1.1.1 Covering All Cases and Definition Matching

When we prove something we need to be careful to cover all cases. For instance, if we want to show that all numbers of the form $3n + 6m$ are multiples of 3 where n and m are integers, we cannot just look at a few examples, see that they work, and then be done. Doing so is logically the same as looking in a lake, seeing only red fish, and then concluding that all fish are red. Something may be true in all the examples we see. But still there is no guarantee that the thing is true in all cases. In fact, usually it is impossible to verify every single example of something. So we need to get away from just looking at examples. We can sometimes use

examples to help us determine general ideas—but examples in and of themselves will not do if we want to show that all cases of something are true.

Make sure to consider every case (not all fish are red)

Let's go back to trying to show that all numbers of the form $3n + 6m$ are multiples of 3 where n and m are integers. We need to do this generally—letting n and m stay as variables where they have certain ideas attached to them. They are integers—and that is all! Here is what proving is then: it is *how to strategize with the general*. We use principles. We know that $3n + 6m$ is divisible by 3 if we can factor 3 out—which algebraically we can! We have: $3(n + 2m)$. We also know that since n and $2m$ are integers that $n + 2m$ is also an integer. Therefore, $3(n + 2m)$ is an integer multiple of 3. We have just written a proof.

Part of writing a proof is being precise and thorough. Even if we simply just think that something is obvious, and needs no words, it still can be done. It is challenging to write the obvious precisely.

Being adept with logical arguments is being able to write the obvious and even the not-so-obvious with precision and clarity.

Really, one of the most important parts of proof writing is the idea of *definition matching*.

Definition matching

The process of checking off boxes to see if A matches all the criteria given in the definition of B .

Often, we want to show that A is an example of B . All we do is go to the precise definition of what it means to be an example of B and then see if A matches that definition.

Really, proving is often just going through a definition and finding reasons to check off the boxes within that definition.

Example 1. For instance, suppose that we define a good tree as *any tall object that has leaves*. Then one could build a tall tower, decorate it with leaves and then check the boxes in the definition. The proof that the tall tower decorated in leaves is a tree would proceed as follows:

The tall tower is a tall object. The tall tower also has leaves on it. Therefore, by the definition of tree given, it is a tree.

Example 2. Let's define a set A to be all numbers that are divisible by 2 or 5. Are all multiples of 25 in that set? Let's write a proof that they are.

First, all multiples of 25 are divisible by 5 since 25 is divisible by 5. Hence, all multiples of 25 are divisible by 2 or 5 (the defining characteristic of being in A). Hence, all multiples of 25 are in A .



Example 3. Now, consider having a set B defined as being all integers x that are even and larger than 11 or odd and less than -10 . Now, write a proof that all numbers $(-1)^n(n - 2)$ where n is an integer so that $n > 20$ are in the set B .

Ok, here it goes: *Take a number of the form $(-1)^n(n - 2)$ where n is an integer so $n > 20$. We keep it general. But you can consider the expression $(-1)^n(n - 2)$ in two separate basic cases which cover all cases. That is, we get something a little different dependent on whether n is even or odd since $(-1)^n$ changes between $+1$ and -1 . So we consider them separately. When n is even, then the expression simplifies to $(n - 2)$ which again is even (the difference of two even numbers is even) and greater than 18 (since $n > 20$) which is definitely larger than 11. Hence, in the even case our numbers match the definition of the set B .*

Now, we just need to check the odd case. We get that $(-1)^n(n - 2) = -(n - 2) < -18$ and that $-(n - 2)$ is odd since an odd plus an even is always odd. Therefore, we match one of the criteria in the definition of being in the set B . All cases considered, the matter is closed. We have just proven that all these numbers are in the set B .

Really, writing a proof is a lot like being a lawyer in a court case. We study our definitions and we try to carefully match each point in the definition. We also make sure all our cases are covered. We need to understand what all the cases are. We need to understand our definitions thoroughly.

1.1.2 Using Counterexamples

What if we would like to prove that something is not always true? A proof would consist of simply finding just one **counterexample**. To know that not all fish are red, one simply just needs to find one that is another color.

Example 4. Suppose that we wish to verify that not all numbers of the form $n^4 - 1$ where n is an integer are divisible by 5. We perhaps notice at first that if $n = 1, 2, 3, 4$, then $n^4 - 1$ is divisible by 5. But we *just need one counterexample*. So here is the proof:

Suppose that $n = 0$, then $n^4 - 1 = -1$ which is not divisible by 5. Therefore, $n^4 - 1 = -1$ is not always divisible by 5.

Example 5. Suppose that we would like to disprove that all functions are continuous on their domains. We just need one counterexample. Here is a proof:

The function

$$f(x) = \begin{cases} 1 & x \leq 0 \\ -1 & x > 0 \end{cases}$$

has a jump discontinuity at $x = 0$. But $x = 0$ is in the domain of $f(x)$ since by the definition $f(0) = 1$. Therefore, not all functions are continuous on their domains.

1.1.3 Finding Contradictions

A very common proof writing technique is to find a problem with the opposite of what we want to be true. We call the problem a **contradiction**: it contradicts the idea that opposite would be true. Hence, the opposite itself must be false. If two ideas are truly **logical opposites**, then showing that one of them is false guarantees that the other is true.

For instance, let's suppose that we claim that a system of equations

$$\begin{aligned} 2x + y &= 4 \\ -2x - y &= 1 \end{aligned}$$

has no solution. Does what we desire to be true have a logical opposite? Indeed it does: *the system of equations has a solution.*

So, let's find a problem with this logically opposite idea! Finding this problem and writing the reasons behind finding it *is a proof*. We assume therefore that the system of equations has a solution and then see what happens when we run some tests or experiments. If an experiment gives us something we know is false, then the original assumption was bad. The false thing we find *is the contradiction*.

A mathematical or logical experiment is a lot nicer than one in a laboratory in that the results are *always reliable!* How do we perform such an experiment? *By just applying true principles and seeing where they take us logically.*

Example 6. Let's actually now do this and write out a proof for why the above system of equations has no solution.

Suppose that the above system of equations has a solution. Then, this means that there is a pair (x, y) that satisfies both equations at the same time. This means that the x and y values in both equations represent the same numbers. We also know that adding two true equations is again a true equation. If we add these two equations together, we can combine like terms, because the x and y variables represent the same numbers. But doing so results in the equation $0 = 5$ which is clearly a false statement. It is our contradiction. So what we assumed was false. This means the opposite of the assumption is true: the system of equations has no solution.

If we are trying to show that something is always true, the the logically opposite idea is that there exists at least one counterexample.

Let's use this counterexample thought in the next example. This is actually a really nice idea because it gives us somewhere to start: *assume that there is a counterexample and now find a problem with it.*



Example 7. Let's write a proof by contradiction for why an odd number plus an odd number is always even.

To assume the opposite is to say that there exists a counterexample. That is, there exists an odd number n and another odd number m such that their sum $n + m$ is odd. This means that $n + m = 2k + 1$ for some integer k . But we also know that $n = 2j + 1$ and $m = 2t + 1$ for some integers j and t since they are odd as well. Therefore,

$$\underbrace{2j+1}_{n} + \underbrace{2t+1}_{m} = 2k+1$$

$$2j+2t+2-2k=1$$

Notice that the number on the left side is even since we can factor a 2 out of it. The number on the right side 1 is odd. This is a contradiction since a number cannot be even and odd at the same time.

Note: this last example did not need to be proven by contradiction. Still, it is good practice to see how to formulate an argument by contradiction.

1.1.4 Using Induction

Suppose that we would like to prove that a list of ideas $I_1, I_2, I_3, I_4, \dots$ are all true at the same time. There is a nice technique which is often useful. If we can prove that the truth of one idea implies the truth of the next idea in the list, then all the ideas in the list would be true if the first idea itself were true. This leads us to the following:

Proof by Induction

If we would like to prove that $I_1, I_2, I_3, I_4, \dots$ are all true at the same time, just prove two things:

1. I_1 is true. (*Base Case*)
2. If I_n is true, then I_{n+1} is true. (*Induction Step*)

The assumption that I_n is true is called the **induction hypothesis** and considering if I_1 is true is called the **base case**. The base case does not need to occur at $n = 1$. It could happen at $n = 0$ or $n = -5$ or $n = 100$. Any integer value could be used as a base case depending on what we are trying to show and how things are labeled.

Trying to show that the induction hypothesis I_n implies that I_{n+1} is true is the heart of an induction argument. We use true principles and ideas to try to turn I_n into the statement representing I_{n+1} .



Example 8. Suppose that we wish to prove that the n th derivative of xe^x is $ne^x + xe^x$ for all $n \geq 1$.

We will attempt to prove this by induction. But wait! We need a list of ideas. Do you see the n appearing in the statement? This gives it to us: I_n is simply the statement that the n th derivative of xe^x is $ne^x + xe^x$. We want to show that all of I_1, I_2, I_3, \dots in this infinite list are true. So let's write a proof:

Let's first verify that I_1 is true. We take the first derivative of xe^x by using the product rule to verify that the derivative is $1 \cdot e^x + xe^x$ as desired.

So we only need to verify one more fact. Let's show that if I_n is true, then I_{n+1} must be true also. We try to turn I_n into the statement I_{n+1} by using true principles and ideas.

Start with the statement I_n which is that the n th derivative is $ne^x + xe^x$. To get to I_{n+1} , we just need to take one more derivative to have the $(n+1)$ st derivative. Using the product rule, we obtain:

$$ne^x + e^x + xe^x = (n+1)e^x + xe^x$$

which is precisely the statement I_{n+1} . We successfully deduced I_{n+1} from I_n so that the proof is complete.

Example 9. Let's use induction to prove that:

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

for all integers $n \geq 1$

First, let's prove the base case when $n = 1$. We do this by simply checking that the sum starting at 1 and ending at 1 (just 1 itself) is equal to $\frac{1 \cdot (1+1)}{2}$ which it is.

Next, we assume that the statement I_n is true:

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

and somehow use true ideas to turn it into the statement with n replaced by $n+1$:

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

Notice that to make I_n look a little more like I_{n+1} , it suffices to add $n+1$ to both sides of the equality since the left side would then be the same as the sum in I_{n+1} :

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

turns into:

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

Let's use algebra on the right side to try to turn it into $\frac{(n+1)(n+2)}{2}$. Why not factor out $(n + 1)$?

$$\frac{n(n+1)}{2} + (n+1) = \left(\frac{n}{2} + 1\right) \cdot (n+1) = \left(\frac{n+2}{2}\right) \cdot (n+1) = \frac{(n+1)(n+2)}{2}$$

and the proof is complete.

1.1.5 Logical Equivalence

if and only if

Often, the phrase *if and only if* appears in mathematical statements. Suppose we write: “ A is true if and only if B is true.” This means that A is true exactly when B is true and vice versa.

If the truth or falsity of A is the exact same as the truth or falsity of B , then we say that A and B are **logically equivalent**. We often use the phrase *if and only if* when writing definitions or equivalent statements.

Example 10. An integer n is defined to be even if and only if it can be written as $n = 2k$ for some integer k .

Example 11. An integer n is defined to be even if and only if it can be written as $n = 2k + 4$ for some integer k .

Notice that we have two different definitions for what it means for a number to be even. We used the phrase *if and only if*. These definitions are said to be **consistent** if and only if the statements after the *if and only if* themselves are logically equivalent. *Notice our use of “if and only if” in the definition of consistent!*

Proving Logical Equivalence

To prove that two ideas A and B are logically equivalent, it suffices to proceed as follows:

1. Prove that if A is true, then B is true.
2. Prove that if B is true, then A is true.



Example 12. Let's write a proof that the two definitions of being an even number are equivalent.

Let's first assume that an integer n can be written as $2k$ for some integer k . Now, let's try to show that it can be written as $n = 2j + 4$ for some integer j . Notice that we use another variable j . This is because we want to compare the two statements and there is nothing that says that the “ k ” used in both statements should be the same.

If we have assumed the first statement, then we have our value of k already. We know that $n = 2k$ and that k is determined. We then somehow use this fact to find a value of j that will work so that $n = 2j + 4$. This would show that the second statement is true. We would have shown that the first statement implies the second one.

The question is, can we find an integer j so that

$$2k = n = 2j + 4?$$

Let's try to find one: just solve for j and verify that it is an integer. Notice that

$$2k - 4 = 2j$$

and

$$k - 2 = j$$

which is definitely an integer. We have found the j value that guarantees that the second statement is true.

Now we need to show that if the second statement is true, then the first statement is true. That is, if we have determined j that makes the second statement true, then let's find the integer k that would make the first statement true. We just solve for k in:

$$2k = 2j + 4$$

$$k = j + 2$$

which again is an integer. We have just shown that the second statement implies the first and vice versa. Therefore, the two definitions are logically equivalent and therefore consistent.

Proving Equality of Sets

To prove that a set A is the same as a set B , we simply prove that the condition for being in set A is *logically equivalent* to the condition for being in set B . Often, we just take an arbitrary element x in A that satisfies the conditions of being in A and then show how it also satisfies the conditions of being in B . Then, we perform this argument with A and B swapped. *It is the same procedure as we have above for proving logical equivalence.*



Example 13. Suppose that we have a set A described by all integers of the form $5k + 2$ where k is an integer and we have another set B described by all integers of the form $5k - 3$ where k is an integer. To prove that set A is the same as set B , we simply take an element that matches the description of set A and show that it also matches the description of set B . Then we go the other way: we take an element that matches the description of set B and show that it matches the description of the set A .

Take an element in set A. It can be written as $5k+2$. Now, $5k+2$ can be written as $5k+5-3 = \underbrace{5(k+1)}_{\text{integer}} - 3$.

Hence, it matches the description of set B so is also in B.

Now take an element in set B. It can be written as $5k-3$. Now, $5k-3$ can be written as $5k-5+2 = \underbrace{5(k-1)}_{\text{integer}} + 3$. Hence, it matches the description of set A so is also in A. Therefore, both sets must be the same.

Key Concepts from this Section

- **definition matching:** (page 23) The process of checking off boxes to see if A matches all the criteria given in the definition of B .
- **counterexample:** (page 24) An example that shows that something is not always true.
- **contradiction:** (page 25) In a proof by contradiction, a *contradiction* is a false statement which logically follows from what we assume. It shows that what we assumed was false itself. The logically opposite statement from our assumption is therefore true.
- **logical opposites:** (page 25) Two statements are logical opposites if the truth of one implies the falsity of the other and vice versa.
- **proof by induction:** (page 26) If we would like to prove that $I_1, I_2, I_3, I_4, \dots$ are all true at the same time, just prove two things:
 1. I_1 is true. (*Base Case*)
 2. If I_n is true, then I_{n+1} is true. (*Induction Step*)
- **induction hypothesis:** (page 26) The induction hypothesis is the assumption that a statement at a particular position n in a list of statements is true. In an induction argument, we try to show that the induction hypothesis implies that the next statement at position $n+1$ is true.
- **base case:** (page 26) In an induction argument, the base case is the consideration of whether the first statement in a list of statements is true.
- **if and only if:** (page 28) Often, the phrase *if and only if* appears in mathematical statements. Suppose we write: “ A is true if and only if B is true.” This means that A is true exactly when B is true and vice versa.
- **logically equivalent:** (page 28) If the truth or falsity of A is the exact same as the truth or falsity of B , then we say that A and B are *logically equivalent*.
- **consistent:** (page 28) Two definitions are said to be consistent if and only if the statements after the *if and only if* are logically equivalent.
- **proving logical equivalence:** (page 28) To prove that two ideas A and B are logically equivalent, it suffices to proceed as follows:

1. Prove that if A is true, then B is true.
 2. Prove that if B is true, then A is true.
- **proving equality of sets:** (page 29) To prove that a set A is the same as a set B , we simply prove that the condition for being in set A is *logically equivalent* to the condition for being in set B . Often, we just take an arbitrary element x in A that satisfies the conditions of being in A and then show how it also satisfies the conditions of being in B . Then, we perform this argument with A and B swapped. *It is the same procedure as we have above for proving logical equivalence.*

1.1.6 Exercises

Cases and Definition Matching

1. Define the set D as the set of all integers x such that if x is even, it should be divisible by 3 and if it is odd, then it is divisible by 5. Prove that the set of all multiples of 15 is contained in D .
2. What is the logical fallacy here: “All mountains in Colorado have the mineral quartz. Therefore, all mountains have the mineral quartz.”
3. Suppose that we define an egg number to be one that is larger than 5 and is a multiple of 3. Suppose that A is the collection of all positive multiples of 9. Prove that every element of A is an egg number.
4. Prove that if we add a number which is one more than a multiple of 5 to another number that is one more than a multiple of 5, then the result will always be two more than a multiple of 5.

Using Counterexamples

5. Show that a number being a multiple of 6 does not mean that the number is a multiple of 12.
6. Prove that not every element of the form $5n + 7m$ where n and m are integers is a multiple of 12.

Finding Contradictions

7. Show that there do not exist numbers a and b such that

$$\begin{aligned} 2a + 3b &= 1 \\ 4a + 6b &= 1 \end{aligned}$$

8. Prove by contradiction that every positive integer has a prime factor. *Hint: Use the definition that a prime number is one whose only positive divisors are 1 and itself. Show that assuming the opposite leads to an infinite number of positive integers in a finite range. This will be your contradiction!*
9. Prove by contradiction that there are no integers x and y such that $18x + 2y = 1$.

- 10.** Prove by contradiction that $\sqrt{2}$ is a not rational number. Use the definition of a rational number as one that can be written as $\frac{a}{b}$ for two integers a and b . *Hint: you may even say the defintion of rational number assumes that $\frac{a}{b}$ is a reduced fraction. In the proof show that the assumption of $\sqrt{2} = \frac{a}{b}$ where $\frac{a}{b}$ is reduced will only lead problems in the end.*

Using Induction

- 11.** Prove by induction that every element of the following sequence is less than 5:

$$a_{n+1} = \sqrt{2a_n + 1} \quad a_0 = 2$$

- 12.** Prove by induction that every element of the form $4^n - 1$ where n is a positive integer is divisible by 3.

- 13.** Prove by induction that the following is divisible by 5 for all nonnegative integers n : $n^5 - n$ (Hint: you may use the fact that $(n + 1)^5 = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1$)

- 14.** Give a simple reason for why the result of the last exercise can be expanded to include all integers n .

- 15.** Prove by induction every nonnegative integer of the form $n(n + 1)(n + 2)$ is divisible by 3.

Proving Logical Equivalence

- 16.** Prove that the following two sets are the same. This is the same as proving that their defining characteristics are logically equivalent:

1. Set A is numbers of the form $3k + 1$ for some integer k .
2. Set B is numbers of the form $3j + 4$ for some integer j .

That is, show that n being written as $3k + 1$ for some integer k is logically equivalent to n being written as $3j + 4$ for some integer j .

- 17.** Prove that two definitions of being a positive number are logically equivalent:

1. The number n is positive if and only if there exists a real number m so that $n = 2^m$.
2. The number n is positive if and only if $n > 0$.

Hint: you might have to think about the range of $f(x) = 2^x$ for one direction and the domain of $\log_2(x)$ for the other direction. This exercise is to see if you can write a proof of logical equivalence.

1.1.7 Solutions

1. Use the idea of definition matching. What is it that we want to show? We want to show that all multiples of 15 are in D . That is, we want to show that all multiples of 15 follow the criteria of being in D . That is, every multiple of 15 must definition match to “an element of D .” There are two cases to consider: when the multiple of 15 is odd and when the multiple of 15 is even. When it is even, we go to the definition: “it is divisible by 3.” Now this definitely matches since any multiple of 15 is divisible by 3 since 15 is. Now we go to the next case when the multiple is odd: the definition we need to match is: “divisible by 5.” Again, this is definitely true since every multiple of 15 is divisible by 5 since 15 is. The cases even and odd cover everything. Therefore, we are done with the proof!
2. We have not checked all cases. We need the case of mountains in Colorado and the case of mountains outside Colorado.
3. Take an element of A and try to apply the conditions of what it means to be an egg number. An element of A is a multiple of 9 which is also a multiple of 3. But what about being greater than 5? We know that the elements of A are positive and multiples of 9. The smallest positive multiple of 9 is 9 itself which is greater than 5. Therefore, all the elements of A are egg numbers.
4. We need to do this generally to cover all cases! Arbitrarily just use the general notion that a number that is one more than a multiple of 5 can be written as $1 + 5k$ for some integer k . If we choose another number that is one more than a multiple of 5, we could write it as $1 + 5j$ for a possibly different integer j . Now, add $1 + 5k$ and $1 + 5j$ together to get:
$$1 + 5k + 1 + 5j = 2 + 5(k + j)$$
which is two more than a multiple of 5. Side note: If we use the definition that a number that is 2 more than a multiple of 5 is defined to be something of the form $2 + 5n$ for some integer n , then we could think of our conclusion as being drawn from definition matching.
5. This is a simple counterexample explanation: just use the example of 6 itself or 18 even. Just one counterexample is enough!
6. Just find one counterexample. Let $n = 1$ and $m = 0$ to get $5 \cdot 1 + 7 \cdot 0 = 5$ which is not a multiple of 12.
7. Assume the opposite and find a problem. That is, if both equations hold and are true equations, then adding

multiples of them to each other will give another true equation. But notice that adding the equations:

$$\begin{aligned} -2 \cdot (2a + 3b) &= 1 \\ 4a + 6b &= 1 \end{aligned}$$

yields

$$0 = -1$$

which is a false statement—it contradicts what we assumed. This means what we assumed was false and therefore we have proven that the nonexistence of such numbers a and b .

8. Suppose that there exists a number n that has no prime factor. This means in particular, that n is not prime, so it has a nontrivial positive factor that is not equal to n or 1. Say it is a . We then know that $a < n$. Now factors of a are factors of n . Our assumption that n has no prime factor consequently means that a has no prime factor either. So, a has a positive factor $b \neq 1$ such that $b < a$. Again, using the same reasoning, b has a positive factor c such that $1 < c < b$. This process continues forever. Do you see what this contradicts? We have an infinite strictly decreasing sequence of integers that starts at n and never actually makes it to 1. We are trying to fit an infinite number of integers between 1 and n . This is impossible. This is our contradiction!

9. If there were such integers x and y , then $9x + y = \frac{1}{2}$. But $9x + y$ is an integer and $\frac{1}{2}$ is not. This is a contradiction.

10. *There are many ways of finding a contradiction. This solution is just one possibility.* Assume that $\sqrt{2} = \frac{a}{b}$ where a and b are integers and they do not share any common factors. Then, $2 = \frac{a^2}{b^2}$ so that $\frac{2b^2}{a} = a$ is an integer. This means that a must cancel out completely in this fraction—but it cannot from any factors in b . Therefore, a cancels out completely from factors of 2. This means that either $a = 1$ or $a = 2$. But if $a = 1$, then

$$\left| \frac{a}{b} \right| = \frac{1}{|b|} \leq 1 < \sqrt{2}.$$

This is a problem and a contradiction in this case. Suppose now that $a = 2$. Then, $\sqrt{2} = \frac{2}{b}$ turns into $b = \sqrt{2}$. But there is no integer which squares to 2. This is a contradiction in this case. Therefore, our original assumption that $\sqrt{2}$ was an integer is false.

11. First, a base condition is satisfied since $a_0 < 5$. Next, assume that the statement is true at an index n so that $a_n < 5$. Now we use this idea to show that $a_{n+1} < 5$. To do this, work with the inequality $a_n < 5$ and turn it into an equality with $\sqrt{2a_n + 1}$ by using some operations. First, $a_n < 5$ turns into $2a_n < 10$ which turns into $2a_n + 1 < 11$ which turns into $\sqrt{2a_n + 1} < \sqrt{11} < 5$. This means that assuming $a_n < 5$, yields that $a_{n+1} < 5$. That is, all elements of the sequence are less than 5.

12. First of all, we have a base case when $n = 1$ (the first positive integer). We have: $4^3 - 1 = 63$ which indeed is divisible by 3. We could even prove a more general statement by taking the base case to be at $n = 0$ to see

that $4^0 - 1 = 0 = 0 \cdot 3$ which is a multiple of 3. Now, assume that $4^n - 1$ is divisible by 3. We will show that $4^{n+1} - 1$ is divisible by 3 based on this assumption. The question is, how do we turn $4^n - 1$ into $4^{n+1} - 1$ and does this process maintain the property of being divisible by 3? We could proceed as follows:

$$4 \cdot (4^n - 1) + 3 = 4^{n+1} - 1$$

So really what we want to show is that the following is a multiple of 3:

$$4 \cdot (\text{multiple of 3}) + 3$$

Yet, this should be clear because we can factor a 3 out of both parts of the sum. Really in the end, a proof is nothing more than restating something enough times until the reason is logically obvious and clear.

13. Let's take a base case $n = 0$ to see that $0^5 - 0 = 0$ is a multiple of 5 and so this case is clearly true. Next, let's assume that $n^5 - n$ is divisible by 5. We will now show that $(n+1)^5 - (n+1)$ must also be divisible by 5. Let's do this by seeing how we can change $n^5 - n$ into $(n+1)^5 - (n+1)$ with a process that would maintain divisibility by 5. Sometimes, it is helpful to pull apart the expression with $(n+1)$ and find the expression of n in it. Using the hint:

$$(n+1)^5 - (n+1) = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - n - 1$$

$$= (n^5 - n) + \underbrace{(5n^4 + 10n^3 + 10n^2 + 5n)}_{\text{divisible by 5}}$$

By assumption, $n^5 - n$ is divisible by 5. Adding two things that are divisible by 5, gives something that is divisible by 5 since we can then factor 5 out of the sum. Hence, we have just shown that $(n+1)^5 - (n+1)$ is divisible by 5 based on the assumption that $n^5 - n$ is divisible by 5.

14. Just notice that $(-n)^5 - (-n) = -(n^5 - n)$. So negating n , just negates the entire expression.

15. A base case would be $n = 0$ yielding $0 \cdot (0+1) \cdot (0+2) = 0$ which is clearly a multiple of 3. Next, let's assume that $n(n+1)(n+2)$ is divisible by 3. But this means that either n or $n+1$ or $n+2$ is divisible by 3. So we have different cases to consider. Our goal is to show that the statement one step further into the integers: $(n+1)(n+2)(n+3)$ is divisible by 3. Now, in the cases that $(n+1)$ or $(n+2)$ are divisible by 3, this is clear since they are again factors of $(n+1)(n+2)(n+3)$. Now in the case that n is a multiple of 3, we actually have that $n+3$ is a multiple of 3 and $(n+3)$ is a factor of $(n+1)(n+2)(n+3)$. Therefore, in all cases of assuming that $n(n+1)(n+2)$ is divisible by 3, we arrive at the fact that $(n+1)(n+2)(n+3)$ is divisible by 3.

16. First show that x being in A implies that x is in B . Suppose that $x = 3k + 1$. We try to show that there exists an integer j so that x is also equal to $3j + 4$. Simply solve for j :

$$3k + 1 = 3j + 4$$

$$3k - 3 = 3j$$

$$j = k - 1.$$

Now we go to the next direction. We show that x in B implies that x is in A . This amounts to solving for k when $3k + 1 = 3j + 4$ and verifying that k is an integer.

$$3k + 1 = 3j + 4$$

$$3k = 3j + 3$$

$$k = j + 1.$$

17. Let A be the statement “there exists m so that $n = 2^m$ ” and let B be the statement “ $n > 0$.” We first show if A , then B . Suppose that $n = 2^m$ for some real number m . This means that n is in the range of $f(x) = 2^x$ which is all numbers greater than 0 which means that $n > 0$. Now, lets show if B , then A . If $n > 0$, then n is in the domain of $\log_2(x)$ so that if we let $m = \log_2(n)$, then for sure $n = 2^m$. This gives that B implies A . Hence, the two definitions are consistent.

Sets, Functions, and Fibers

1.2

1.2.1 Sets and Subsets	38
1.2.2 Basic Set Operations	41
1.2.3 Defining Functions	43
1.2.4 Mapping Subsets to Subsets	45
1.2.5 Injectivity, Surjectivity, Bijectivity	50
1.2.6 Exercises	58
1.2.7 Solutions	61

Questions to Guide Your Study:

- *What are some common notations associated with sets?*
- *What are operations we can perform between sets?*
- *What is needed in the definition of a function?*
- *What are the terms domain, codomain, image, preimage and fiber and how do they pertain to functions?*
- *What is a fiber box diagram and how can we use it to discuss injectivity, surjectivity and bijectivity?*
- *What is the relationship between fibers and solving systems of equations?*
- *How can chunking up a set into a partition define a function?*

1.2.1 Sets and Subsets

In linear algebra, we deal with a lot of sets and collections. So naturally, we need some notation to describe sets and what we can do with them.

First, let's introduce symbols that denote some common sets: \mathbb{R} , \mathbb{R}^2 , \mathbb{R}^3 , \mathbb{C} , \mathbb{Z} , \mathbb{N} , $P^n(R)$, $R[x]$.

Some Common Sets

- \mathbb{R} : the set of all *real numbers*.
- \mathbb{R}^2 : the set of all ordered pairs (x, y) of *real numbers*. That is, *the xy plane!*
- \mathbb{R}^3 : the set of all ordered triples (x, y, z) of *real numbers*. That is, *3 space!*
- \mathbb{C} : the set of *complex numbers* of the form $a + bi$ where $i = \sqrt{-1}$ and a and b are *real numbers*.
- \mathbb{Z} : the set of *integers*. (Think: integerz.)
- \mathbb{N} : the set of *natural (counting) numbers* 1, 2, 3, ... or in other words, the collection of *positive integers*.
- \mathbb{Q} : the set of all fractions $\frac{a}{b}$ of integers a and b where $b \neq 0$. (Think: *quotient.*)
- $P^n(R)$: the set of all *polynomials* of degree n with coefficients in the set R and variable x (the x is not given in this notation).
- $R[x]$: the set of all polynomials with variable x and with coefficients in the set R . (This notation allows us to replace x with another variable.)
- \emptyset : this is the empty set that does not have anything in it.

We need a way of saying that something is an element of a set:

\in “element of”

We write $x \in A$ to mean that x is an element of A or when we say “ x is in A .”

Example 1. Let’s use the symbol \in :

- $4 \in \mathbb{Z}$
- $\sqrt{2} \in \mathbb{R}$
- $2 + 5i \notin \mathbb{R}$
- $5t^7 - t^2 + 1 \in \mathbb{Z}[t]$

We also need a way of describing what elements actually live in a set. We use:

Set builder notation

$$\text{Set } S = \{ \underbrace{\text{Expression } E}_{\text{"the what"}} : \underbrace{\text{Criteria for } E \text{ to satisfy}}_{\text{"the conditions"}} \}$$

We say *what* we want to consider to be in the set and then we give the conditions for it to be in the set. Defining what the elements of a set are is the same as defining what a set is.



Video Before giving examples of this notation, we state an important rule:

Variable Initialization Rule

Every time we use a variable, make sure it is clear what it stands for and where it comes from.

Example 2. Under the assumption that $i = \sqrt{-1}$, we can use set builder notation to define what the set of complex numbers \mathbb{C} looks like:

$$\mathbb{C} = \{ \underbrace{a + bi}_{\text{expression}} : \underbrace{a \in \mathbb{R}, b \in \mathbb{R}}_{\text{criteria for expression}} \}$$

Example 3. We can express the set \mathbb{N} of natural numbers in set builder notation:

$$\mathbb{N} = \{ z : z > 0, z \in \mathbb{Z} \}$$

Example 4. The collection of polynomials with variable x of degree 3 with coefficients in \mathbb{Z} can be expressed as:

$$P^3(\mathbb{Z}) = \{ a_0 + a_1x + a_2x^2 + a_3x^3 : a_0, a_1, a_2, a_3 \in \mathbb{Z}, a_3 \neq 0 \}$$

Notice that we require the coefficient $a_3 \neq 0$. This is to ensure that the degree of the polynomial is 3.

Example 5. The collection of polynomials with variable x and with coefficients in \mathbb{C} can be written in set builder notation as:

$$\mathbb{C}[x] = \left\{ \sum_{k=0}^n a_k x^k : n \geq 0, n \in \mathbb{Z}, a_k \in \mathbb{C} \text{ for } k = 0, 1, 2, \dots, n \right\}$$

Notice that in the “what” of the set builder definition we have a sum:

$$\sum_{k=0}^n a_k x^k = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

which is a polynomial of degree n .

Example 6. We can write $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$ and $\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}$.

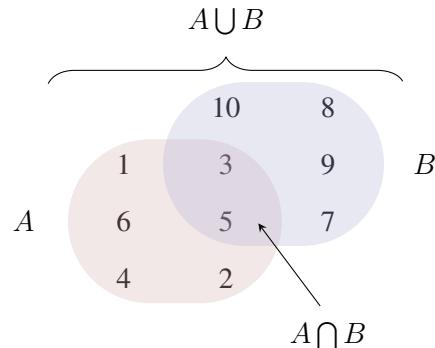
1.2.2 Basic Set Operations



Now that we have notation for describing what goes into a set, let’s see some notation for some basic set operations and comparisons. Consider the sets

$$A = \{1, 2, 3, 4, 5, 6\} \quad B = \{3, 5, 7, 8, 9, 10\}$$

pictured as follows:



We write the intersection “ \cap ”

$$A \cap B = \{3, 5\},$$

read “ A intersect B ,” for all the elements that are in both A and B . We write the union “ \cup ”

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\},$$

read “ A union B ,” for all the elements that are either in A or in B . The set subtraction “ \setminus ”

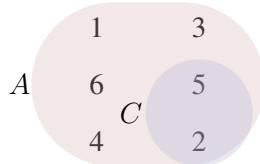
$$A \setminus B = \{1, 2, 4, 6\},$$

read “ A minus B ,” denotes all the elements in A which are not in B .

Example 7. $\{1, 5, 4\} \setminus \{4, 8\} = \{1, 5\}$

Example 8. $\mathbb{Z} \setminus \mathbb{N} = \{k : k < 1, k \in \mathbb{Z}\}$

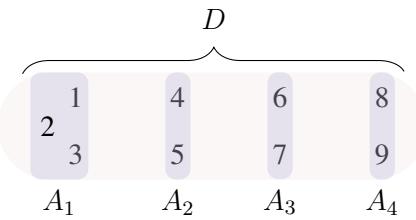
In the following, notice that C is a **subset** of A :



We use the symbol \subset and write $C \subset A$.

Example 9. $P^5(\mathbb{R}) \subset \mathbb{R}[x]$

Suppose that a set D is the **disjoint union** of smaller subsets such as in the following picture:



We say that the subsets A_1, A_2, A_3, A_4 **partition** D . They, themselves, are *nonempty* yet every pairwise intersection between them is empty “ \emptyset ”:

$$A_i \cap A_j = \emptyset \quad \text{for } i \neq j$$

and their union is all of D :

$$D = A_1 \cup A_2 \cup A_3 \cup A_4.$$

We use the **disjoint union** symbol “ \coprod ”:

$$D = A_1 \coprod A_2 \coprod A_3 \coprod A_4.$$



Example 10. Notice that polynomials of degree 3 are not degree 2 polynomials and vice versa.

Therefore, polynomials in the variable x with real coefficients can be partitioned as follows:

$$\mathbb{R}[x] = P^0(\mathbb{R}) \coprod P^1(\mathbb{R}) \coprod P^2(\mathbb{R}) \coprod P^3(\mathbb{R}) \coprod \dots$$

Another way of writing this infinite partition is:

$$\mathbb{R}[x] = \coprod_{k=0}^{\infty} P^k(\mathbb{R})$$

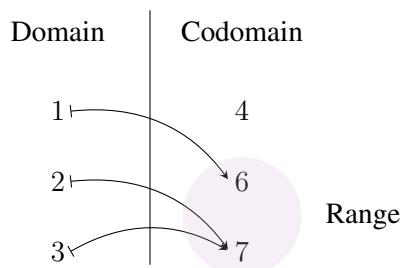
1.2.3 Defining Functions

Often, linear algebra is thought of as the study of matrices. Loosely thought of, these are just rectangular arrays of numbers. Yet they mean so much more! They are actually functions. We are going to have to start thinking of functions in new ways to make this connection.



First, what is a function? It is *an assignment mapping* given by the following **mapping diagram**:

The function f :



The word **mapping** means there are “routes” mapped between points. We are mapping from beginning points in the “**domain** country” and arriving at destinations in the “**codomain** country.” The arrow \mapsto shows this route. The tail \leftarrow tells us where we start and the tip \rightarrow tells us where we finish. The **range** is the actual collection of destinations that are hit. For the function f , writing $f(1) = 6$ is equivalent to writing $1 \mapsto 6$. We say that 6 is the **image** of 1 via the map f . *Imagine that the function is like a reflecting pool, the domain element like an object by it, and the codomain element it is sent to is the image in the reflecting pool.*

Notice that our diagram above is *different* from a function table like:

x	$f(x)$
1	6
2	7
3	7

The table is *deceiving!* It does not tell us the *codomain country!* It also de-emphasizes the fact that two of the routes have the same destination. The mapping picture on the other hand tells the whole story of what the function is.

A programmer knows that it is important to be aware of the “data type” output of a function. The idea of codomain is the idea of “data type.” In defining a function, we do not need to know all *specific outputs* of the function—we just need to know what *type of output* to expect. If the routes we define take us into the expected codomain set, then the function is well-defined.

There are three essential elements of a well-defined function:

Defining Functions

To define a function f , we need:

- a domain set D
- a codomain set C
- a well-defined rule, process or algorithm that takes *each* element in the domain set D to an element of the codomain set C .

Function Definition Notation

For a function with domain D and codomain C , we write:

$$f : D \rightarrow C$$

Example 11. The function $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = \frac{1}{x}$ is *not well-defined* since the function rule at $x = 0$ does not produce an output in codomain \mathbb{R} .

Example 12. Define $f : \mathbb{R} \rightarrow \mathbb{R} \cup \{\infty\}$ by

$$f(x) = \begin{cases} \frac{1}{x} & x \neq 0 \\ \infty & x = 0 \end{cases}$$

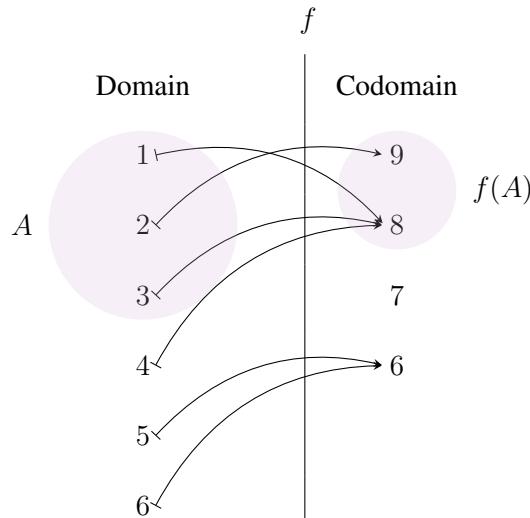
This is a well-defined function.

Example 13. The function $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = \sqrt{x}$ is *not well-defined* since for all $x < 0$, \sqrt{x} is not a real output.

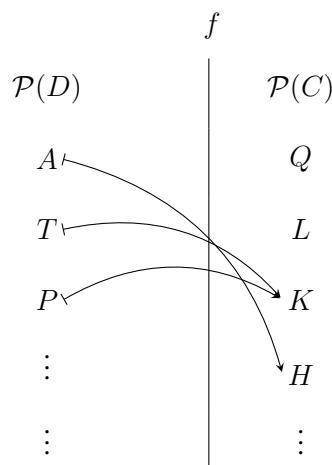
1.2.4 Mapping Subsets to Subsets



Video Functions do not just describe how *elements* are assigned destinations, but they also describe map routes from *subsets* in the domain to *subsets* in the codomain and even *backwards* routes from *subsets* in the codomain to *subsets* in the domain. Suppose that we have a function $f : D \rightarrow C$ defined by the following mapping diagram:

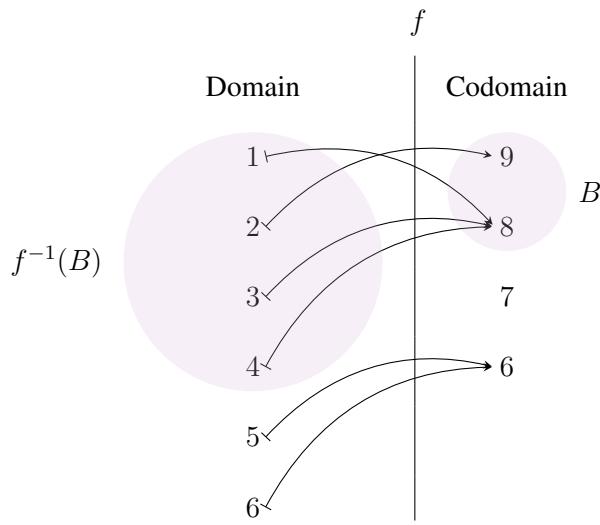


From this diagram, you should be able to see how the function naturally takes the subset $A \subset D$ and then assigns it a destination subset $f(A) \subset C$ called the **set image** of A via the function f . If we let $\mathcal{P}(S)$ represent the collection of subsets of a set, then we suddenly have a new mapping diagram specifying routes that start in $\mathcal{P}(D)$ and end in $\mathcal{P}(C)$ that comes from the original function f itself:



Example 14. The image of $\{4, 5, 6\}$ via the above function f is $\{6, 8\}$. We write: $f(\{4, 5, 6\}) = \{6, 8\}$. We are plugging a whole set into a function that was originally defined on elements!

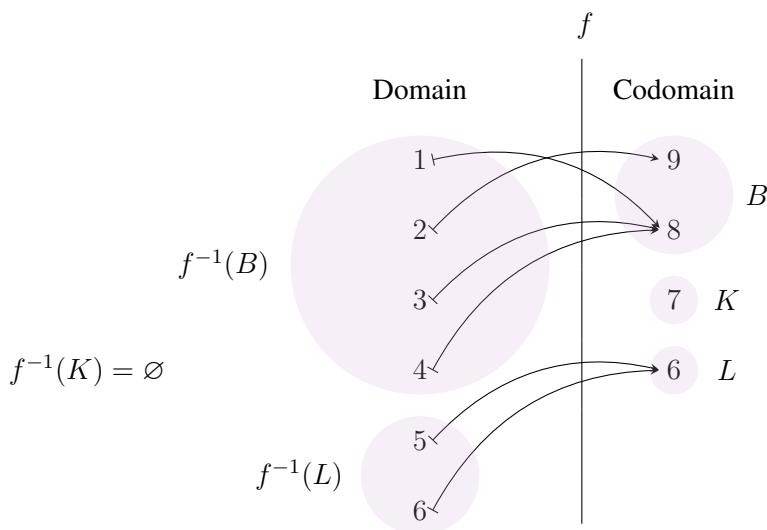
Notice the following relationship from a set B in the codomain and tracing the element maps backwards to find a **preimage** set in the domain:



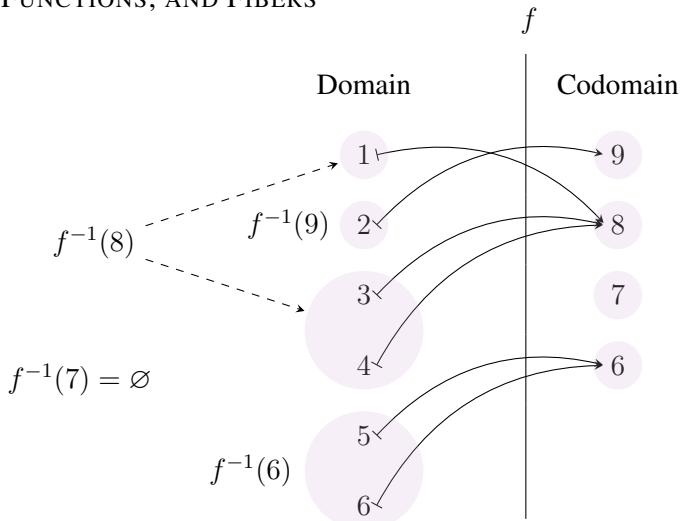
Example 15. The preimage of the set $\{6, 9\}$ via f is $\{2, 5, 6\}$. We write $f^{-1}(\{6, 9\}) = \{2, 5, 6\}$.

Example 16. The preimage of the set $\{7\}$ is \emptyset . We can write $f^{-1}(\{7\}) = \emptyset$.

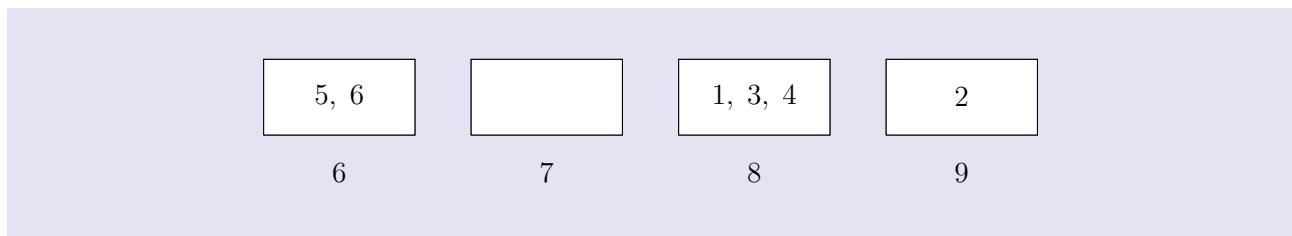
Consider the following preimages:



Notice that a disjoint union in the codomain pulls back to a disjoint union in the domain! In particular, let's just consider the preimages of single points in the codomain. Since distinct points in the codomain are *distinct* (i.e. disjoint), then their respective preimages should be disjoint as well:



Notice that when we are considering preimages of single points, we dispense with set notation: instead of writing $f^{-1}(\{8\})$, we write $f^{-1}(8)$. Let's use the fact that these preimages are disjoint to come up with another way to view this same function f —we use a ***fiber box diagram***:



The boxes are indexed below by codomain elements. What goes inside each box is the preimage of that particular codomain element. This diagram completely describes the function. The boxes are the *building blocks* of the function itself—the *fibers* of the function.

Fiber

Each of the boxes in a fiber box diagram is called a *fiber*. Given a function $f : D \rightarrow C$, the preimage of a subset of C that consists of a single point y denoted as $f^{-1}(\{y\})$ or simply $f^{-1}(y)$ is called the *fiber* over y via the function f .

Example 17. The fiber over 8 via the function f above is $\{1, 3, 4\}$.

Example 18. Define a function $g : \mathbb{R} \rightarrow \mathbb{R}$ by $g(x) = x^2$. Then the fiber over 4 is $\{-2, 2\}$ and the fiber over -1 is \emptyset .



Example 19. Define a function $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ by $g(x, y) = (2x + y, x - y)$. Let's find the fiber of g

over

(a) $(0, 0)$

(b) $(1, 2)$.

For (a), we think:

$$(x, y) \mapsto (2x + y, x - y) = (0, 0)$$

This amounts to solving a system of equations:

$$\begin{aligned} 2x + y &= 0 \\ x - y &= 0 \end{aligned}$$

Adding the two equations, we have: $3x = 0$ so that $x = 0$. When $x = 0$, we notice from either equation that $y = 0$. The only way to get $(0, 0)$ as the image then is for $x = 0$ and $y = 0$. This tells us that the fiber is a subset of the domain consisting of a single element: $g^{-1}(0, 0) = \{(0, 0)\}$.

For (b), we solve the system:

$$\begin{aligned} 2x + y &= 1 \\ x - y &= 2 \end{aligned}$$

Adding the equations, we have $3x = 3$ so that $x = 1$. So every element of the preimage of $(1, 2)$ will look like $(1, *)$. Using either equation, we notice that y must be -1 . For instance, $2(1) + y = 1$ becomes $y = -1$. Therefore, $g^{-1}(1, 2) = \{(1, -1)\}$.



Example 20. Define a function $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ by $g(x, y) = (x + y, 2x + 2y)$. Let's find the fiber of g over

(a) $(0, 0)$

(b) $(1, 2)$

(c) $(1, 1)$

For (a), we think:

$$(x, y) \mapsto (x + y, 2x + 2y) = (0, 0)$$

This amounts to solving a system of equations:

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

Notice that the second equation is really the same as the first equation since:

$$2 \cdot \left(x + y = 0 \right) = 2x + 2y = 0$$

Therefore, the second equation gives no new restrictions on the values x and y beyond what the first equation gives. This tells us that the only condition to guarantee that a domain element $(x, y) \in \mathbb{R}^2$ maps to $(0, 0)$ is simply $x + y = 0$ or rather $y = -x$. This is a straight line in the plane. *It is the fiber over $(0, 0)$ via the function g .*

$$g^{-1}(0, 0) = \{ (x, y) : y = -x, (x, y) \in \mathbb{R}^2 \}$$

For (b), we want $(x, y) \mapsto (x + y, 2x + 2y) = (1, 2)$. We solve the system:

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

Notice again that both equations are really the same since the second equation is double the first. Therefore, the condition $x + y = 1$ which is $y = -x + 1$ is enough to guarantee that (x, y) is in $g^{-1}(1, 2)$. Therefore:

$$g^{-1}(1, 2) = \{ (x, y) : y = -x + 1, (x, y) \in \mathbb{R}^2 \}.$$

The nonempty fibers look like:

For (c), we want to find all $(x, y) \in \mathbb{R}^2$ such that $(x, y) \mapsto (1, 1)$. We consider the system of equations:

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

We multiply the first equation by -2 and add it to the second equation to obtain: $0 = -1$. This is a false statement. We arrived at it by assuming that we could find $(x, y) \mapsto (1, 1)$. In other words, we were assuming that $g^{-1}(1, 1) \neq \emptyset$. We just showed that this assumption was false. Therefore,

$$g^{-1}(1, 1) = \emptyset$$



Example 21. Notice in the last example that the only way to have a nonempty fiber is for the system to look like:

$$\begin{aligned} x + y &= a \\ 2x + 2y &= 2a \end{aligned}$$

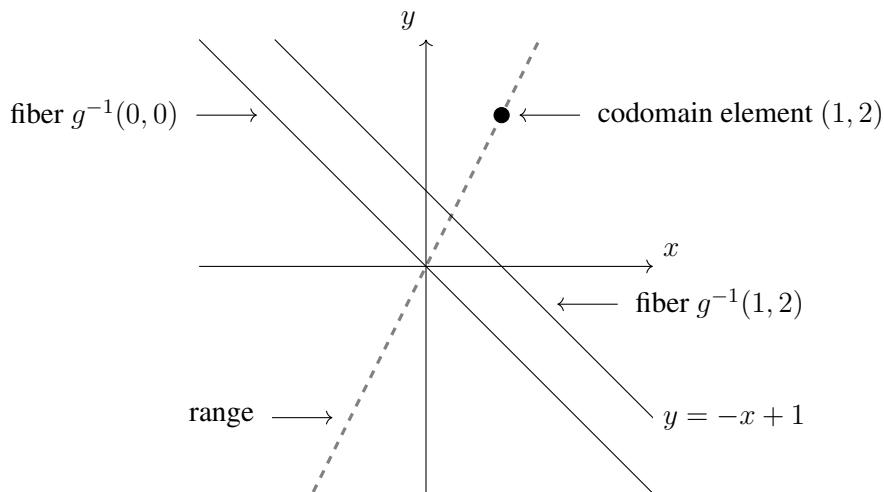
In other words, we need $(x, y) \mapsto (a, 2a)$. That is, a codomain element (x, y) has a nonempty fiber if there is

some $a \in \mathbb{R}$ so that $x = a$ and $y = 2a$. In other words, $y = 2x$. So, the codomain elements that have nonempty fibers are:

$$\{(x, y) : y = 2x, (x, y) \in \mathbb{R}^2\}.$$

Saying a codomain element has a nonempty fiber is another way of saying that the element is in the range of the function. The range is simply the line $y = 2x$.

Notice that $g^{-1}(a, 2a) = \{ (x, y) : y = -x + a, (x, y) \in \mathbb{R}^2 \}$ That is, all nonempty fibers look like lines parallel to $y = -x$. Here is a picture description of what we are seeing:



Fiber Description of Range

The range of a function is simply the collection of codomain elements that have nonempty fibers.

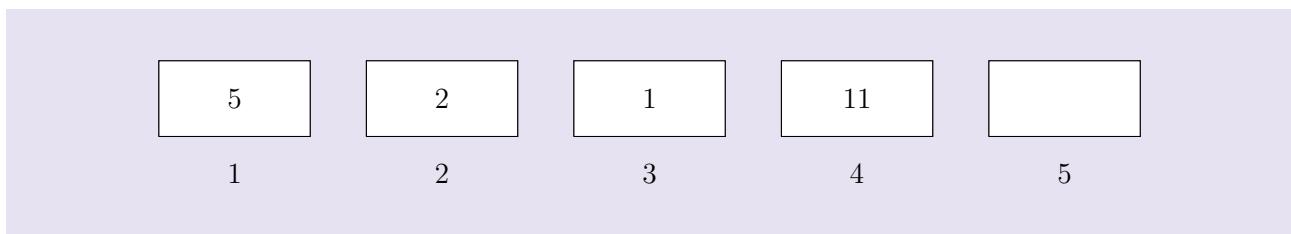
1.2.5 Injectivity, Surjectivity, Bijectivity

Fiber box diagrams allow us to easily define some notions that follow.

Injective

A function is *injective* if none of the fibers have *more* than one element.

Example 22. The following diagram represents an injective function:



The codomain is {1, 2, 3, 4, 5} and the domain is {1, 2, 5, 11}.



Example 23. The function $g : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ defined by $g(x, y) = (x + y, x - y, x - y)$ is an injective function since for any codomain element $(a, b, c) \in \mathbb{R}^3$, the following system of equations:

$$\begin{aligned} x + y &= a \\ x - y &= b \\ x - y &= c \end{aligned}$$

either has a unique solution or no solution. (Each fiber has one element or no elements.) For instance, when $b \neq c$, then there is no solution since subtracting the last two equations gives $0 = b - c$.

When $b = c$, then we are just solving the system:

$$\begin{aligned} x + y &= a \\ x - y &= b \end{aligned}$$

Adding the two equations gives $2x = a + b$ so that $x = \frac{a+b}{2}$ and then $y = \frac{a-b}{2}$. Hence,

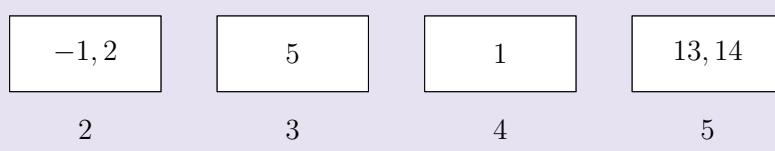
$$g^{-1}(a, b) = \left\{ \left(\frac{a+b}{2}, \frac{a-b}{2} \right) \right\}$$

Therefore, each fiber has at most one element. It is like we are plotting a transformed copy of the domain into the range—where nothing has been *merged*—just “injected in.”

Surjective

A function is *surjective* if none of the fibers are empty.

Example 24. The following diagram represents a surjective function:



The codomain is {2, 3, 4, 5} and the domain is {−1, 1, 2, 5, 13, 14}.



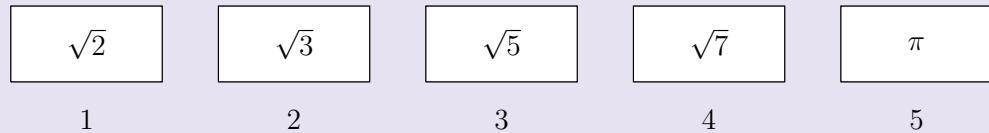
Example 25. Consider the function $g : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ defined by $(x, y, z) \mapsto (x, y)$. This function is surjective because for any codomain element (x, y) ,

$$g^{-1}(x, y) = \{ (x, y, z) : (x, y, z) \in \mathbb{R}^3 \} \neq \emptyset$$

Bijection

A function is *bijection* if it is *both* injective and surjective.

Example 26. The following diagram represents a bijective function:



The codomain is $\{1, 2, 3, 4, 5\}$ and the domain is $\{\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \pi\}$.



Example 27. Consider the function $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by $g(x, y) = (x + y, x - y)$. This is a lot like the function we saw in [example 23](#) except the system of three equations becomes:

$$\begin{aligned} x + y &= a \\ x - y &= b \end{aligned}$$

Every $(a, b) \in \mathbb{R}^2$ has a unique solution. Therefore, every fiber is nonempty and has at most one element. The function is bijective. Every coordinate point of \mathbb{R}^2 has simply just been relabeled.

Theorem 1.2.1 Fiber Partitions

The fibers of a *surjective* function partition the domain.

Proof. See the exercises—just carefully match definitions! □

Chunking Principle

To make a surjective function, just chunk up a set and give *distinct* labels to each chunks. *This is equivalent to a fiber box diagram!*



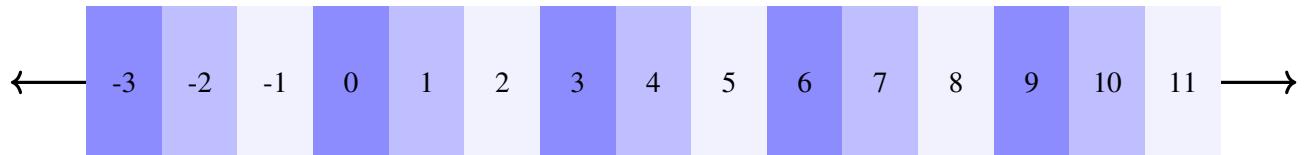
Example 28. By chunking up the plane \mathbb{R}^2 and labeling the parts we will have a function $f : \mathbb{R}^2 \rightarrow C$ to a set C which denotes the labels we have used.

For instance, suppose that we chunk the plane up into horizontal lines $y = k$. The collection of all horizontal lines partitions the plane. We just need a label for each horizontal line which is distinct from every other horizontal line. We can just use the y -value k for the horizontal line $y = k$. Therefore, we have a fiber box diagram: each horizontal line of points is a box. The box at $y = k$ has codomain label k . This chunking has produced the function:

$$f(x, y) = y.$$

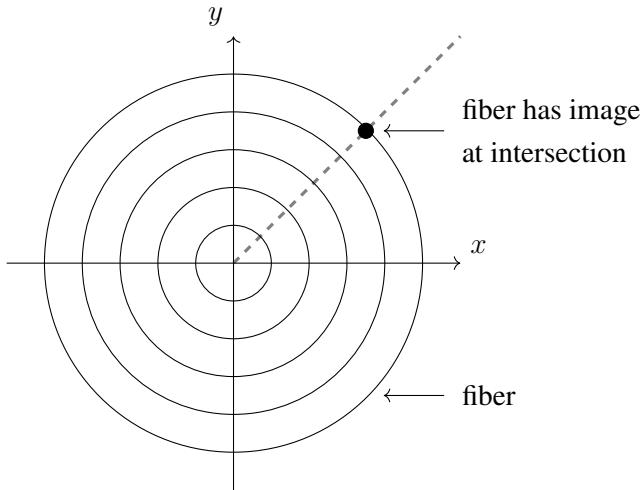
Example 29. Chunking the plane into lines $x + y = k$ can be thought of as a fiber box diagram for the function $f(x, y) = x + y$.

Example 30. Consider the following chunking of \mathbb{Z} into three different shades:



This produces a well-defined function $f : \mathbb{Z} \rightarrow \{0, 1, 2\}$ defined by the idea $x \mapsto k$ where x is k more than a multiple of 3 and $k \in \{0, 1, 2\}$.

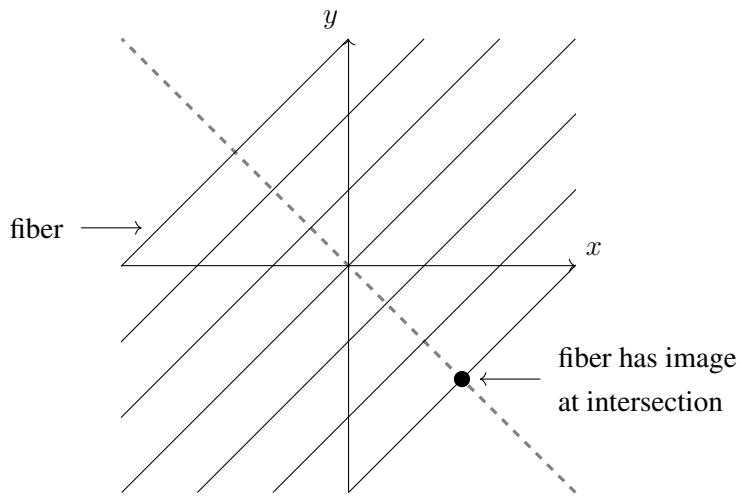
Example 31. We can define a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ by the following picture:



The fibers are just the circular lines centered at the origin. These fill up and partition the plane. The range is the collection of points appearing on the dashed line $y = x$, $x \geq 0$. Because the codomain is larger than the range, then there are a lot of empty fibers. Think of this as a fiber box diagram. The codomain element that each circle fiber is sent to via the function is precisely the intersection of the fiber with the line $y = x$. For instance,

$$f\left(\{(x, y) : x^2 + y^2 = 1\}\right) = \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$$

Example 32. We can define $g: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ by the following picture:



The fibers are just lines parallel to $y = x$. These fill up and partition the plane. The range is the collection of points appearing on the dashed line $y = -x$. Because the codomain is larger than the range, then there are a lot of empty fibers. Think of this as a fiber box diagram. The codomain element that each line fiber is sent to via the function is precisely the intersection of the fiber with the line $y = -x$. For instance,

$$f\left(\{(x, y) : y = x - 2\}\right) = (1, -1)$$



Example 33. Consider the functions f and g in the last two examples. If we consider the function $g \circ f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by $(x, y) \mapsto g(f(x, y))$, let's see what happens. The function f will take (x, y) and find what circle fiber it is in. Then, it will send it to the intersection of that circle with $y = x$, $x \geq 0$. So at this point, only points in $y = x$ are going into the function $g(x)$. But now notice that $y = x$ itself is a single fiber of g which means that all of the range of f has the same image via g . This image is the intersection of the fiber $y = x$ of g with the line $y = -x$. This is precisely $(0, 0)$. That is, $g \circ f$ sends every point of \mathbb{R}^2 to the origin!

Example 34. A contour map (a topographical map) used to describe altitudes and changes of terrain *is a fiber box diagram* of a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ where the output is altitude and the input is coordinate position. That is, every altitude is a codomain element. A curve on the map representing that altitude *is the preimage of that altitude!*

Key Concepts from this Section

- **\mathbb{R} :** (page 38) The set of real numbers.
- **\mathbb{R}^2 :** (page 38) The set of ordered pairs of real numbers (x, y) .
- **\mathbb{R}^3 :** (page 38) The set of ordered triples of real numbers (x, y, z) .
- **\mathbb{C} :** (page 38) The set of complex numbers of the form $a + bi$ where $i = \sqrt{-1}$ and a and b are real numbers.
- **\mathbb{Z} :** (page 38) The set of integers. (Think: integerz.)
- **\mathbb{N} :** (page 38) The set of *natural* (counting) numbers 1, 2, 3, ... or in other words, the collection of positive integers.
- **$P^n(R)$:** (page 38) The set of all *polynomials* of degree n with coefficients in the set R and variable assumed to be x (the x is not given in this notation).
- **$R[x]$:** (page 38) The set of all polynomials with variable x and with coefficients in the set R . (This notation allows us to replace x with another variable.)
- **\in “element of”:** (page 39) We write $x \in A$ to mean that x is an element of A or when we say “ x is in A .”
- **set builder notation:** (page 39)

$$\text{Set } S = \{ \underbrace{\text{Expression } E}_{\text{“the what”}} : \underbrace{\text{Criteria for } E \text{ to satisfy}}_{\text{“the conditions”}} \}$$

We say *what* we want to consider to be in the set and then we give the conditions for it to be in the set. Defining what the elements of a set are is the same as defining what a set is.

- **variable initialization rule:** (page 40) Every time we use a variable, make sure it is clear what it stands for and where it comes from.
- **\cap :** (page 41) The notation $A \cap B$, read “ A intersect B ,” means all the elements that are in both A and B .
- **\cup :** (page 41) The notation $A \cup B$, read “ A union B ,” means all the elements that are either in A or in B .
- **\setminus :** (page 41) The notation $A \setminus B$, read “ A minus B ,” denotes all the elements in A which are not in B .
- **subset:** (page 42) A subset of a set A is a collection of some of the elements of the set A —but not necessarily all of them.
- **\subset :** (page 42) The notation $A \subset B$ means that A is a subset of B or that B is a superset of A . That is, B contains all of the elements that A contains.
- **disjoint union:** (page 42) A disjoint union is a union of sets which pairwise do not intersect. That is any two of the sets in the union such as a set A and a set B have $A \cap B = \emptyset$.
- **partition:** (page 42) A partition of a set D is a disjoint union of subsets that equals D .
- **\emptyset :** (page 42) The empty set.
- **disjoint union:** (page 42) If two sets A and B have trivial intersection, we say that their union $A \cup B$ is a disjoint union. To emphasize this fact, we may write $A \coprod B$.
- **\coprod :** (page 42) We write $A \coprod B$ to mean that disjoint union of the sets A and B .
- **mapping diagram:** (page 43) A mapping diagram, in contrast to a function table shows all of the domain and codomain. We know when a domain element is sent to a codomain element when we use an assignment arrow \mapsto .
- **mapping:** (page 43) Another word for a function is a *map* or a *mapping*.
- **domain:** (page 43) The set of elements that a function sends through routes to the codomain.
- **codomain:** (page 43) A set which contains all the destinations of a function. It is thought of as the “data type” of the output of the function.
- **\mapsto :** (page 43) The assignment arrow. It shows how an element in the domain is sent to its image in the codomain.
- **range:** (page 43) The actual destinations of the routes from the domain into the codomain for a function. It is the collection of all the images of a function.

- **image:** (page 43) The image of a domain element via a function is the destination of the domain element through its mapping route \longmapsto .
- **defining functions:** (page 44) To define a function f , we need:
 - a domain set D
 - a codomain set C
 - a well-defined rule, process or algorithm that takes *each* element in the domain set D to an element of the codomain set C .

- **function definition notation:** (page 44) For a function with domain D and codomain C , we write:

$$f : D \rightarrow C$$

- **set image:** (page 45) The image of a subset of the domain via a function is collection of images of the points that are in that subset.
- **preimage:** (page 46) A preimage of a codomain subset is the subset of the domain of all elements that map to that codomain subset.
- **fiber box diagram:** (page 47)
- **fiber:** (page 47) Each of the boxes in a fiber box diagram is called a *fiber*. Given a function $f : D \rightarrow C$, the preimage of a subset of C that consists of a single point y denoted as $f^{-1}(\{y\})$ or simply $f^{-1}(y)$ is called the *fiber* over y via the function f .
- **fiber description of range:** (page 50) The range of a function is simply the collection of codomain elements that have nonempty fibers.
- **injective:** (page 50) A function is *injective* if none of the fibers have *more* than one element.
- **surjective:** (page 51) A function is *surjective* if none of the fibers are empty.
- **bijective:** (page 52) A function is *bijective* if it is *both* injective and surjective.
- **theorem 1.2.1 fiber partitions:** (page 52) The fibers of a *surjective* function partition the domain.
- **chunking principle:** (page 52) To make a surjective function, just chunk up a set and give *distinct* labels to each chunks. *This is equivalent to a fiber box diagram!*

1.2.6 Exercises

Computation Practice

1. Suppose that $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ is given by $f(x, y) = (x + y, x - y, 2x)$. Determine what the following fibers are:

- (a) $f^{-1}(1, 1, 2)$
- (b) $f^{-1}(1, 1, 0)$

Do you think this function is injective, surjective or neither? Explain your reasoning.

2. Suppose that $f : \mathbb{R}^3 \rightarrow \mathbb{R}$ is given by $f(x, y, z) = x + y + z$. Write the following fibers in set builder notation:

- (a) $f^{-1}(0)$
- (b) $f^{-1}(1)$

Do you think this function is injective, surjective or neither? Explain your reasoning.

3. Let $C = \{y : y \in \mathbb{R}, y > 0\}$. Suppose that $D \subset \mathbb{R}$ is an interval of the form “ (a, b) ” using interval notation. Determine all conditions on D that would guarantee that $f : D \rightarrow C$ given by $x \mapsto x^2$ would be a bijective function.

4. Suppose that $f : D \rightarrow C$ with $D = \{2, 3, 4, 5\}$, $C = \{5, 6, 9, 11, 23\}$, $f(D) = \{6, 9, 11\}$, and $f(2) = f(3) = 6$. Answer the following:

- (a) $f^{-1}(5) \cap f^{-1}(6) \cap f^{-1}(9) \cap f^{-1}(11) \cap f^{-1}(23)$
- (b) $f^{-1}(5) \cup f^{-1}(6) \cup f^{-1}(9) \cup f^{-1}(11) \cup f^{-1}(23)$
- (c) $\{f(2)\} \cap \{f(3)\}$
- (d) $\{f(2)\} \cap \{f(3)\} \cap \{f(4)\} \cap \{f(5)\}$
- (e) $\{f(2)\} \cup \{f(3)\}$
- (f) $\{f(2)\} \cup \{f(3)\} \cup \{f(4)\} \cup \{f(5)\}$

5. Compute the following which will be true for *any* function $f : D \rightarrow C$ such that $f(D) = \{4, 7\}$ and $C = \{4, 5, 6, 7\}$ and $f^{-1}(4) = \{3, 5, 8\}$:

(a) $f^{-1}(4) \cap f^{-1}(7)$

(b) $f(f^{-1}(\{4, 5\}))$

(c) $f^{-1}(f(3))$

6. Consider the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x, y) = \frac{1}{x - y}$.

(a) Why is f not well-defined?

(b) Name one domain point where f is not defined.

7. Consider the function $f : [0, 2\pi] \rightarrow [0, 1]$ defined by $f(x) = \sin(x)$. It is not well-defined.

(a) Why?

(b) Change the codomain so that f is well-defined.

Notation Practice:

Remember the variable initialization rule!

8. Express the set of solutions to the following systems of equations as fibers of functions. In particular, give the notation that defines a well-defined function and then the notation that describes the fiber using that function. *You do not need to determine the solutions in this exercise!*

(a) $2x + 3y + z + w = 2$

$x - y + 5z = 1$

(b) $2x + 3y = 0$

$x - y = 1$

(c) $2x + 3y + z + w + u = 7$

$5x = 5$

9. Write the following in set builder notation:

(a) $\mathbb{C} \setminus \mathbb{R}$

(b) $\mathbb{R}[x] \setminus \mathbb{R}$

(c) $f(\mathbb{R}) \cap g(\mathbb{R})$ where $f : \mathbb{R} \rightarrow \mathbb{R}$ is given by $f(x) = 2 \cos(x) + 1$ and $g : \mathbb{R} \rightarrow \mathbb{R}$ is given by $g(x) = 2 \sin(x)$.

(d) $P^1(\mathbb{R}) \coprod P^2(\mathbb{R})$

10. Write the following in set builder notation:

(a) $\coprod_{n=1}^{\infty} \{x : n < x < n + 1, x \in \mathbb{R}\}$

(b) $\bigcup_{n=1}^{\infty} \{x : x > n\}$

(c) $\bigcap_{n=1}^{\infty} \{x : x > n\}$

Proof Practice

11. Use definition matching to prove the [Fiber Partition Theorem](#).

12. Write a well-written proof for the final result of [exercise 1](#) that the function is injective.

13. Write a well-written proof for the final result of [exercise 2](#) that the function is surjective.

14. Suppose that we have a function f whose domain is \mathbb{R}^2 . The nonempty fibers of f partition \mathbb{R}^2 into parallel lines of slope 2. Suppose that we have a function g whose range is $\{(x, 2x + a) : x \in \mathbb{R}, a = 1 \text{ or } 2\}$. Prove that range of $f \circ g$ has only two elements.

15. Prove that any injective map can easily be turned into a bijection by changing the codomain.

1.2.7 Solutions

1. The fibers are:

(a) $\{ (1, 0) \}$

(b) \emptyset

This function is injective. Trying various fibers they seem to either be empty or have only one element.

2. Solutions by part:

(a) $\{ (x, y, z) : x, y, z \in \mathbb{R}, z = -x - y \}$

(b) $\{ (x, y, z) : x, y, z \in \mathbb{R}, z = -x - y - 1 \}$

This function is surjective. All fibers that we try seem to be nonempty.

3. Any open interval $D \subset C$ or $D \subset \mathbb{R} \setminus (\mathbb{C} \cup \{0\})$ would do. This would guarantee that no fiber would have more than one element since we would be avoiding $f(-x) = f(x)$.

4. Solutions/hints by part:

(a) \emptyset In order for a function to be well-defined, its fibers should not overlap.

(b) $D = \{2, 3, 4, 5\}$ This is the union of all the fibers. Remember that the fibers partition the domain. So this union must be the whole domain.

(c) $\{6\}$ The element 6 is the single image of both 2 and 3.

(d) \emptyset We require that $f(D) = \{f(2), f(3), f(4), f(5)\} = \{6, 9, 11\}$. This forces $f(\{4, 5\}) = \{9, 11\}$ so that $f(4) \neq 6$ and $f(5) \neq 6$.

(e) $\{6\}$ The images of 2 and 3 are both 6.

(f) $f(D) = \{6, 9, 11\}$ We are just looking at the collection of all images of the function.

5. Solutions/hints by part:

(a) \emptyset Fibers do not overlap for well-defined functions.

(b) $\{4\}$ Note that 5 is not a possible image—it is not in the range. Therefore, it cannot come out of f . The preimage of $\{4, 5\}$ is the same as the preimage of 4. Then, everything in the preimage of 4 is sent to 4.

- (c) $f^{-1}(4) = \{3, 5, 8\}$ Realize that $f(3) = 4$.

6. Solutions/hints by part:

- (a) the domain element $(0, 0)$ has no where to go in the codomain by this definition.
 (b) $(0, 0)$

7. Solutions/hints by part:

- (a) There is not enough codomain.
 (b) Change the codomain to $[-1, 1]$

8. Solutions by part:

- (a) The solutions would live in the fiber $f^{-1}(2, 1)$ where $f : \mathbb{R}^4 \rightarrow \mathbb{R}^2$ is defined by: $f(x, y, z, w) = (2x + 3y + z + w, x - y + 5z)$.
 (b) The solutions would live in the fiber $f^{-1}(0, 1, 5)$ where $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ is defined by: $f(x, y) = (2x + 3y, x - y, 5x)$.
 (c) The solutions would live in the fiber $f^{-1}(7)$ where $f : \mathbb{R}^5 \rightarrow \mathbb{R}$ is defined by: $f(x, y, z, w, u) = 2x + 3y + z + w + u$.

9. Solutions by Part:

- (a) $\{x + yi : x, y \in \mathbb{R}, y \neq 0\}$
 (b) $\{\sum_{k=0}^n a_k x^k : n \geq 1, n \in \mathbb{Z}, a_k \in \mathbb{R} \text{ for } k = 0, 1, 2, \dots, n, a_n \neq 0\}$ We just ensure that there are no polynomials of degree 0. Writing the solution as $\{f(x) : f(x) \in \mathbb{R}[x] \setminus \mathbb{R}\}$ is still proper notation but does not emphasize the specific criteria for being in the set!
 (c) $\{y : -1 \leq y \leq 2\}$ This is the intersection of the two ranges of the functions.
 (d) $\{a_0 + a_1 x + a_2 x^2 : a_0, a_1, a_2 \in \mathbb{R}, \text{ either } a_1 \neq 0 \text{ or } a_2 \neq 0\}$

10. Solutions by Part:

- (a) $\{x : x \in \mathbb{R} \setminus \mathbb{Z}, x > 1\}$
 (b) $\{x : x \in \mathbb{R}, x > 1\}$
 (c) \emptyset : No real number is larger than every integer!

11. Think about what it means to be surjective—all fibers are nonempty. What does it mean to be a partition: a disjoint union of *nonempty* sets. We know that all of the fibers of a function are disjoint and cover all of the domain since every element in the domain has an image in order to be a function. Since none of the fibers are empty, the collection of fibers satisfy the criterion of being a partition. *Really the proof is just taking care of subtle details in the definitions.*

12. We use definition matching—think about the definition of *injective*: each fiber has at most one element. We obtain the elements of the each fiber by considering a system of equations: The fiber $f^{-1}(a, b, c)$ is obtained by finding the solutions to the system of equations:

$$\begin{aligned}x + y &= a \\x - y &= b \\2x &= c\end{aligned}$$

Notice that just solving the first two equations:

$$\begin{aligned}x + y &= a \\x - y &= b\end{aligned}$$

yields $x = \frac{a+b}{2}$ and $y = a - \frac{a+b}{2}$. So, $\left(\frac{a+b}{2}, a - \frac{a+b}{2}\right)$ is the only (x, y) pair that could possibly map to (a, b, c) . If $c = a + b$, then this (x, y) maps to (a, b, c) since this would cause $2\underbrace{\left(\frac{a+b}{2}\right)}_x = c$. Otherwise, when $c \neq a + b$, there is no (x, y) pair that could map to (a, b, c) since we need all three equations to be satisfied. Hence, $f^{-1}(a, b, c)$ has either one element or no elements. This tells us that f is injective.

13. We use definition matching—think about what it means to be *surjective*: each fiber is nonempty. Consider an arbitrary fiber $f^{-1}(c)$ for $c \in \mathbb{R}$ which is precisely the solutions of $x + y + z = c$. Notice that $(0, 0, c) \in f^{-1}(c)$. This tells us that $f^{-1}(c) \neq \emptyset$. Hence, no fiber is nonempty and the function f is surjective.

14. Notice that the range of g only touches two fibers of f : the line of slope 2 given by $y = 2x + 1$ and another line of slope 2 given by $y = 2x + 2$. Each fiber is only sent to one codomain element. Hence, the composition ends up in only two elements in the codomain of f .

15. If we make the codomain the range, then the function would be surjective. Since the function is already injective, then the function would be bijective.

Set Products, Compositions

1.3

and Inverses

1.3.1 Cartesian Products	64
1.3.2 Less Important Side Notes (optional)	66
1.3.3 Composition Diagrams	66
1.3.4 Surjective Maps, the Identity Function, and Right Inverses	69
1.3.5 Injective Maps, and Left Inverses	71
1.3.6 Exercises	76
1.3.7 Solutions	78

Questions to Guide Your Study:

- *What is a Cartesian product?*
- *What is a commutative diagram and how do we check if a diagram is commutative?*
- *What are left inverses and right inverses and how do you find them in simple situations?*

1.3.1 Cartesian Products

One very common set that you have probably used a lot is what we call a *cartesian product* of the set \mathbb{R} with itself. Namely, it is all the points in the xy -plane. The points in the xy -plane are represented by ordered pairs representing coordinate points. This allows you to easily find positions in the plane. Although the word “cartesian” comes from the mathematician Descartes’ name, one can also see it as sharing the root “cart” with “cartography,” the science of map making. Another way of writing the xy -plane is to write $\mathbb{R} \times \mathbb{R}$ or simply \mathbb{R}^2 . We use \times to signify the product between sets which may be different.

Cartesian Product between Two Sets

The cartesian product between two sets A and B is denoted as $A \times B$. It represents the collection of ordered pairs (a, b) where $a \in A$ and $b \in B$. We can write

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

We can write $A^2 = A \times A$.

Cartesian Product between Finitely Many Sets

The cartesian product $A_1 \times A_2 \times \cdots \times A_n$ represents the collection of all ordered n -tuples (a_1, a_2, \dots, a_n) such that $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$.

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) : a_k \in A_k \text{ for } k = 1, 2, \dots, n\}$$

If $A_1 = A_2 = \cdots = A_n$, then we can write the cartesian product as A^n . If \mathcal{I} is a collection of indices, then we can write:

$$\prod_{k \in \mathcal{I}} A_k$$

If \mathcal{C} is a collection of sets, we can even write:

$$\prod_{A \in \mathcal{C}} A$$

Example 1. The collection of All the points (x, y, z) in 3-space with real coordinates can be written as: \mathbb{R}^3 .

Example 2. Three-dimensional complex space can be written as \mathbb{C}^3 which represents all ordered triples (z_1, z_2, z_3) where $z_1, z_2, z_3 \in \mathbb{C}$.

Example 3. The set $\mathbb{R}^3 \times \mathbb{Z}^2$ is given as $\{(x, y, z), (w, u) : x, y, z \in \mathbb{R}, w, u \in \mathbb{Z}\}$

Example 4. The collection of all 4-tuples (a, b, c, d) of integers a, b, c, d can be written as \mathbb{Z}^4 .

Example 5. Pairing a letter in the alphabet \mathcal{A} with an integer in \mathbb{Z} gives an ordered pair (a, z) where $a \in \mathcal{A}$ and $z \in \mathbb{Z}$. The collection of all such pairs is denoted as $\mathcal{A} \times \mathbb{Z}$.

Example 6. A polynomial is equivalent to a tuple of coefficients. That is, a fourth degree polynomials $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ in $P^4(\mathbb{R})$ can be thought of as $(a_0, a_1, a_2, a_3, a_4) \in \mathbb{R}^5$. Because there is a unique polynomial for each tuple and vice versa, we obtain an injective map $P^4(\mathbb{R}) \rightarrow \mathbb{R}^5$. If we reduce the codomain of an injective map to its range, we get a bijection. Therefore, $P^4(\mathbb{R})$ is in bijection with a subset of \mathbb{R}^5 . Notice that we require $a_4 \neq 0$. This is why our map that represents these polynomials as 5-tuples is not surjective.

Therefore, there exists a bijection f such that $f(P^4(\mathbb{R})) \subset \mathbb{R}^5$.

1.3.2 Less Important Side Notes (optional)

The disjoint union \coprod is also called a set coproduct in contrast to the set product \prod . The notions satisfy a functional property which is exactly dual or reverse from each other—this is beyond our needs however!

The cartesian product $\prod_{A \in \mathcal{C}} A$ between all the sets in a collection \mathcal{C} , which collection can be infinite and even *unordered* (how do you write an unordered tuple?), can be defined as the collection of all functions $f : \mathcal{C} \rightarrow \bigcup_{A \in \mathcal{C}} A$ such that $f(A) \in A$. That is, the product is a collection of “choice functions” which choose just one element from each set among all the sets in the collection. This is the generalization of a tuple. For instance, suppose that $\mathcal{C} = \{\mathbb{R}_1, \mathbb{R}_2\}$ where \mathbb{R}_1 and \mathbb{R}_2 are two *different* copies of \mathbb{R} . Then to write an ordered pair like $(2, 3)$ is the same as making a function $f : \mathcal{C} \rightarrow \mathbb{R}_1 \cup \mathbb{R}_2$. The domain only has two elements: \mathbb{R}_1 and \mathbb{R}_2 . So we completely determine the function by their images. We can say: $f(\mathbb{R}_1) = 2 \in \mathbb{R}_1$ (taken from the first copy of \mathbb{R}) and $f(\mathbb{R}_2) = 3 \in \mathbb{R}_2$ (taken from the second copy). This function is described completely by the ordered pair $(2, 3)$. Every ordered tuple is a function. When the indexing set is too big or unordered so that it is too hard to think of tuples, we turn to the *choice function* interpretation.

1.3.3 Composition Diagrams

Sometimes we will want to visualize compositions of functions in a diagram. First, what is composition?

Composition of Two Functions

Given a function $f : D \rightarrow C$ and a function $g : C \rightarrow B$, we define $(g \circ f) : D \rightarrow B$ by the rule

$$x \mapsto g(f(x)).$$

Notice the ordering: *what we input is on the right and what we output is on the left*. Notice that it is important here that the codomain of f is the domain of g .

There is some nice, alternate notation for functions which makes thinking about compositions more intuitive:

Functions: Alternate Notation

We can write $D \xrightarrow{f} C$ instead of $f : D \rightarrow C$.

Now, if we want to think about a composition, we can draw:

$$D \xrightarrow{f} C \xrightarrow{g} B$$

and even:

$$\begin{array}{ccccc} & & g \circ f & & \\ & \nearrow & \curvearrowright & \searrow & \\ D & \xrightarrow{f} & C & \xrightarrow{g} & B \end{array}$$

The latter diagram is what we call a *commutative diagram*: one where following any *function arrow path* is the same. If we travel the top route or the bottom route, it is the same overall function (*just by the definition of composition itself.*)

Commutative Diagrams

A diagram of compositions such as

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ h \downarrow & \swarrow r & & & \downarrow j \\ D & \xrightarrow{v} & E & & \end{array}$$

is called a commutative diagram *if and only if* every arrow path between two sets represents the exact same function.

Element Chasing

In a commutative diagram we can run specific elements through the functions.



Example 7. Consider the following composition diagram:

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f} & \mathbb{R} \\ h \downarrow & & \downarrow g \\ \mathbb{R} & \xrightarrow{h} & \mathbb{R} \end{array}$$

where $f(x) = 9x$, $g(x) = 16x$, and $h(x) = 12x$. Let's determine if this diagram is commutative by element chasing:

$$\begin{array}{ccc} x & \xrightarrow{\quad} & 9x \\ \downarrow & & \downarrow \\ 12x & \xrightarrow[12 \cdot 12x]{} & 16 \cdot 9x \end{array}$$

Yes! The diagram is commutative.

Example 8. Define $\lfloor x \rfloor = \max\{y : y \leq x, y \in \mathbb{Z}\}$. Let $g : \mathbb{R} \rightarrow \mathbb{Z}$ be given by $g(x) = \lfloor x \rfloor$ and $f : \mathbb{R} \rightarrow \mathbb{R}$ be given by $f(x) = x + 7$. Consider the composition diagram:

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f} & \mathbb{R} \\ g \downarrow & & \downarrow g \\ \mathbb{Z} & \xrightarrow{f} & \mathbb{Z} \end{array}$$

Let's determine if this diagram is commutative by element chasing:

$$\begin{array}{ccc} x & \xrightarrow{\quad} & x + 7 \\ \downarrow & & \downarrow \\ \lfloor x \rfloor & \xrightarrow[\lfloor x \rfloor + 7]{} & \lfloor x + 7 \rfloor \end{array}$$

The question is:

$$\underbrace{\lfloor x + 7 \rfloor}_{\text{The floor of } 7 \text{ more than } x} \stackrel{?}{=} \underbrace{\lfloor x \rfloor + 7}_{\text{the floor of } x \text{ raised by } 7}$$

Though this may seem obvious when you think about it, let's practice a little proof by simply using definitions to restate things:

$$\lfloor x + 7 \rfloor = \max\{y : y \leq x + 7, y \in \mathbb{Z}\} = \max\{y : y - 7 \leq x, y \in \mathbb{Z}\}$$

Since $k = y - 7 \in \mathbb{Z}$ if and only if $y \in \mathbb{Z}$, then this is

$$= \max\{k + 7 : k \leq x, k \in \mathbb{Z}\} = \max\{k : k \leq x, k \in \mathbb{Z}\} + 7 \stackrel{\checkmark}{=} \lfloor x \rfloor + 7$$

where we use the idea that since 7 is constant, then $k + 7$ achieves a maximum when k does.

1.3.4 Surjective Maps, the Identity Function, and Right Inverses

Thinking about commutative diagrams, there is a nice criterion that says if a function is surjective.

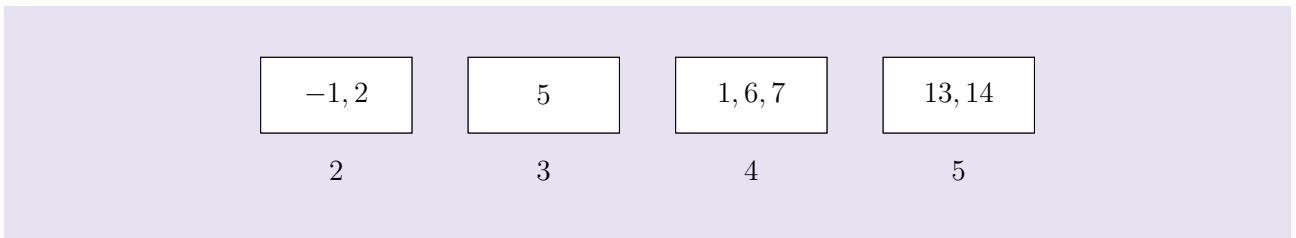
Before doing so, let's define the identity function id_S :

Identity Function

Suppose we have a set S . The identity function $\text{id}_S : S \rightarrow S$ on the set S is defined as $\text{id}_S(y) = y$ for $y \in S$.

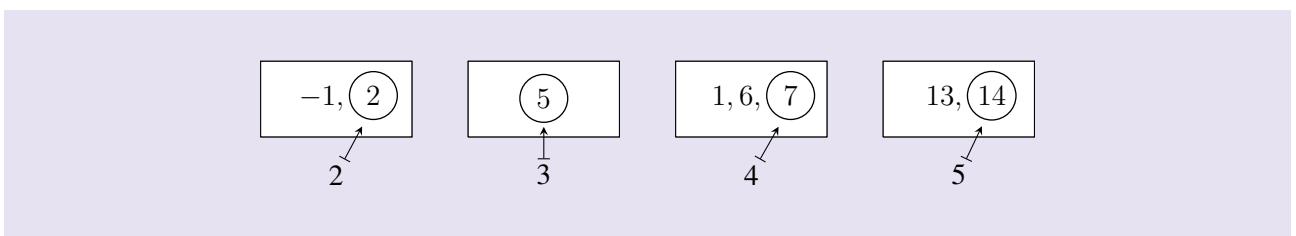
Suppose first that we have a surjective function such as in the following fiber box diagram:

A function $f : D \rightarrow C$



Since each box is nonempty, we can choose an element in each box and create a function mapping that goes *backwards* from the codomain element to what we have chosen:

A backwards mapping $g : C \rightarrow D$:

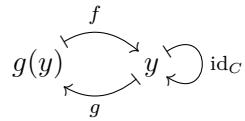


Observe that $f(g(2)) = 2$ and in general, $f(g(y)) = y$. That is, the following diagram is commutative:

$$\begin{array}{ccc} & f & \\ D & \swarrow & \curvearrowright C & \curvearrowleft id_C \\ & g & \end{array}$$

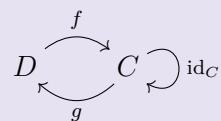
Saying that this diagram is commutative is saying that the following *element-chasing* diagram brings y back to

the same place if we follow the path $(f \circ g) : C \rightarrow C$ or the path $\text{id}_C : C \rightarrow C$.



Right Function Inverse

Given a map $f : D \rightarrow C$, any function $g : C \rightarrow D$ that makes the following diagram commute is called a *right inverse* to f .



$$\underbrace{f \circ g}_{g \text{ is on right}} = \text{id}_C$$

Theorem 1.3.1 Surjectivity by Right Inverse

A function is surjective if and only if it has a right inverse.

Proof. You get to write out a nice proof for this in the exercises! □



Example 9. The function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ given by $(x, y, z) \mapsto (x, y)$ has a right inverse $g : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ given by $(x, y) \mapsto (x, y, 0)$. One can check that

$$(f \circ g)(x, y) = f(g(x, y)) = f(x, y, 0) = (x, y)$$

so that $f \circ g = \text{id}_{\mathbb{R}^2}$. Therefore, the function f is surjective.

Example 10. In the last example we could have defined $g : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ as $(x, y) \mapsto (x, y, 1)$. This is also a right inverse and also shows that the function is surjective.

Example 11. The function $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ defined by $(x, y) \mapsto x + y$ has a right inverse $g : \mathbb{R} \rightarrow \mathbb{R}^2$ given by

$z \mapsto (z, 0)$. One can check that

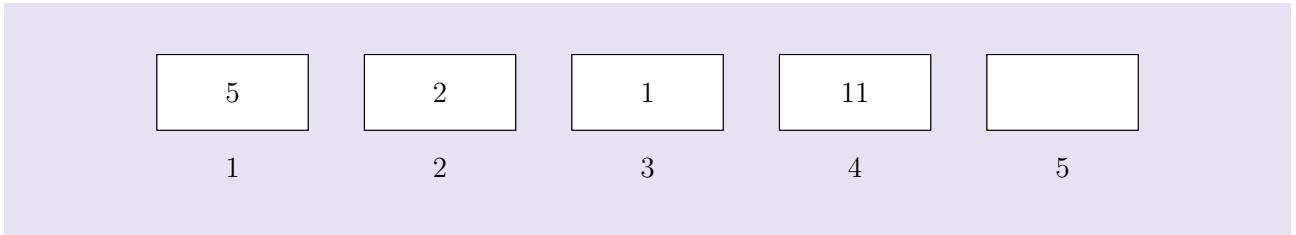
$$(f \circ g)(z) = f(g(z)) = f(z, 0) = z + 0 = z$$

so that $f \circ g = \text{id}_{\mathbb{R}}$. This shows that f is surjective.

1.3.5 Injective Maps, and Left Inverses

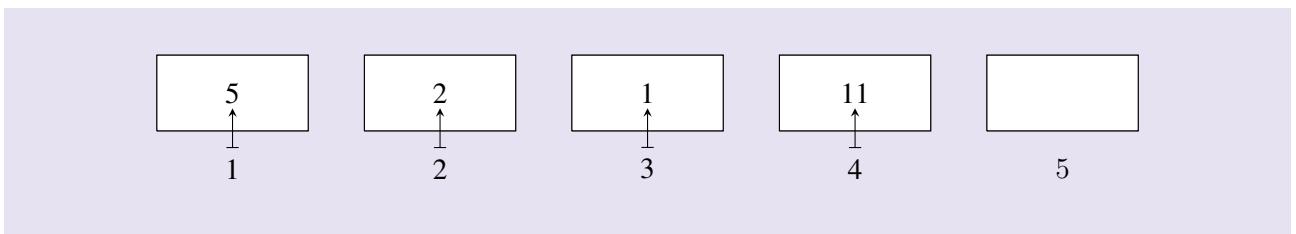
Suppose that we have an injective function such as in the following fiber box diagram:

A function $f : D \rightarrow C$



We can make a backwards map from the range $f(D)$ (the collection of images) to D :

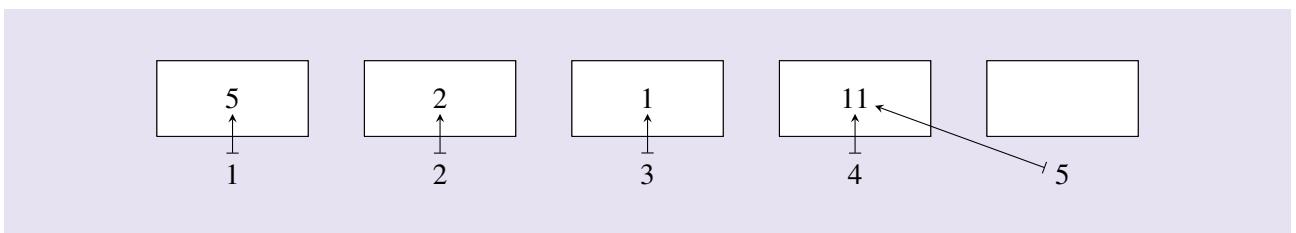
A function $g : f(D) \rightarrow D$



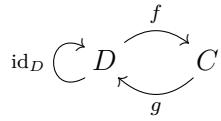
Now, extend the definition of g from the codomain element(s) under the empty fiber(s) to *anything*:

We can make a backwards map from the *full codomain C* to D :

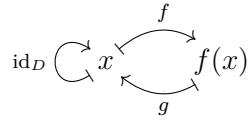
A function $g : C \rightarrow D$



Notice that $g(f(2)) = 2$ and in general, $g(f(x)) = x$. That is, $g \circ f = \text{id}_D$. We can equivalently say that the following diagram is commutative:

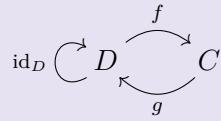


Saying that this diagram is commutative is saying that the following *element-chasing* diagram brings x back to the same place if we follow the path $(g \circ f) : C \rightarrow C$ or the path $\text{id}_C : C \rightarrow C$.



Left Function Inverse

Given a map $f : D \rightarrow C$, any function $g : C \rightarrow D$ that makes the following diagram commute is called a *left inverse* to f .



$$\underbrace{g \circ f}_{g \text{ is on left}} = \text{id}_D$$

Theorem 1.3.2 Injectivity by Left Inverse

A function is injective if and only if it has a left inverse.

Proof. You get to write out a nice proof for this in the exercises! □



Example 12. The function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ defined by $f(x, y) = (x, y, x)$ has a left inverse $g : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ given by $(x, y, z) \mapsto (x, y)$. One can check:

$$(g \circ f)(x, y) = g(f(x, y)) = g(x, y, x) = (x, y).$$

Therefore, $g \circ f = \text{id}_{\mathbb{R}^2}$. This shows that f is injective.

Example 13. The function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^4$ defined by $(x, y) \mapsto (x + y, y, 2y - x + 1, x)$ has a left inverse $g : \mathbb{R}^4 \rightarrow \mathbb{R}^2$ given by $(x, y, z, w) \mapsto (w, y)$. One can check:

$$(g \circ f)(x, y) = g(f(x, y)) = g(x + y, y, 2y - x + 1, x) = (x, y).$$

Therefore, $g \circ f = \text{id}_{\mathbb{R}^2}$. This shows that f is injective.

If a function has a right inverse and a left inverse, both of these will actually be the same and will just be what we call *the inverse* of a function.

Theorem 1.3.3 Uniqueness of Inverses for Bijective Maps

Suppose that $f : D \rightarrow C$ has a left inverse $g_L : C \rightarrow D$ and a right inverse $g_R : C \rightarrow D$. Then, $g_L = g_R$. This means that $g_L(y) = g_R(y)$ for all $y \in C$. In fact, all left inverses and right inverses are the same.

Proof. Start with:

$$f \circ g_R = \text{id}_C$$

and apply g_L on the left of both sides of this equation via composition:

$$g_L \circ f \circ g_R = g_L \circ \text{id}_C$$

$$\underbrace{(g_L \circ f)}_{\text{id}_D} \circ g_R = g_L$$

$$g_R = g_L$$

Now, this says that if g_R and h_R are both right inverses, that both are equal to g_L so that $g_R = h_R$. Similarly, if g_L and h_L are both left inverses, then $g_L = h_L$. \square

Inverse of a Function

Given a function $f : D \rightarrow C$, we define $g : C \rightarrow D$ to be the inverse of f if and only if g is both a right inverse and a left inverse for f . If it exists, it is unique.

Key Concepts from this Section

- **\times :** (page 64) We write $A \times B$ to mean the cartesian product between two sets.
- **cartesian product between two sets:** (page 64) The cartesian product between two sets A and B is denoted as $A \times B$. It represents the collection of ordered pairs (a, b) where $a \in A$ and $b \in B$. We can

write

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

We can write $A^2 = A \times A$.

- **cartesian product between finitely many sets:** (page 65) The cartesian product $A_1 \times A_2 \times \cdots \times A_n$ represents the collection of all ordered n -tuples (a_1, a_2, \dots, a_n) such that $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$.

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) : a_k \in A_k \text{ for } k = 1, 2, \dots, n\}$$

If $A_1 = A_2 = \cdots = A_n$, then we can write the cartesian product as A^n . If \mathcal{I} is a collection of indices, then we can write:

$$\prod_{k \in \mathcal{I}} A_k$$

If \mathcal{C} is a collection of sets, we can even write:

$$\prod_{A \in \mathcal{C}} A$$

- **composition of two functions:** (page 66) Given a function $f : D \rightarrow C$ and a function $g : C \rightarrow B$, we define $(g \circ f) : D \rightarrow B$ by the rule

$$x \mapsto g(f(x)).$$

Notice the ordering: *what we input is on the right and what we output is on the left. Notice that it is important here that the codomain of f is the domain of g .*

- **functions: alternate notation:** (page 67) We can write $D \xrightarrow{f} C$ instead of $f : D \rightarrow C$.
- **commutative diagrams:** (page 67) A diagram of compositions such as

$$\begin{array}{ccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ & & h \downarrow & \nearrow r & & & j \downarrow \\ D & \xrightarrow{v} & E & & & & \end{array}$$

is called a commutative diagram if and only if every arrow path between two sets represents the exact same function.

- **element chasing:** (page 67) In a commutative diagram we can run specific elements through the functions.
- **id_S :** (page 69) This is notation for the identity function on the set S
- **identity function:** (page 69) Suppose we have a set S . The identity function $\text{id}_S : S \rightarrow S$ on the set S is defined as $\text{id}_S(y) = y$ for $y \in S$.

- **right function inverse:** (page 70) Given a map $f : D \rightarrow C$, any function $g : C \rightarrow D$ that makes the following diagram commute is called a *right inverse* to f .

$$\begin{array}{ccc} & f & \\ D & \swarrow \curvearrowright & C \curvearrowright \text{id}_C \\ & g & \end{array}$$

$$\underbrace{f \circ g}_{g \text{ is on right}} = \text{id}_C$$

- **theorem 1.3.1 surjectivity by right inverse:** (page 70) A function is surjective if and only if it has a right inverse.
- **left function inverse:** (page 72) Given a map $f : D \rightarrow C$, any function $g : C \rightarrow D$ that makes the following diagram commute is called a *left inverse* to f .

$$\begin{array}{ccc} & f & \\ \text{id}_D \curvearrowright & D & \curvearrowright C \\ & \nwarrow \curvearrowright & \end{array}$$

$$\underbrace{g \circ f}_{g \text{ is on left}} = \text{id}_D$$

- **theorem 1.3.2 injectivity by left inverse:** (page 72) A function is injective if and only if it has a left inverse.
- **theorem 1.3.3 uniqueness of inverses for bijective maps:** (page 73) Suppose that $f : D \rightarrow C$ has a left inverse $g_L : C \rightarrow D$ and a right inverse $g_R : C \rightarrow D$. Then, $g_L = g_R$. This means that $g_L(y) = g_R(y)$ for all $y \in C$. In fact, all left inverses and right inverses are the same.
- **inverse of a function:** (page 73) Given a function $f : D \rightarrow C$, we define $g : C \rightarrow D$ to be the inverse of f if and only if g is both a right inverse and a left inverse for f . If it exists, it is unique.

1.3.6 Exercises

Computational Practice

1. Show that the following diagram is commutative:

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f} & \mathbb{R} \\ g \downarrow & \searrow h & \downarrow i \\ \mathbb{R} & \xrightarrow{j} & \mathbb{R} \end{array}$$

where $f(x) = \sqrt{|x|}$, $i(x) = x^4$, $h(x) = x^2$, $g(x) = x + 1$, $j(x) = (x - 1)^2$

2. Consider the following commutative diagram:

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{f} & \mathbb{Q} \\ g \downarrow & \nearrow k & \downarrow h \\ \mathbb{Q} & \xrightarrow{r} & \mathbb{Q} \end{array}$$

where $f(x) = x^2 + 1$, $h(x) = x - 2$ and $r(x) = 2x$. Determine what the functions g and k should be so that this diagram is commutative.

3. Find three left inverses for $f : \mathbb{R} \rightarrow \mathbb{R}^3$ given by $f(x) = (x^2 + 1, x - 1, x + 1)$. Conclude that f is injective.
4. Find two left inverses of $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ given by $f(x, y) = (x, x + y, 2x)$. Conclude that f is injective.
5. Find two right inverses for $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ where $f(x, y) = x - y$. Conclude that f is surjective.
6. Find two right inverses for $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ where $f(x, y, z) = (x + y, z)$. Conclude that f is surjective.

Proof Practice

7. In the text, we give an idea of why injective functions have left inverses by constructive examples. Now, prove the following direction of [The Injectivity by Left Inverse Theorem](#) in this section. That is, given $f : D \rightarrow C$ with a left inverse $g : C \rightarrow D$, prove that f is injective. Hint: just use definition matching of what it

means to be injective—take an arbitrary fiber and show that it must have one element by using the existence of the left inverse. You might want to use contradiction! Being a left inverse means...

8. Prove the following direction of [The Injectivity by Left Inverse Theorem](#): Suppose that the function $f : D \rightarrow C$ is injective. Then f has a left inverse.
9. Prove the following direction of [The Surjectivity by Right Inverse Theorem](#): Suppose that $f : D \rightarrow C$ has a right inverse $g : C \rightarrow D$. Then, f is surjective.
10. Prove the following direction of [The Surjectivity by Right Inverse Theorem](#): Suppose that $f : D \rightarrow C$ is surjective, then it has a right inverse. *Optional Note: in the solution, we assume that we can choose an element in each fiber (each of which is nonempty). The process of making such a choice is the same as applying a choice function: input a fiber and then output a chosen element in that fiber. When we find our right inverse, we are assuming the existence of a choice function—this assumption is called “the axiom of choice” in set theory.*

1.3.7 Solutions

1. Showing that the diagram is commutative amounts to verifying that $(i \circ f)(x) = h(x) = (j \circ g) = x^2$.

2. Let $k(x) = \frac{x-2}{2}$ and $g(x) = \frac{x^2-1}{2}$.

3. Some options $g_1, g_2, g_3 : \mathbb{R}^3 \rightarrow \mathbb{R}$ are: $g_1(x, y, z) = y + 1$ or $g_2(x, y, z) = z - 1$ or $g_3(x, y, z) = \frac{y+z}{2}$.

4. Some options $g_1, g_2 : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ are: $g_1(x, y, z) = (x, y - x)$ or $g_2(x, y, z) = \left(\frac{z}{2}, y - x\right)$.

5. Some options $g_1, g_2 : \mathbb{R} \rightarrow \mathbb{R}^2$ are: $g_1(x) = (x, 0)$ or $g_2(x) = (0, -x)$.

6. Some options $g_1, g_2 : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ are: $g_1(x, y) = \left(\frac{x}{2}, \frac{x}{2}, y\right)$ or $g_2(x, y) = (x - y, y, y)$.

7. Suppose that $c \in C$. Assume that $a, b \in f^{-1}(c)$ such that $a \neq b$. Then, $f(a) = f(b) = c$. We know that $g \circ f = \text{id}_D$. So apply g on the left to both sides of the equation $f(a) = f(b)$ to get: $(g \circ f)(a) = (g \circ f)(b)$ which turns into $\text{id}_D(a) = \text{id}_D(b)$ which means that $a = b$ which contradicts our original assumption. Hence, there is at most one element in each fiber $f^{-1}(c)$ for $c \in C$ so that f is injective.

8. Let a be *any* element of D . Then define $g : C \rightarrow D$ by

$$g(y) = \begin{cases} f^{-1}(y) & y \in f(D) \\ a & y \notin f(D) \end{cases}$$

This is a well-defined function. Note that $g(f(x)) = f^{-1}(f(x))$. Since f is injective, there is at most one element in the fiber over $f(x)$: namely the element x is the one and only one element in this fiber because x maps to $f(x)$ via the function f . Hence, $g(f(x)) = x$. That is, $g \circ f = \text{id}_D$ so that g is a left inverse to f .

9. Suppose that $f : D \rightarrow C$ has a right inverse $g : C \rightarrow D$. Take any $y \in C$. Then, $f(g(y)) = y$ so that $g(y)$ is in the fiber over y . Hence, the fiber over y is nonempty. This is true for all fibers over codomain elements in C . Hence, f is surjective.

10. In all of the fibers of f , choose just one element. We can do this since f is surjective so all of the fibers are nonempty. Define $g : C \rightarrow D$ by

$$g(y) = (\text{the element we chose in the fiber over } y)$$

Now,

$$f(g(y)) = f(\text{something that is in the fiber over } y) = y.$$

Hence, g is a right inverse for f .

Additive Structure on Sets and Functions

1.4

1.4.1 Set Addition	80
1.4.2 Groups	82
1.4.3 Additive Functions	85
1.4.4 Exercises	92
1.4.5 Solutions	94

Questions to Guide Your Study:

- *How do you add two sets together?*
- *What are groups and some examples of them? How do you show that something is a group?*
- *What is an additive function and how do you show that a function is additive?*
- *What is so special about the nonzero fibers of an additive function? How does this help us easily check for injectivity?*

1.4.1 Set Addition

Suppose that we take a set that has a nice addition defined on it like \mathbb{Z} . Another way of saying this is that $+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ is a well-defined function given by $+(x, y) = x + y$ or $(x, y) \mapsto x + y$. *This is the adding function—it takes a pair of integers and outputs the sum of the integers!*

If we take two subsets A and B of \mathbb{Z} , we can add them together to get another subset of \mathbb{Z} :

$$A + B = \{a + b : a \in A, b \in B\}$$



Example 1. Consider the following set addition:

$$\{1, 4, 5\} + \{2, 3\} = \{1+2, 4+2, \underbrace{5+2}_{\text{repeated}}, 1+3, \underbrace{4+3}_{\text{repeated}}, 5+3\}$$

Eliminate the repeats:

$$= \{3, 4, 6, 7, 8\}$$

Set Addition

Let S be a set with a well-defined addition between its elements. That is, there exists a well-defined addition function $+ : S \times S \rightarrow S$. Let $A, B \subset S$. Then:

$$A + B = \{a + b : a \in A, b \in B\}.$$

Adding a Set and an Element

If we want to add a set A and a one-element set $\{x\}$ together, simply write:

$$x + A$$

instead of $\{x\} + A$.

Multiplying an Element to a Set

The notation for multiplying every element of a set S by the same number k is simply $k \cdot S$ or $S \cdot k$.

Example 2. The set $5\mathbb{Z}$ is all integer multiples of 5. The set $1 + 5\mathbb{Z}$ is the set of all integers that are 1 more than a multiple of 5. *Everything in the set $5\mathbb{Z}$ has been shifted up by 1.*

Example 3. Suppose that we define multiplication of a real number k to an element $(x, y) \in \mathbb{R}^2$ as $(k \cdot x, k \cdot y)$. Then,

$$\mathbb{R} \cdot (0, 1) = \{(0, x) : x \in \mathbb{R}\}.$$

We have the following relationship which we will be using in this book:

$$\mathbb{R}^2 = \mathbb{R} \cdot (1, 0) + \mathbb{R} \cdot (0, 1).$$

Example 4. We have a relationship for \mathbb{R}^3 :

$$\mathbb{R}^3 = \mathbb{R} \cdot (1, 0, 0) + \mathbb{R} \cdot (0, 1, 0) + \mathbb{R} \cdot (0, 0, 1).$$

1.4.2 Groups

This subsection is mainly for terminology so that we can classify different types of sets—sets that are *additive* or *multiplicative groups*. These notions will become useful as we consider vector spaces in the next chapter. It will become easier to “group” the properties of *associativity*, *identity* and *inverse* together with *one* word.

Additive Group

An additive group is a set S that has a well-defined addition function $+ : S \times S \rightarrow S$ such that the addition is

- associative: this means that $(a + b) + c = a + (b + c)$ for $a, b, c \in S$. We can regroup our parentheses.
- has an additive identity. That is, there is an element that behaves 0 (called the additive identity) so that $0 + a = a + 0 = a$
- every element has an additive inverse: given $a \in S$, there is an element $b \in S$ so that $a + b = 0$. In other words, $b = -a \in S$.

Example 5. The sets \mathbb{R} , \mathbb{Z} , and \mathbb{C} are additive groups with regular addition $+$.

Example 6. The sets $P^2(\mathbb{R})$ and \mathbb{N} are *not* additive groups since they do not contain the additive identity 0.



Example 7. The set $\{0, 1, 2, 3, 4\}$ is an additive group with the following addition:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

The number 0 is the additive identity. Notice that the additive inverse of 3 is 2 since $3 + 2 = 0$.

Multiplicative Group

A multiplicative group is a set S that has a well-defined multiplication function $\bullet : S \times S \rightarrow S$ such that the multiplication is

- associative: this means that $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ for $a, b, c \in S$. We can regroup our parentheses.
- has a multiplicative identity. That is, there is an element that behaves 1 (called the multiplicative identity) so that $1 \bullet a = a \bullet 1 = a$
- every element has a multiplicative inverse: given $a \in S$, there is an element $b \in S$ so that $a \bullet b = 1$. In other words, $b = \frac{1}{a} \in S$.

Example 8. The set \mathbb{R} is not a multiplicative group since 0 does not have a multiplicative inverse.

Example 9. The set $\mathbb{R} \setminus \{0\}$ is a multiplicative group.

Example 10. The set \mathbb{N} is not a multiplicative group since no element has an inverse.

Example 11. The set $\mathbb{Q} \setminus \{0\}$ is a multiplicative group.

Example 12. The set $\{-1, 1\}$ is a multiplicative group with the normal multiplication in \mathbb{R} . The multiplicative

identity is 1. The multiplicative inverse of -1 is itself: -1 . This is the statement that $\frac{1}{-1} = -1$.

Theorem 1.4.1 Cartesian Products of Additive Groups

Suppose that A is an additive group with the operation $+_A$ and B is an additive group with the operation $+_B$. Then, $A \times B$ is an additive group if we define addition $+$ as follows. Let $(a_1, b_1), (a_2, b_2) \in A \times B$. Then:

$$(a_1, b_1) + (a_2, b_2) = (a_1 +_A a_2, b_1 +_B b_2)$$

Proof. Prove this in the exercises. Just match the definition of an additive group! □



Example 13. The set \mathbb{R}^2 is an additive group. For instance, $(2, 3) + (4, 5) = (2 + 4, 3 + 5) = (6, 8)$. The additive identity element that behaves like “0” is $(0, 0)$. Notice that we have additive inverses: $(2, 3) + (-2, -3) = (0, 0)$. Associativity follows from the associativity per component. Work this out precisely in the exercises!

Example 14. The set \mathbb{R}^3 is an additive group with additive identity $(0, 0, 0)$. We could say that $0_{\mathbb{R}^3} = (0, 0, 0)$. We can add: $(2, 3, 1) + (0, 3, -1) = (2, 6, 0)$. Notice that $(4, 5, -2)$ and $(-4, -5, 2)$ are additive inverses.

Example 15. The cartesian product $\mathbb{R}^3 \times \mathbb{R}^2$ is an additive group. The following addition takes place in this group:

$$\left((1, 2, 3), (1, 2) \right) + \left((5, 0, 3), (-1, -2) \right) = \left((6, 2, 6), (0, 0) \right)$$

Of course, there exists an obvious bijection $f : \mathbb{R}^3 \times \mathbb{R}^2 \rightarrow \mathbb{R}^5$ given by $\left((x, y, z), (w, u) \right) \mapsto (x, y, z, w, u)$. This bijection is a trivial example of an additive map (function).

Important Notational Comment

The reason why we distinguish the addition $+_A$ from $+_B$ or even the additive identities 0_A and 0_B for two different groups is because inherently the addition and the identities may be quite different. For instance, the additive identity of \mathbb{R}^2 is $(0, 0)$ but in \mathbb{R} it is just 0. Also, the way we add elements of \mathbb{R}^2 looks different from the way we add things in \mathbb{R} simply because there is more to do—in \mathbb{R}^2 , we are adding two things at a time.

Notational Convention for Group Operations

Though sometimes we label the addition $+_A$ and the additive identity 0_A with a subscript for a group A , we will *often not do so* and just understand what we mean from context. *Sometimes, the subscripts are just too much!*

Associativity Convention

We usually will not check associativity in our examples since it is often inherited from something else. A careful study of associativity is not necessary for linear algebra. For instance, \mathbb{R}^2 is an additive group with the addition $(a, b) + (c, d) = (a + c, b + d)$. Notice that the addition is done component-wise: we add in \mathbb{R} in the first component and also in the second component. The set \mathbb{R}^2 naturally inherits associativity from associativity in each component \mathbb{R} . Hence, *we will often take associativity for granted and just focus on checking the other properties.*

1.4.3 Additive Functions

In linear algebra, nearly all of the functions we will deal with are *additive*. This means that adding in the domain and *then* applying the function is *equivalent to* just applying the function and *then* adding the results in the codomain.

Additive Function

A function $f : D \rightarrow C$ where

- D has an addition $+_D$ defined between its elements
- C has an addition $+_C$ defined between its elements

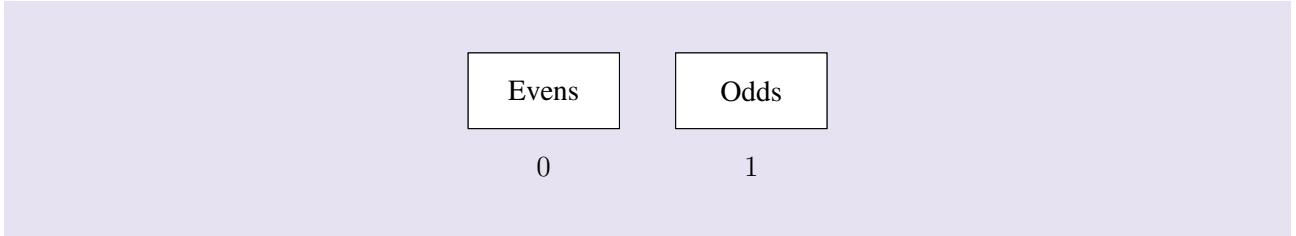
is called an *additive function* if for $x, y \in D$:

$$f(\underbrace{x +_D y}_{\text{addition in domain}}) = \underbrace{f(x) +_C f(y)}_{\text{addition in codomain}}$$

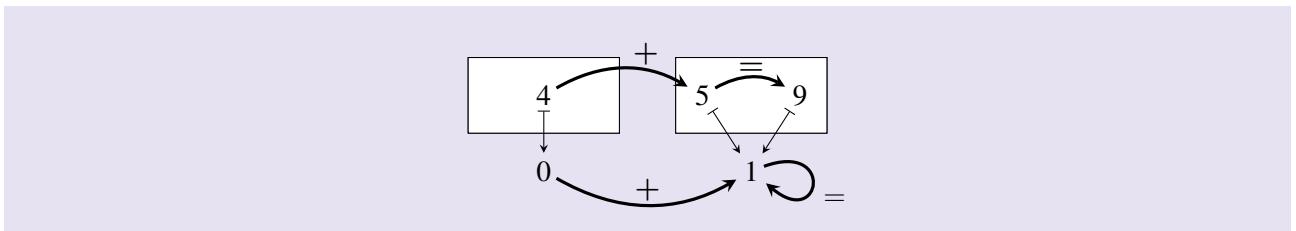
Example 16. Let's define an addition on the set $\{0, 1\}$ by the following addition table:

+	0	1
0	0	1
1	1	0

Then the function $f : \mathbb{Z} \rightarrow \{0, 1\}$ given by the following fiber box diagram is additive:

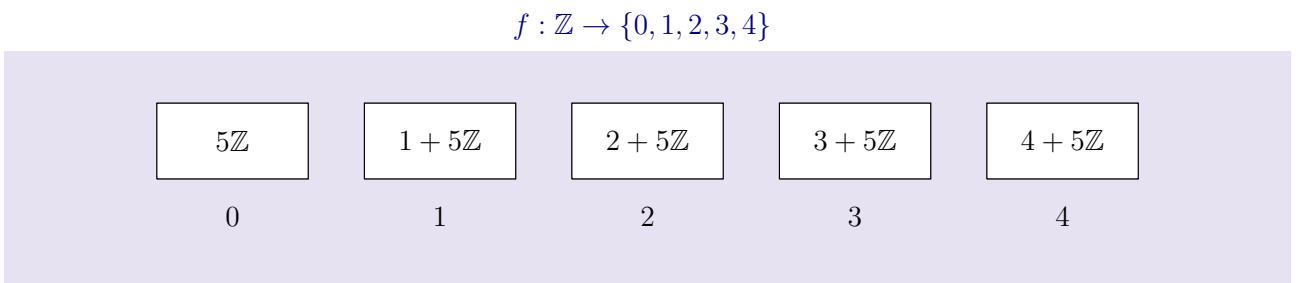


Let's visualize an *example* of what makes this function additive:



Essentially, the statement that this is an additive function is the statement that if we think of “even” as “0” and “odd” as “1,” then the rules for adding even and odd numbers together is given by the addition table we gave above on the set $\{0, 1\}$. The addition in the codomain can be determined by the addition that happens in the domain. *That is what makes an additive function additive!*

Example 17. Let $G = \{0, 1, 2, 3, 4\}$ and give it the addition structure $+$ given in [example 7](#). Then, the function given by the following fiber box diagram is additive:



This function sends all integers that are 1 more than a multiple of 5 to 1, all integers that are 2 more than a multiple of 5 to 2. The fact that this function is additive tells us that if we add any number in $1 + 5\mathbb{Z}$ to any number in $2 + 5\mathbb{Z}$, then we should get a number in $3 + 5\mathbb{Z}$.

Example 18. Define $f : \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = 4x$. Then, $f(x)$ is an additive function since

$$f\left(\underbrace{x+y}_{\text{addition in domain}}\right) = 4(x+y) = \underbrace{4x}_{f(x)} + \underbrace{4y}_{f(y)} = \underbrace{f(x)+f(y)}_{\text{addition in codomain}}$$



Example 19. The function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ defined as

$$f(x, y) = (2x + 3y, x, y)$$

is additive. To see this take two elements in the domain: $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ and compute:

$$\begin{aligned} f((x_1, y_1) + (x_2, y_2)) &= f(x_1 + x_2, y_1 + y_2) = \left(2(x_1 + x_2) + 3(y_1 + y_2), x_1 + x_2, y_1 + y_2 \right) \\ &= \left(\underbrace{(2x_1 + 3y_1) + (2x_2 + 3y_2)}_{\text{associativity of } +_{\mathbb{R}}}, (x_1) + (x_2), (y_1) + (y_2) \right) = \underbrace{(2x_1 + 3y_1, x_1, y_1)}_{f(x_1, y_1)} + \underbrace{(2x_2 + 3y_2, x_2, y_2)}_{f(x_2, y_2)} \\ &= f(x_1, y_1) + f(x_2, y_2) \end{aligned}$$

Theorem 1.4.2 Additive Functions Preserve Group Properties

Suppose that D is an additive group with addition $+_D$ and identity 0_D and C is an additive group with addition $+_C$ and identity 0_C . Suppose that $f : D \rightarrow C$ is an additive function.

- (a) $f(0_D) = 0_C$ That is, the image of an additive identity of C is the additive identity of D .
Additive identities map to additive identities:

the “0” in the domain \mapsto the “0” in codomain

- (b) $f(-a) = -f(a)$ where $-()$ means the additive inverse of $()$. That is, the image of an additive inverse of a is the additive inverse of the image of a . Additive inverses map to additive inverses:

additive inverse in domain \mapsto additive inverse in codomain

Proof. (a) Let $a \in D$ such that $a \neq 0_D$. Notice that $f(a) = f(a + 0_D) = f(a) + f(0_D)$ Therefore, if we add both sides of this equation by the additive inverse $-f(a)$ of $f(a)$, we see: $f(a) - f(a) = f(0_D)$ which becomes $0_C = f(0_D)$.

- (b) Using (a), notice that $0_C = f(0_C) = f(a + (-a)) = f(a) + f(-a)$ which automatically tells us that $f(-a)$ is the additive inverse of $f(a)$. Therefore, we can write $f(-a) = -f(a)$.

□

One of the most fundamental ideas that we will be using about fibers of additive functions between additive groups in linear algebra is that all of the fibers are just *shifts of the fiber over 0*. This makes it a lot easier to think about and work with these functions! Here is the result:

Theorem 1.4.3 Additive Group Fibers

Suppose that D is an additive group with addition $+_D$ and C is an additive group with addition $+_C$. Suppose that $f : D \rightarrow C$ is an additive function. Then if 0_C is the additive identity of C , then all of the fibers of f look like this:

$$f^{-1}(y) = \underbrace{t + f^{-1}(0_C)}_{\text{Set Addition}}$$

where t is *any* element of $f^{-1}(y)$.

Proof. We approach this proof by showing two directions: if $w \in f^{-1}(y)$, then $w \in t + f^{-1}(0_C)$. Then we show that if $w \in t + f^{-1}(0_C)$, then $w \in f^{-1}(y)$. First, if $w \in f^{-1}(y)$, then $f(w) = y$. We know that $t \in f^{-1}(y)$ so that $f(t) = y$. Therefore,

$$f(w - t) = f(w + (-t)) = f(w) + f(-t) = f(w) - f(t) = y - y = 0.$$

So, $w - t \in f^{-1}(0)$ which means that $w \in t + f^{-1}(0)$.

Now assume that $w \in t + f^{-1}(0_C)$. This means that $w = t + k$ where $k \in f^{-1}(0)$ which means that $f(k) = 0$. Therefore,

$$f(w) = f(t + k) = f(t) + f(k) = y + 0 = y$$

so that $w \in f^{-1}(y)$. □

Example 20. Suppose that $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ is defined as $f(x, y) = x + y$. The reader should verify that this function is additive. Consider the following fibers:

- $A = f^{-1}(0) = \{(x, y) : (x, y) \in \mathbb{R}^2, y = -x\} = \{(x, -x) : x \in \mathbb{R}\}$
- $B = f^{-1}(1) = \{(x, y) : (x, y) \in \mathbb{R}^2, y = -x + 1\} = \{(x, -x + 1) : x \in \mathbb{R}\}$
- $C = f^{-1}(2) = \{(x, y) : (x, y) \in \mathbb{R}^2, y = -x + 2\} = \{(x, -x + 2) : x \in \mathbb{R}\}$

Now look at the set addition $A + \{(0, 1)\}$ which notationally can be written as $A + (0, 1)$:

$$A + (0, 1) = \{(x, -x) + (0, 1) : x \in \mathbb{R}\} = \{(x, -x + 1) : x \in \mathbb{R}\} = B$$

Similarly,

$$A + \{(0, 2)\} = C$$

Every fiber is an additive shift of A = f⁻¹(0).

Suppose that we would like to check to see if an additive function $f : D \rightarrow C$ is injective or not. To be injective, the function should only have precisely one element in each fiber. All fibers are just additive shifts by a single element a to the set $f^{-1}(0_C)$. In order for the set addition $a + f^{-1}(0_C)$ to result in a set with a single element, the set $f^{-1}(0_C)$ must have only one element.

Theorem 1.4.4 Zero Fiber Check for Injectivity

To see if an additive function $f : D \rightarrow C$ is injective, one *only* needs to check the fiber over 0_C .



Example 21. The reader is welcome to check that the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ given by

$$f(x, y) = (x + y, x - y, x)$$

is additive. Then to show that this function is injective, it suffices just to check to see if the fiber

$$f^{-1}(0_{\mathbb{R}^3}) = f^{-1}(0, 0, 0)$$

only has one element. This fiber is all of the solutions to the system of equations:

$$\begin{aligned} x + y &= 0 \\ x - y &= 0 \\ x &= 0 \end{aligned}$$

The reader is invited to check that the only solution to this system is $(x, y) = (0, 0)$. Hence, since the fiber over $0_{\mathbb{R}^3}$ only has one element, all the other fibers do too. This function is injective. This function, therefore, has a left inverse $g : \mathbb{R}^3 \rightarrow \mathbb{R}^2$. Yet, the question remains if there exists a left inverse g that is an additive function too. The answer is yes! But this is for a later time and even the applications of such an idea will need to wait—but they will come!

Key Concepts from this Section

- **set addition:** (page 81) Let S be a set with a well-defined addition between its elements. That is, there

exists a well-defined addition function $+ : S \times S \rightarrow S$. Let $A, B \subset S$. Then:

$$A + B = \{a + b : a \in A, b \in B\}.$$

- **adding a set and an element:** (page 81) If we want to add a set A and a one-element set $\{x\}$ together, simply write:

$$x + A$$

instead of $\{x\} + A$.

- **multiplying an element to a set:** (page 81) The notation for multiplying every element of a set S by the same number k is simply $k \cdot S$ or $S \cdot k$.
- **associativity:** (page 82) An operation \star is associative if we can regroup with parentheses: $(a \star b) \star c = a \star (b \star c)$.
- **identity:** (page 82) An operation \star has an identity ℓ if $\ell \star a = a \star \ell = a$ for all a in the set under consideration.
- **inverse:** (page 82) An element a has an inverse b with respect to the operation \star if $a \star b = b \star a = \ell$ if ℓ is the identity with respect to \star .
- **additive group:** (page 82) An additive group is a set S that has a well-defined addition function $+ : S \times S \rightarrow S$ such that the addition is
 - associative: this means that $(a + b) + c = a + (b + c)$ for $a, b, c \in S$. We can regroup our parentheses.
 - has an additive identity. That is, there is an element that behaves 0 (called the additive identity) so that $0 + a = a + 0 = a$
 - every element has an additive inverse: given $a \in S$, there is an element $b \in S$ so that $a + b = 0$. In other words, $b = -a \in S$.
- **multiplicative group:** (page 83) A multiplicative group is a set S that has a well-defined multiplication function $\bullet : S \times S \rightarrow S$ such that the multiplication is
 - associative: this means that $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ for $a, b, c \in S$. We can regroup our parentheses.
 - has an multiplicative identity. That is, there is an element that behaves 1 (called the multiplicative identity) so that $1 \bullet a = a \bullet 1 = a$
 - every element has a multiplicative inverse: given $a \in S$, there is an element $b \in S$ so that $a \bullet b = 1$. In other words, $b = \frac{1}{a} \in S$.

- **theorem 1.4.1 cartesian products of additive groups:** (page 84) Suppose that A is an additive group with the operation $+_A$ and B is an additive group with the operation $+_B$. Then, $A \times B$ is an additive group if we define addition $+$ as follows. Let $(a_1, b_1), (a_2, b_2) \in A \times B$. Then:

$$(a_1, b_1) + (a_2, b_2) = (a_1 +_A a_2, b_1 +_B b_2)$$

- **additive function:** (page 85) A function $f : D \rightarrow C$ where

- D has an addition $+_D$ defined between its elements
- C has an addition $+_C$ defined between its elements

is called an *additive function* if for $x, y \in D$:

$$f\left(\underbrace{x +_D y}_{\text{addition in domain}}\right) = \underbrace{f(x) +_C f(y)}_{\text{addition in codomain}}$$

- **theorem 1.4.2 additive functions preserve group properties:** (page 87) Suppose that D is an additive group with addition $+_D$ and identity 0_D and C is an additive group with addition $+_C$ and identity 0_C . Suppose that $f : D \rightarrow C$ is an additive function.

- (a) $f(0_D) = 0_C$ That is, the image of an additive identity of C is the additive identity of D . Additive identities map to additive identities:

the “0” in the domain \mapsto the “0” in codomain

- (b) $f(-a) = -f(a)$ where $-()$ means the additive inverse of $()$. That is, the image of an additive inverse of a is the additive inverse of the image of a . Additive inverses map to additive inverses:

additive inverse in domain \mapsto additive inverse in codomain

- **theorem 1.4.3 additive group fibers:** (page 88) Suppose that D is an additive group with addition $+_D$ and C is an additive group with addition $+_C$. Suppose that $f : D \rightarrow C$ is an additive function. Then if 0_C is the additive identity of C , then all of the fibers of f look like this:

$$f^{-1}(y) = \underbrace{t + f^{-1}(0_C)}_{\text{Set Addition}}$$

where t is *any* element of $f^{-1}(y)$.

- **theorem 1.4.4 zero fiber check for injectivity:** (page 89) To see if an additive function $f : D \rightarrow C$ is injective, one *only* needs to check the fiber over 0_C .

1.4.4 Exercises

Computation Practice

- 1.** Suppose that you know that $(1, 1, 2)$ is a solution to the following system of equations:

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

Use the fact that the function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ given by $f(x, y, z) = (x + y + z, x - y + 2z)$ is additive to find *all* the solutions to this system of equations by realizing that

$$f^{-1}(4, 4) = (1, 1, 2) + f^{-1}(0, 0).$$

The set of all solutions should be expressed in set builder notation. Try to express everything in terms of z where $z \in \mathbb{R}$.

- 2.** Perform the following set additions:

(a) $\{1, 0, 3\} + \{1, 2\}$

(b) $5 + 2 \cdot \{3, 5, 1\}$

(c) $2 \cdot \{1, 1\} + \{1, -1\}$

- 3.** Show that the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ where $f(x, y) = (x + y, x - y)$ is injective by finding all the solutions in $f^{-1}(0, 0)$.

- 4.** Show that the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^4$ where $f(x, y) = (x + y, x - y, x, x)$ is injective by finding all the solutions in $f^{-1}(0, 0, 0, 0)$.

- 5.** Show that the function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ where $f(x, y, z) = (x + y + z, z - y)$ is not injective by looking at $f^{-1}(0, 0)$.

- 6.** Show that the function $f : \mathbb{R}^4 \rightarrow \mathbb{R}^2$ where $f(x, y, z, w) = (x + y, z + w)$ is not injective by looking at $f^{-1}(0, 0)$.

Proof Practice

7. Prove that $\mathbb{R}^3 = \mathbb{R} \cdot (1, 1, 0) + \mathbb{R} \cdot (0, 1, 1) + \mathbb{R} \cdot (0, 0, 1)$. *Hint: remember the logical equivalence ideas that we have for proofs. Show that if an element is in the set on the left, then it is in the set on the right and then if it is in the set on the right then it is in the set on left.*
8. Use definition matching to prove the [Cartesian Products of Additive Groups Theorem](#), if we assume that the addition defined is well-defined on the Cartesian Product. (*Check all properties—even associativity.*)
9. Prove that the following function is additive: $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ where $f(x, y) = (2x, 3x + y)$
10. Prove that the following function is additive: $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ where $f(x, y) = x + y$
11. Prove that $\mathbb{R}^2 \setminus (0, 0)$ **is not** a multiplicative group under component-wise multiplication: $(a, b) \cdot (c, d) = (ac, bd)$. *Hint: find an element that does not have an inverse.*

1.4.5 Solutions

- 1.** In other words, we just add $(1, 1, 2)$ to all solutions of:

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

Adding the equations, we have $2x + 3z = 0$ so that $x = -\frac{3}{2}z$. Plugging this into the top equation, we can solve for x in terms of z : $-\frac{3}{2}z + y + z = 0$ so that $y = \frac{1}{2}z$. Therefore,

$$f^{-1}(0, 0) = \left\{ \left(-\frac{3}{2}z, \frac{1}{2}z, z \right) : z \in \mathbb{R} \right\}$$

Hence, the solutions are:

$$f^{-1}(4, 4) = (1, 1, 2) + \left\{ \left(-\frac{3}{2}z, \frac{1}{2}z, z \right) : z \in \mathbb{R} \right\} = \left\{ \left(-\frac{3}{2}z + 1, \frac{1}{2}z + 1, z + 2 \right) : z \in \mathbb{R} \right\}$$

- 2.** Solutions by parts:

(a) $\{1, 0, 3\} + \{1, 2\} = \{2, 1, 4, 3, 5\}$

(b) $5 + 2 \cdot \{3, 5, 1\} = \{11, 15, 7\}$

(c) $2 \cdot \{1, -1\} + \{1, -1\} = \{3, -1, 1, -3\}$

- 3.** The only solution (i.e. element of $f^{-1}(0, 0)$) is $(0, 0)$. Hence, all fibers only have one element.

- 4.** The only solution (i.e. element of $f^{-1}(0, 0, 0, 0)$) is $(0, 0)$. Hence, all fibers only have one element.

- 5.** Notice that $(0, 0, 0)$ and $(-2, 1, 1)$ are both in $f^{-1}(0, 0)$. Hence, the function cannot be injective.

- 6.** Notice that $(0, 0, 0, 0)$ and $(1, -1, 1, -1)$ are both in $f^{-1}(0, 0)$. Hence, the function cannot be injective.

- 7.** First suppose that $(x, y, z) \in \mathbb{R}^3$. The set on the right can be written in set builder notation as:

$$\{a \cdot (1, 1, 0) + b \cdot (0, 1, 1) + c \cdot (0, 0, 1) : a, b, c \in \mathbb{R}\} = \{(a, a+b, b+c) : a, b, c \in \mathbb{R}\}.$$

Therefore, we need to show that there are a , b , and c such that $x = a$, $y = a + b$ and $z = b + c$. Well, we can let $a = x$. Then $b = y - a = y - x$ and $c = z - b = z - (y - x)$ so that we can find a , b , and c that really do give the x , y , and z that we are interested in. Notice that $(a, a + b, b + c) \in \mathbb{R}^3$ for sure so that the other direction is automatically take care of.

8. Assuming that the addition is well-defined, we simply need to show that the addition is associative, has an identity and inverses. Note that $(a, b) + (0_A, 0_B) = (a +_A 0_A, b +_B 0_B) = (a, b)$ so that $(0_A, 0_B)$ is the additive identity. Further, $(a, b) + (-a, -b) = (a +_A -a, b +_B -b) = (0_A, 0_B)$ so that every element has an additive inverse. To show associativity, we consider:

$$\begin{aligned} ((a, b) + (c, d)) + (e, f) &\stackrel{?}{=} (a, b) + ((c, d) + (e, f)) \\ (a +_A c, b +_B d) + (e, f) &\stackrel{?}{=} (a, b) + (c +_A e, d +_B f) \\ (a +_A c +_A e, b +_B d +_B f) &\stackrel{\checkmark}{=} (a +_A c +_A e, b +_B d +_B f) \end{aligned}$$

9. We let (x_1, y_1) and (x_2, y_2) be two points in the domain. We simply verify the condition for being an additive function:

$$\begin{aligned} f((x_1, y_1) + (x_2, y_2)) &= f(x_1 + x_2, y_1 + y_2) = \left(2x_1 + 2x_2, 3x_1 + 3x_2 + y_1 + y_2 \right) \\ &= (2x_1, 3x_1 + y_1) + (2x_2, 3x_2 + y_2) = f(x_1, y_1) + f(x_2, y_2). \end{aligned}$$

10. We let (x_1, y_1) and (x_2, y_2) be two points in the domain. We simply verify the condition for being an additive function:

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

11. This is a proof by counterexample. Notice that multiplication by $(1, 1)$ is a multiplicative identity. We find an element that does not have an inverse: $(0, 2)$. This is because $(a, b) \cdot (0, 2) = (0, 2b)$. *We can never get $(1, 1)$ when multiplying $(0, 2)$ by any (a, b) .*

Chapter 1 Selected Review Questions

Section 1.1

Can you properly construct and work out a proof by induction?

1. Prove by induction that every number of the form $n^{11} - n$ where n is a positive integer is divisible by 11. Use the following fact: If p is a prime number, then:

$$(n + 1)^p = n^p + (\text{terms where the coefficients are all multiples of } p) + 1.$$

2. Prove by induction that every element of the form $73^n - 1$ is divisible by 72 for all positive integers n .

Can you properly construct and work out a proof by contradiction?

3. Prove by contradiction that there are no integers x and y such that $3x + 6y = 1$.

You should be able to properly construct and work out a proof that shows that two sets are the same:

4. Let A be the set of numbers of the form $3k + 1$ where k is an integer and let B be the set of numbers of the form $3k + 10$ where k is an integer. Prove that $A = B$.

Section 1.2

Can you find a fiber of a function via a system of equations and understand what the terms injective and surjective mean as you look at the fibers?

5. Suppose that $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ is given by $f(x, y) = (x + 2y, x - y, 2x)$. Determine what the following fibers are:

(a) $f^{-1}(3, 0, 2)$

(b) $f^{-1}(3, 0, 1)$

Do you think this function is injective, surjective or neither? Explain your reasoning.

- 6.** Suppose that $f : \mathbb{R}^3 \rightarrow \mathbb{R}$ is given by $f(x, y, z) = y - x$. Write the following fibers in set builder notation:

(a) $f^{-1}(0)$

(b) $f^{-1}(1)$

Do you think this function is injective, surjective or neither? Explain your reasoning.

Can you properly construct and work out a proof that shows a function is either injective or surjective?

- 7.** Write a well-written proof for the final result of [exercise 5](#) that the function is injective.

- 8.** Write a well-written proof for the final result of [exercise 6](#) that the function is surjective.

Section 1.3

Do you understand what a commutative diagram is and how to use it to help you determine a missing function?

- 9.** Consider the following commutative diagram:

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{f} & \mathbb{Q} \\ g \downarrow & \swarrow k & \downarrow h \\ \mathbb{Q} & \xrightarrow{r} & \mathbb{Q} \end{array}$$

where $f(x) = x + 1$, $h(x) = x - 2$ and $r(x) = 2x$. Determine what the functions g and k should be so that this diagram is commutative.

Do you understand what it means to be a left and a right inverse and know how to find some for either an injective or a surjective function? Do you remember that having a right inverse is the same things as surjectivity and that having a left inverse is the same thing as injectivity?

- 10.** Find three left inverses for $f : \mathbb{R} \rightarrow \mathbb{R}^3$ given by $f(x) = (\sin(x), x - 5, x + 1)$. Conclude that f is injective.

- 11.** Find two right inverses for $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ where $f(x, y) = 2x + 2y$. Conclude that f is surjective.

Section 1.4

Can you add two sets together?

12. Perform the following set additions:

(a) $\{1, 0, 3\} + \{1, 3\}$

(b) $1 + 2 \cdot \{3, 5, 1, 2\}$

Can you prove that a function is additive?

13. Prove that the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ given by $f(x, y) = 2x + y$ is additive.

You should be able to identify if an additive function is injective or not by considering its fiber over the additive identity (i.e. zero) of the codomain:

14. Show that the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^5$ where $f(x, y) = (x + 2y, x - y, 3x, y, x)$ is injective by finding all the solutions in $f^{-1}(0, 0, 0, 0, 0)$.

15. Show that the function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ where $f(x, y, z) = (x+y, z)$ is not injective by looking at $f^{-1}(0, 0)$.

You should understand what properties a set must satisfy to be a group:

16. Prove that $\mathbb{R}^2 \setminus (0, 0)$ *is not a multiplicative group* under component-wise multiplication: $(a, b) \cdot (c, d) = (ac, bd)$. Hint: find an element that does not have an inverse.

Solutions/Hints

- 1.** In the following proof, we let $p = 11$. Base Case when $n = 1$: $1^p - 1 = 0$ which is divisible by p . Induction Step: assume that $n^p - n$ is divisible by p . Then, consider $(n + 1)^p - (n + 1)$. The fact we are allowed to use tells us:

$$\underbrace{n^p + (\text{multiple of } p) + 1 - (n + 1)}_{(n+1)^p}$$

Then further, we use the *induction hypothesis* which is that $n^p - n$ is divisible by p :

$$= n^p - n + (\text{multiple of } p) + 1 - 1 = \underbrace{(n^p - n)}_{\text{divisible by } p} + \underbrace{(\text{multiple of } p)}_{\text{divisible by } p}.$$

Therefore, $(n + 1)^p - (n + 1)$ is divisible by p since we can factor p out of the sum that we have obtained so far.

- 2.** Base case when $n = 1$: $1^n - 1 = 0$ which is divisible by 72. Induction Step: Assume that $73^n - 1$ is divisible by 72. Now we try to show that this implies that $73^{n+1} - 1$ is divisible by 72. To do so, we try to turn $73^n - 1$ into $73^{n+1} - 1$ via multiplication and addition that will maintain divisibility by 72 of the expression. We can write:

$$73 \cdot \underbrace{(73^n - 1)}_{\text{divisible by 72}} = \underbrace{73^{n+1} - 73}_{\text{divisible by 72}}$$

So if we add 72, we still will have a multiple of 72:

$$73^{n+1} - 73 + (72) = 73^{n+1} - 1.$$

Therefore, we are done with the induction step.

- 3.** By way of contradiction, assume that there are integers x and y such that $3x + 6y = 1$. Then, $3x + 6y$ is an integer which is a multiple of 3. But this multiple of 3 is equal to 1. This means that 1 is a multiple of 3. But it is not. This is a contradiction.

- 4.** If x is in A , then we can write $x = 3k + 1$ for some integer k . We write:

$$\begin{aligned} x &= 3k + \underbrace{(10 - 10)}_0 + 1 = (3k - 10 + 1) + 10 \\ &= (3k - 9) + 10 = 3\underbrace{(k - 3)}_{\text{an integer}} + 10. \end{aligned}$$

Hence, x satisfies the defining characteristic of the set B . Therefore, x is in B .

Now, if x is B , then $x = 3j + 10$ for some integer j . Then, write

$$x = 3j + 10 = 3j + \underbrace{(9 - 9)}_0 + 10 = (3j + 9) + (-9 + 10) = 3\underbrace{(j + 3)}_{\text{an integer}} + 1$$

so that x satisfies the defining characteristic of A . Therefore, x is in A .

This shows that the two sets A and B are the same.

5. The fibers are:

(a) $\{(1, 1)\}$

(b) \emptyset

This function is injective. Trying various fibers they seem to either be empty or have only one element.

6. Solutions by part:

(a) $\{(x, y, z) : x, y, z \in \mathbb{R}, x = y\}$

(b) $\{(x, y, z) : x, y, z \in \mathbb{R}, y = x + 1\}$

This function is surjective. All fibers that we try seem to be nonempty.

7. We use definition matching—think about the definition of *injective*: each fiber has at most one element. We obtain the elements of the each fiber by considering a system of equations: The fiber $f^{-1}(a, b, c)$ is obtained by finding the solutions to the system of equations:

$$\begin{aligned} x + 2y &= a \\ x - y &= b \\ 2x &= c \end{aligned}$$

Notice that just solving the first two equations:

$$\begin{aligned} x + 2y &= a \\ x - y &= b \end{aligned}$$

yields $x = \frac{a-b}{3} + b$ and $y = \frac{a-b}{3}$. So, $\left(\frac{a-b}{3} + b, \frac{a-b}{3}\right)$ is the only (x, y) pair that could possibly map to (a, b, c) . If $c = 2\left(\underbrace{\frac{a-b}{3} + b}_x\right)$, then this (x, y) maps to (a, b, c) . Otherwise, when c is not equal to this expression, there is no (x, y) pair that could map to (a, b, c) since we need all three equations to be satisfied. Hence, $f^{-1}(a, b, c)$ has either one element or no elements. This tells us that f is injective.

8. We use definition matching—think about what it means to be *surjective*: each fiber is nonempty. Consider an arbitrary fiber $f^{-1}(c)$ for $c \in \mathbb{R}$ which is precisely the solutions of $y - x = c$. Notice that $(0, c, 0) \in f^{-1}(c)$. This tells us that $f^{-1}(c) \neq \emptyset$. Hence, no fiber is nonempty and the function f is surjective.

9. Let $k(x) = \frac{x-2}{2}$ and $g(x) = \frac{x-1}{2}$.

10. Some options $g_1, g_2, g_3 : \mathbb{R}^3 \rightarrow \mathbb{R}$ are: $g_1(x, y, z) = y + 5$ or $g_2(x, y, z) = z - 1$ or $g_3(x, y, z) = \frac{y+z+4}{2}$.

11. Some options $g_1, g_2 : \mathbb{R} \rightarrow \mathbb{R}^2$ are: $g_1(x) = (\frac{x}{2}, 0)$ or $g_2(x) = (0, \frac{x}{2})$.

12. Solutions by parts:

$$(a) \{1, 0, 3\} + \{1, 3\} = \{2, 0, 4, 3, 6\}$$

$$(b) 1 + 2 \cdot \{3, 5, 1\} = \{7, 11, 3, 5\}$$

13. Just compare both sides of the following equation:

$$f((a, b) + (c, d)) \stackrel{?}{=} f(a, b) + f(c, d)$$

$$f(a+c, b+d) \stackrel{?}{=} 2a + b + 2c + d$$

$$f(a+c, b+d) \stackrel{?}{=} 2(a+c) + (b+d)$$

$$2(a+c) + (b+d) \stackrel{?}{=} 2(a+c) + (b+d)$$

14. The only solution (i.e. element of $f^{-1}(0, 0, 0, 0, 0)$) is $(0, 0)$. Hence, all fibers only have one element. You could also find a left inverse to accomplish the task as well: $(x, y, z, w, r) \mapsto (r, w)$.

15. Notice that $(0, 0, 0)$ and $(1, -1, 0)$ are both in $f^{-1}(0, 0)$. Hence, the function cannot be injective.

16. This is a proof by counterexample. Notice that multiplication by $(1, 1)$ is a multiplicative identity. We find an element that does not have an inverse: $(0, 2)$. This is because $(a, b) \cdot (0, 2) = (0, 2b)$. *We can never make the first component 1.*

Linear Transformations

2

Vector Spaces and Their Subspaces

2.1

2.1.1 Fields of Scalars	105
2.1.2 Vector Spaces	106
2.1.3 Subspaces and Spans	108
2.1.4 Quotient Vector Spaces	114
2.1.5 Function Vector Spaces	116
2.1.6 Rings and Modules	117
2.1.7 Exercises	121
2.1.8 Solutions	124

Questions to Guide Your Study:

- *What are vectors, scalars and how do they add and interact?*
- *What are some simple examples of vector spaces?*
- *What properties must a set have to be a vector space?*
- *What is a subspace of a vector space?*
- *What are some simple examples of subspaces?*
- *What do the words span and linear combination mean?*
- *What is a basis of a vector space?*
- *What is the dimension of a vector space?*

You have probably heard people talk about vectors as arrows or things with magnitude and direction. But the truth is—these do not tell the whole story. These are only examples of vectors. But the story goes a lot deeper and what vectors are goes much deeper. They can be positions in a tick tack toe game or color configurations on a board. They could even be infinite stacks of objects, functions, polynomials, series, integrals, and much, much more. From concrete to abstract, vectors are lurking around every corner. Sometimes they are

arrows. But often they are not. The methods and laws that govern arrows also govern them. In this text, I hope to open your eyes to a fascinating process of “morphing vectors until you see what you are looking for.”

2.1.1 Fields of Scalars

Simply, a vector space is a space where vectors live, or a set that contains vectors that allows certain movement of those vectors. We want this space to be an additive group—and we want the space to contain all possible “rescalings” of the vectors. We want “rescaling” to work compatibly with addition and we want that rescaling to be reversible. That being said, the set of possible rescalings, or **scalars**, called the (*commutative*) field of scalars needs to take on a certain flavor:

Field

A field is a set S with the following properties:

- S itself is an additive group with respect to $+$ with an additive identity 0.
- $S \setminus \{0\}$ forms a multiplicative group with a multiplicative identity 1.
- Multiplication is “ringed” over addition with in S : *multiplication distributes over addition*:
 $a \cdot (b + c) = a \cdot b + a \cdot c$.
- For our purposes, we assume that both the addition $+$ and the multiplication \cdot are *commutative*: $a \cdot b = b \cdot a$ and $a + b = b + a$ so that the order we write it does not matter.

Example 1. The sets \mathbb{R} , \mathbb{C} and \mathbb{Q} are all fields and perfectly acceptable places from which to take scalars.

Example 2. The set \mathbb{Z} is not a field since $\mathbb{Z} \setminus \{0\}$ is not a multiplicative group—most elements do not have inverses! For instance, $\frac{1}{2}$ is the multiplicative inverse of 2 but $\frac{1}{2} \notin \mathbb{Z}$.

Example 3. Take the set $F = \{0, 1, 2, 3, 4\}$ and define:

- $a + b = \text{remainder of } (a + b) \div 5$
- $a \cdot b = \text{remainder of } (a \cdot b) \div 5$

These operations make F into a field—a *finite field!* There are plenty of finite vectors spaces whose scalars live in finite fields. Linear algebra techniques work perfectly well here too!

Finite Fields \mathbb{F}_p

Define the finite field \mathbb{F}_p for a prime p to be the set $\{0, 1, 2, \dots, p - 1\}$ where

- $a + b = \text{remainder of } (a + b) \div p$
- $a \cdot b = \text{remainder of } (a \cdot b) \div p$

Then, \mathbb{F}_p is a field.

Example 4. The field $\mathbb{F}_2 = \{0, 1\}$ allows us to study vectors spaces that have binary representations—and are useful for signal transmissions. The linear algebra done with such vector spaces is done completely with 0's and 1's.

2.1.2 Vector Spaces



Video

What are vectors? Anything that lives in a vector space. So what is a vector space?

Vector Space

A F -vector space is an additive commutative group V . The elements of the field F can “rescale” the elements (vectors) of the set V . But this must be done compatibly with the addition in V .

Particularly, for any scalars $k, r \in F$ and any vectors $u, v \in V$:

- $k \cdot (v + u) = k \cdot v + k \cdot u$ (Rescaling before or after addition is the same.)
- $(k + r) \cdot v = k \cdot v + r \cdot v$ (Addition of scalars applied to a vector becomes the addition of the two scaled versions of that vector.)
- $k \cdot v \in V$ (The action of F keeps things inside of V .)
- $k \cdot (r \cdot v) = (k \cdot r) \cdot v$ (“Associativity” mixes between F and V .)

Additive Identity

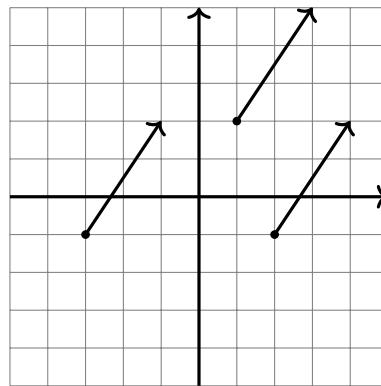
The additive identity of a vector space V is often denoted by 0_V .

Example 5. The set \mathbb{R}^2 is a \mathbb{R} -vector space with the addition $(a, b) + (c, d) = (a + c, b + d)$ and scalar multiplication $k \cdot (a, b) = (k \cdot a, k \cdot b)$. The zero vector, the additive identity is simply $(0, 0)$.

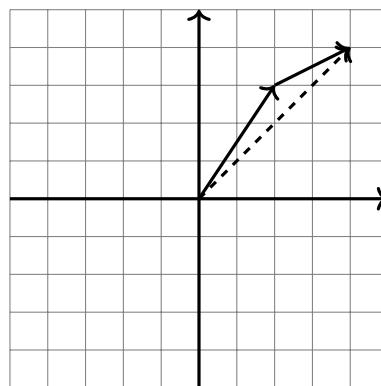
Example 6. When we add vectors (the points) in \mathbb{R}^2 , there is a nice visual representation. First, just think of a point like $(2, 3) \in \mathbb{R}^2$. Think of it as a pair of “shifts” meaning:

- shift 2 in the x direction
- shift 3 in the y direction

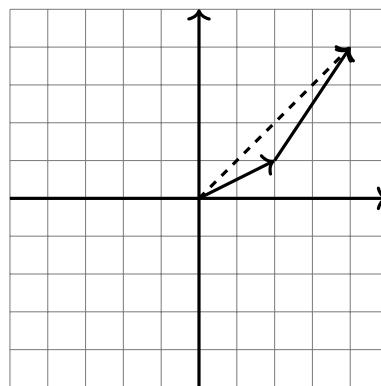
If we were to apply such a shift to any point in the plane the result would be to move that point along an arrow that represents these two shifts simultaneously:



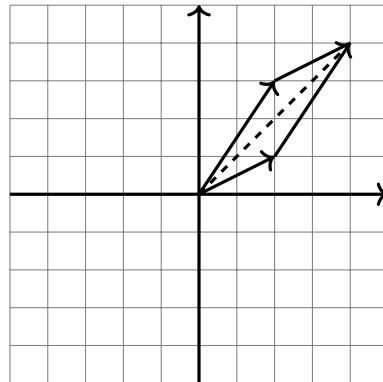
To add two vectors in \mathbb{R}^2 together is to see what the cumulative shift would be by doing one shift and then the other. That is, we send a point along the arrow “ $(2, 3)$ ” (shift x by +2, shift y by +3) and then send that result along the arrow “ $(2, 1)$ ” (shift x by +2, shift y by +1) and see what the *combined shifting arrow* would be:



Notice that if we shift $(2, 1)$ and then $(2, 3)$ the picture looks like:



We can put both orders together and get a parallelogram:



Vector addition in \mathbb{R}^2 can be thought of visually as finding the diagonal of a parallelogram.

Computationally, it can be thought of as simply adding coordinates component-wise:

$$(a, b) + (c, d) = (a + c, b + d).$$

Example 7. The set \mathbb{F}_2^4 is a vector space where all the vectors are 4-tuples of 1's and 0's. For instance $(0, 1, 1, 0)$ and $(1, 1, 0, 1)$ are vectors in this space.

To visually explore different examples of vector spaces go to the following SageMath activity:



2.1.3 Subspaces and Spans

Subspace

A subset $H \subset V$ of a vector space V is called a subspace if it is a vector space in and of itself.

Theorem 2.1.1 Subspace Criteria

If a subset $H \subset V$ satisfies the following, it is a subspace:

- When we restrict the addition operation of the additive group V to H , it is well-defined—the operation is closed in H . That is, if $a, b \in H$, then $a + b \in H$.
- Scaling keeps us within H too. If the scalars are in a field F and $k \in F$, then $k \cdot v \in H$ for all $v \in H$ and $k \in F$.

Proof. We just need to verify that the other properties of being a vector space tag along. First, since H is closed under scaling, if $h \in H$, then $-1 \cdot h = -h \in H$ so that every element has an additive inverse in H . Since H is closed under addition, $0_V = h + (-h) \in H$ so that H has an additive identity. Associativity and the compatibility of scalar multiplication with addition is inherited from V . Hence, just the two criteria *are enough*. \square



Example 8. Take the two vectors $(1, 3, 2)$ and $(0, 2, 3)$ in \mathbb{R}^3 . Let

$$H = \{a \cdot (1, 3, 2) + b \cdot (0, 2, 3) : a, b \in \mathbb{R}\}.$$

In a picture, this is the set of vertices of parallelograms formed with rescalings of the two vectors. These vertices, elements in H , fill out an entire plane in \mathbb{R}^3 . That is, H is a plane. Let's show that this plane is a subspace of V . We just check the two criteria.

First, we check to see if addition is closed in H . Take two arbitrary elements of H : $a \cdot (1, 3, 2) + b \cdot (0, 2, 3)$ and $c \cdot (1, 3, 2) + d \cdot (0, 2, 3)$. When they add together we get: $(a+c) \cdot (1, 3, 2) + (b+d) \cdot (0, 2, 3)$ which is in H since it matches the condition of being (real number)· $(1, 3, 2)$ added to (real number)· $(0, 2, 3)$. Therefore, addition is closed in H .

Now, what about rescaling? Again, take an arbitrary element of H which we can write as $a \cdot (1, 3, 2) + b \cdot (0, 2, 3)$ and multiply it by a scalar $k \in \mathbb{R}$. We get: $(k \cdot a) \cdot (1, 3, 2) + (k \cdot b) \cdot (0, 2, 3)$ which again is of the form (real number)· $(1, 3, 2)$ added to (real number)· $(0, 2, 3)$. Hence, it is in H so that H is closed under scaling. Hence, H is a subspace. We call it the *span* of the vectors $(1, 3, 2)$ and $(0, 2, 3)$. Or we could say that the vectors $(1, 3, 2)$ and $(0, 2, 3)$ span a plane in space. This plane is a subspace of V .

Before we talk about the word “span,” let’s look at some examples of the types of spans (*which are subspaces*) that we get in \mathbb{R}^3 :

Possible Subspaces of \mathbb{R}^3

The possible options for subspaces of \mathbb{R}^3 are:

- just $\{0_{\mathbb{R}^3}\}$,
- a line through the origin *spanned by one nonzero vector*,
- a plane through the origin *spanned by two nonzero vectors*,
- or all of \mathbb{R}^3 *spanned by three nonzero vectors*.

Notice that we require that these spans *which are subspaces* to pass through the origin. This is necessary since

every subspace, being an additive group, contains the additive identity which is the origin. Notice that $\{0_{\mathbb{R}^3}\}$ meets all the criteria of a vector space. For instance, $0_{\mathbb{R}^3} + 0_{\mathbb{R}^3} = 0_{\mathbb{R}^3}$, and $k \cdot 0_{\mathbb{R}^3} = 0_{\mathbb{R}^3}$ for every $k \in \mathbb{R}$.

Span

The span of a collection of vectors $\{v_1, v_2, v_3, \dots, v_n\}$ in a F -vector space V is the smallest subspace H of V such that $\{v_1, v_2, v_3, \dots, v_n\} \subset H$.

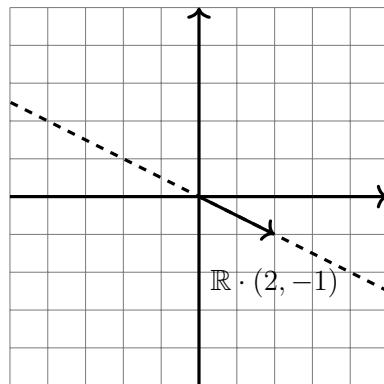
To denote the span of a collection of vectors $\{v_1, v_2, v_3, \dots, v_n\}$, we use the symbols “ $\langle \cdots \rangle$ ” and write $\langle v_1, v_2, v_3, \dots, v_n \rangle$.

Theorem 2.1.2 Vector Span Description

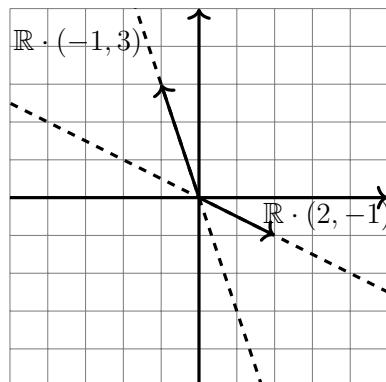
The span of a collection of vectors $\langle v_1, v_2, v_3, \dots, v_n \rangle$ in a F -vector space is equal to $F \cdot v_1 + F \cdot v_2 + \dots + F \cdot v_n$.

Example 9. The span $\langle(1, 0, 0), (0, 1, 0)\rangle \subset \mathbb{R}^3$ is equal to all of the vectors of the form $\{(a, b, 0) : a, b \in \mathbb{R}\}$. We can also write it as $\mathbb{R} \cdot (1, 0, 0) + \mathbb{R} \cdot (0, 1, 0)$.

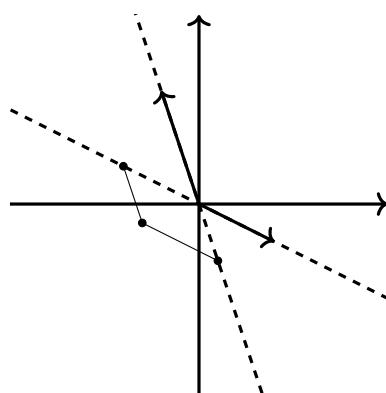
Example 10. Let's visualize a span in \mathbb{R}^2 . The span of the single vector $(2, -1)$ is $\mathbb{R} \cdot (2, -1)$ which is any point on the line in the direction of the arrow $(2, -1)$. Multiply the arrow by 2 and its length doubles and takes us to a point twice as far from the origin but on the same line. Multiply it by -1 , it reverses the direction of the arrow to a point in the opposite direction. All in all, every point that is obtained is on the same straight line. We can call this line $\mathbb{R} \cdot (2, -1)$.



Example 11. Now what happens when we add two spans together in \mathbb{R}^2 . Consider the following:



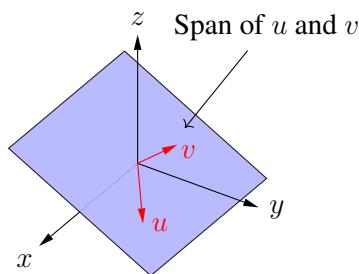
When we add a point on one line to a point on the other line it is as if we are plotting a coordinate pair thinking of those lines as axes:



In essence, this particular span fills \mathbb{R}^2 so that $\mathbb{R}^2 = \mathbb{R} \cdot (2, -1) + \mathbb{R} \cdot (-1, 3)$.

Example 12. If H and K are subspaces of a vector space V , then the set addition $H + K$ is also a subspace of V . In the exercises, you get to write a proof of this fact.

Example 13. The span of two vectors in \mathbb{R}^3 that are not parallel is a plane:



Example 14. Video We have an equality of spans:

$$\langle(1, 1, 0), (0, 1, 1), (1, 2, 1)\rangle = \langle(1, 1, 0), (0, 1, 1)\rangle$$

This is because $(1, 2, 1) \in \langle(1, 1, 0), (0, 1, 1)\rangle$ since $(1, 2, 1) = 1 \cdot (1, 1, 0) + 1 \cdot (0, 1, 1)$. So: $k \cdot (1, 2, 1) = k \cdot (1, 1, 0) + k \cdot (0, 1, 1)$ is included in $\mathbb{R} \cdot (1, 1, 0) + \mathbb{R} \cdot (0, 1, 1)$ already. If we wanted to write a little proof for the set equality, we would take an arbitrary element of the first set and show it is in the second. Then, we would take an arbitrary element of the second set and show that it is in the first. Let $a, b, c \in \mathbb{R}$. Taking an element of $\langle(1, 1, 0), (0, 1, 1), (1, 2, 1)\rangle$, we have:

$$a \cdot (1, 1, 0) + b \cdot (0, 1, 1) + c \cdot (1, 2, 1) = (a + c) \cdot (1, 1, 0) + (b + c) \cdot (0, 1, 1) \in \langle(1, 1, 0), (0, 1, 1)\rangle.$$

Now, taking an element in $\langle(1, 1, 0), (0, 1, 1)\rangle$, we have:

$$a \cdot (1, 1, 0) + b \cdot (0, 1, 1) = a \cdot (1, 1, 0) + b \cdot (0, 1, 1) + 0 \cdot (1, 2, 1) \in \langle(1, 1, 0), (0, 1, 1), (1, 2, 1)\rangle.$$

Example 15. Notice that \mathbb{C} itself is a \mathbb{Q} -vector space since \mathbb{C} is an additive group and multiplication by rational numbers in \mathbb{Q} follows all of the rules of scalars. Notice that $\langle 1, \sqrt{2} \rangle$ is a \mathbb{Q} -subspace of \mathbb{C} which is not \mathbb{C} . Try it out!

Example 16. The polynomials $\mathbb{R}[x]$ are a \mathbb{R} -vector space. The span

$$\langle 1, x, x^2, x^3, x^4 \rangle = \mathbb{R} \cdot 1 + \mathbb{R} \cdot x + \mathbb{R} \cdot x^2 + \mathbb{R} \cdot x^3 + \mathbb{R} \cdot x^4$$

is a subspace of $\mathbb{R}[x]$. It is the collection of all polynomials which have degree at most 4. You can equivalently write this subspace as:

$$\langle 1, x, x^2, x^3, x^4 \rangle = \underbrace{P^0(\mathbb{R}) + P^1(\mathbb{R}) + P^2(\mathbb{R}) + P^3(\mathbb{R}) + P^4(\mathbb{R})}_{\text{The set addition between}} = \sum_{n=0}^4 P^n(\mathbb{R}).$$

polynomials of degree 0, 1, 2, 3,
and 4.

Linear Combination

Given a set of vectors $\{v_1, v_2, v_3, \dots, v_n\}$, the elements of a F -span $\langle v_1, v_2, v_3, \dots, v_n \rangle$ are called *F-linear combinations* of $v_1, v_2, v_3, \dots, v_n$. In other words, a linear combination of the vectors $v_1, v_2, v_3, \dots, v_n$ is a finite sum of the form $a_1 \cdot v_1 + a_2 v_2 + a_3 v_3 + \dots + a_n v_n$.

Example 17. $(\sqrt{2}, 3) = \sqrt{2} \cdot (1, 0) + 3 \cdot (0, 1)$ is a \mathbb{R} -linear combination of $(1, 0)$ and $(0, 1)$.

Example 18. $\frac{1}{2} + \frac{5}{3}\sqrt{2}$ is a \mathbb{Q} -linear combination of 1 and $\sqrt{2}$.

Minimal Spanning Set

Consider a vector space V . Take all sets S of nonzero vectors such that the span of the elements of S denoted as $\langle S \rangle$ is equal to all of V . These sets have different sizes. Take one of the sets S that has the smallest size possible. This set S is a *minimal spanning set* of V .

Dimension

The dimension of a vector space V is the number of vectors in a minimal spanning set.

Basis Definition 1

Any minimal spanning set of a vector space is called a *basis*.

Example 19. The dimension of \mathbb{R}^5 is ≥ 5 since we know that $(1, 0, 0, 0, 0)$, $(0, 1, 0, 0, 0)$, $(0, 0, 1, 0, 0)$, $(0, 0, 0, 1, 0)$, and $(0, 0, 0, 0, 1)$ span it. But even more is true. This turns out to be a minimal spanning set so that the dimension of it is 5. Therefore, we can call it a basis of \mathbb{R}^5 .

Example 20. The set \mathbb{R} is a vector space of dimension 1. We can take the set $\{1\}$ to be the basis.

Example 21. The set $\{0\}$ is a \mathbb{R} -vector space of dimension 0. This is because there are no nonzero vectors in $\{0\}$ to make a minimal spanning set of nonzero vectors. *There is no basis!* One should check that the single element set $\{0\}$ satisfies all the conditions required of a vector space. *See the exercises!*

Example 22. in \mathbb{R}^3 , the dimension of a plane is 2, of a line is 1, of the origin is 0.

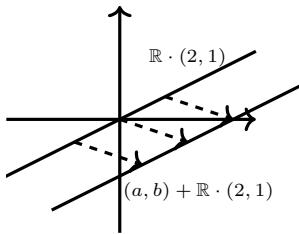
Example 23. Let $H = \langle (1, 2, 1), (2, 3, 0), (1, 1, -1) \rangle$. The dimension of H must be ≥ 2 since $(1, 1, -1) \in \langle (1, 2, 1), (2, 3, 0) \rangle$. Notice that $(1, 1, -1) = (2, 3, 0) - (1, 2, 1)$.

2.1.4 Quotient Vector Spaces

Example 24. Choose a vector in \mathbb{R}^2 such as $(2, 1)$. Now take its span: $\mathbb{R} \cdot (2, 1)$. This span itself can be considered a vector! All additive shifts by elements in \mathbb{R}^2 are other vectors. That is, we can define a new vector space:

$$\{(a, b) + \mathbb{R} \cdot (2, 1) : (a, b) \in \mathbb{R}^2\}$$

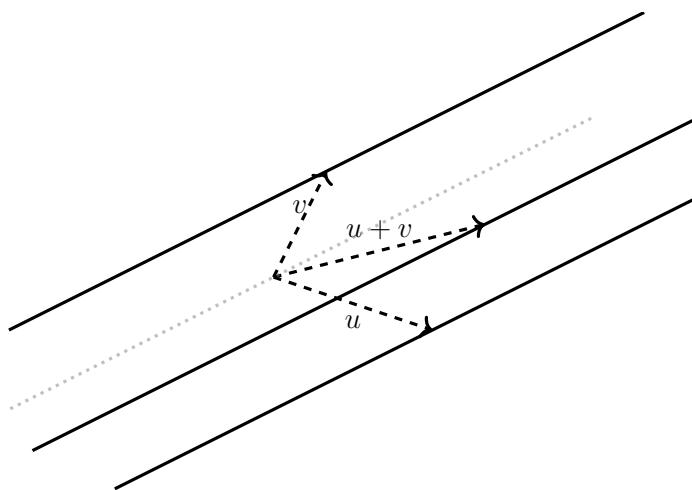
The collection of all shifts of a subspace *is a vector space!* Let's try to visualize this a little: $\mathbb{R} \cdot (2, 1)$ is a straight line in the plane.



Now, if we add (a, b) to every point of $\mathbb{R} \cdot (2, 1)$, it shifts each point a units in the x direction and b units in the y direction. We have just shifted the line $\mathbb{R} \cdot (2, 1)$. The result is a parallel line! That is, all lines parallel to $\mathbb{R} \cdot (2, 1)$ are the vectors. How do they add? We define addition as follows:

$$\left((a, b) + \mathbb{R} \cdot (2, 1) \right) + \left((c, d) + \mathbb{R} \cdot (2, 1) \right) = (a + c, b + d) + \mathbb{R} \cdot (2, 1).$$

In other words, they add just as the vectors that shifted them do!



Quotient Vector Space

Given a vector space V and a subspace H , define the quotient vector space V/H , read “ V over H ” or “ V mod H ,” as the space where the vectors are simply shifts of H . That is,

$$V/H = \{v + H : v \in V\}.$$

The addition is defined as

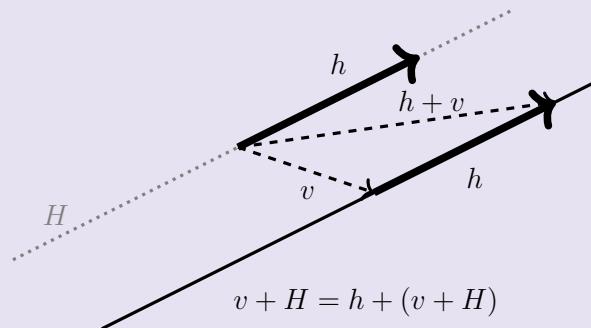
$$(v + H) +_{V/H} (w + H) = (v + w) + H$$

and the action of a scalar k is defined as

$$k \cdot (v + H) = k \cdot v + H.$$

The additive identity $0_{V/H}$ is simply H itself. This type of vector space arises often.

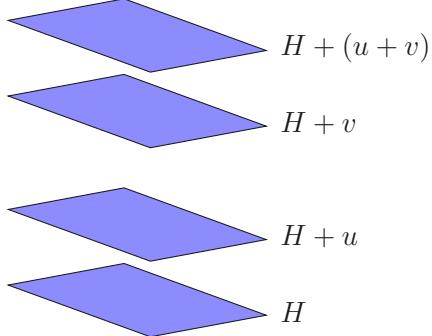
One way of thinking about quotient vector spaces is to think: *ignore everything in H or just pretend that vectors in H are zero.* Shifting $v + H$ by something in H keeps us with $v + H$. For instance, suppose that H is a line through the origin. Any vector h in H is parallel to H . The following shows how shifting by h does not change $v + H$ at all:



That is, we are letting the whole subspace H behave like 0. We “mod out by H .”

Example 25. The parallel lines in the last example make up the quotient vector space $\mathbb{R}^2/\mathbb{R} \cdot (2, 1)$.

Example 26. Let H be a plane in \mathbb{R}^3 that passes through the origin. Then, it is a subspace of \mathbb{R}^3 . The quotient \mathbb{R}^3/H is the collection of planes that are parallel to this one. The following is a picture of how these parallel planes add together:



For instance, let's add the planes $(1, 1, 1) + H$ and $(3, 1, 4) + H$. We get: $(1, 1, 1) + (3, 1, 4) + H = (4, 2, 5) + H$.

2.1.5 Function Vector Spaces

More vector spaces arise when we start thinking about functions. Functions add and can be rescaled. They can be thought of as vectors. Let's call $\text{Hom}(D, C)$ the vector space of functions $D \rightarrow C$ where C itself is a vector space.

Vector Space of Functions

Suppose that $f : D \rightarrow C$ and $g : D \rightarrow C$. Suppose that C is a F -vector space. Then the following definitions turn the set $\text{Hom}(D, C)$ into a vector space:

- The addition of functions $(f + g) : D \rightarrow C$ is defined by $x \mapsto f(x) + g(x)$.
- Given a scalar $k \in F$, we can define $k \cdot f : D \rightarrow C$ as the function $x \mapsto k \cdot f(x)$.
- The constant function $D \rightarrow C$ given by $x \mapsto 0_C$ is the additive identity element $0_{\text{Hom}(D, C)}$ of $\text{Hom}(D, C)$.

the set $\text{Hom}(D, C)$ becomes a vector space.

Example 27. The set $\text{Hom}(\mathbb{R}^3, \mathbb{R}^2)$ of functions $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ is a vector space. We will be representing some of the functions (i.e. vectors) in $\text{Hom}(\mathbb{R}^3, \mathbb{R}^2)$ as matrices in a couple sections ahead. The fact that we can add and rescale functions tells us that we can do so to matrices and that we can actually have vector spaces of matrices: *matrices can be vectors too! It is quite useful at times to think of them this way.*

Example 28. Let $C([0, 2\pi])$ denote all continuous functions $[0, 2\pi] \rightarrow \mathbb{R}$. The set $C([0, 2\pi])$ is a *real vector space: it is a subspace of $\text{Hom}([0, 2\pi], \mathbb{R})$ since adding continuous functions and rescaling them give*

continuous functions back again. It is actually an *infinite dimensional* vector space. Linear algebra techniques look like integrations and summations! There is actually a lot of advanced calculus, analysis and differential equation techniques which are really just linear algebra—the matrices just do not look like matrices! Usually with vector spaces we only look at finite sums—but here we look at infinite sums. A possible basis for this vector space turns out to be

$$\{1\} \cup \left(\bigcup_{n=1}^{\infty} \{\sin(nx), \cos(nx)\} \right) = \{1, \sin(x), \cos(x), \sin(2x), \cos(2x), \sin(3x), \cos(3x), \dots\}.$$

Every function (i.e. vector) in $C([0, 2\pi])$ is an “*infinite* linear combination” of these basis elements: it is an infinite sum

$$b_0 + \sum_{n=1}^{\infty} a_n \sin(nx) + b_n \cos(nx)$$

Such an infinite sum is called a *Fourier series*. The space $C([0, 2\pi])$ is *too small* to describe *all* functions we get from this basis however. The space enlarges to what we call a *Hilbert space*. Our theory of integration has to even depart from Riemann integrals to something called *Lebesgue* integrals to even describe what can come from all of this! Such topics are beyond the scope of this text. Yet still, they are common and useful enough to give as an example to look forward to! Later in the text, after we have explored the linear algebra of finite dimensional spaces, we may work through some examples just remembering that there are incomplete (quite literally—the word “incomplete” is a specific mathematical term that correctly describes the situation) details.

Example 29. The set $\mathbb{R}[[x]]$ of power series—“infinite polynomials” in x and coefficients in \mathbb{R} is an \mathbb{R} -vector space with infinite basis $\{1, x, x^2, \dots\}$. This basis can be used as a basis for $C([-1, 1])$ —but it is not as pretty or usable as the sines and cosines in the last example because things are not “orthogonal”—meaning perpendicular enough in some way. We will talk about a process to make bases “orthogonal” (nicer) called *Gram-Schmidt orthogonalization*. In this book, we mainly use such a process on *nice finite dimensional vector spaces*. But still, this process can be used on this infinite basis. The result? Polynomials called Legendre polynomials—sometimes used to solve differential equations and in many other places.

2.1.6 Rings and Modules

Sometimes we want to consider “vectors” when scaling is not necessarily reversible. One common example is when we want to consider tuples of integer coordinates like in \mathbb{Z}^4 or \mathbb{Z}^5 . We do not call these elements vectors any more. *The word vector is a special term—reserved for when rescaling is reversible!*

Ring

A set R is called a ring if it meets all the criteria for being a field except it is not necessary to admit multiplicative inverses. For our purposes, we assume that rings are commutative in both addition and multiplication.

Example 30. The set \mathbb{Z} is a ring.

Example 31. The set $\mathbb{R}[x]$ of polynomials in x with coefficients in \mathbb{R} is a ring.

Example 32. All fields are rings. This means that \mathbb{R} , \mathbb{C} , \mathbb{Q} , and even \mathbb{F}_2 are rings. Rings can have multiplicative inverses for all nonzero elements—but they do not have to. They are more general than fields.

Example 33. The set of polynomials $\mathbb{R}[x]$ in the variable x and coefficients in \mathbb{R} is a ring but not a field since reciprocals of polynomials are not always polynomials (i.e. $\left(\frac{1}{x}\right)$ is not a polynomial). Yet it is also a \mathbb{R} -vector space!

Modules

A R -module is the exact same thing as a vector space except the scalars are taken in a (commutative) ring R . This simply means that rescaling may not be reversible.

Example 34. \mathbb{Z}^3 is a \mathbb{Z} -module. This means that the scalars are in the ring \mathbb{Z} .

Example 35. Vector spaces are just modules over a field. For instance, the \mathbb{R} -vector space \mathbb{R}^3 is a \mathbb{R} -module.

Key Concepts from this Section

- **scalars:** (page 105) A scalar is an element of a field F that can be multiplied to a vector in a F -vector space to “scale” it.
- **commutative:** (page 105) An operation \star is called commutative if $a \star b = b \star a$.
- **field:** (page 105) A field is a set S with the following properties:
 - S itself is an additive group with respect to $+$ with an additive identity 0.
 - $S \setminus \{0\}$ forms a multiplicative group with a multiplicative identity 1.
 - Multiplication is “ringed” over addition with in S : *multiplication distributes over addition*: $a \cdot (b + c) = a \cdot b + a \cdot c$.
 - For our purposes, we assume that both the addition $+$ and the multiplication \cdot are *commutative*: $a \cdot b = b \cdot a$ and $a + b = b + a$ so that the order we write it does not matter.
- **finite fields \mathbb{F}_p :** (page 105) Define the finite field \mathbb{F}_p for a prime p to be the set $\{0, 1, 2, \dots, p-1\}$ where

- $a + b = \text{remainder of } (a + b) \div p$
- $a \cdot b = \text{remainder of } (a \cdot b) \div p$

Then, \mathbb{F}_p is a field.

- **vector space:** (page 106) A F -vector space is an additive commutative group V . The elements of the field F can “rescale” the elements (vectors) of the set V . But this must be done compatibly with the addition in V . Particularly, for any scalars $k, r \in F$ and any vectors $u, v \in V$:

- $k \cdot (v + u) = k \cdot v + k \cdot u$ (Rescaling before or after addition is the same.)
- $(k + r) \cdot v = k \cdot v + r \cdot v$ (Addition of scalars applied to a vector becomes the addition of the two scaled versions of that vector.)
- $k \cdot v \in V$ (The action of F keeps things inside of V .)
- $k \cdot (r \cdot v) = (k \cdot r) \cdot v$ (“Associativity” mixes between F and V .)

- **additive identity:** (page 106) The additive identity of a vector space V is often denoted by 0_V .
- **subspace:** (page 108) A subset $H \subset V$ of a vector space V is called a subspace if it is a vector space in and of itself.
- **theorem 2.1.1 subspace criteria:** (page 108) If a subset $H \subset V$ satisfies the following, it is a subspace:
 - When we restrict the addition operation of the additive group V to H , it is well-defined—the operation is closed in H . That is, if $a, b \in H$, then $a + b \in H$.
 - Scaling keeps us within H too. If the scalars are in a field F and $k \in F$, then $k \cdot v \in H$ for all $v \in H$ and $k \in F$.

- **possible subspaces of \mathbb{R}^3 :** (page 109) The possible options for subspaces of \mathbb{R}^3 are:
 - just $\{0_{\mathbb{R}^3}\}$,
 - a line through the origin *spanned by one nonzero vector*,
 - a plane through the origin *spanned by two nonzero vectors*,
 - or all of \mathbb{R}^3 *spanned by three nonzero vectors*.
- **span:** (page 110) The span of a collection of vectors $\{v_1, v_2, v_3, \dots, v_n\}$ in a F -vector space V is the smallest subspace H of V such that $\{v_1, v_2, v_3, \dots, v_n\} \subset H$.
- **theorem 2.1.2 vector span description:** (page 110) The span of a collection of vectors $\langle v_1, v_2, v_3, \dots, v_n \rangle$ in a F -vector space is equal to $F \cdot v_1 + F \cdot v_2 + \dots + F \cdot v_n$.
- **linear combination:** (page 112) Given a set of vectors $\{v_1, v_2, v_3, \dots, v_n\}$, the elements of a F -span $\langle v_1, v_2, v_3, \dots, v_n \rangle$ are called F -*linear combinations* of $v_1, v_2, v_3, \dots, v_n$. In other words, a linear combination of the vectors $v_1, v_2, v_3, \dots, v_n$ is a finite sum of the form $a_1 \cdot v_1 + a_2 v_2 + a_3 v_3 + \dots + a_n v_n$.

- **minimal spanning set:** (page 113) Consider a vector space V . Take all sets S of nonzero vectors such that the span of the elements of S denoted as $\langle S \rangle$ is equal to all of V . These sets have different sizes. Take one of the sets S that has the smallest size possible. This set S is a *minimal spanning set* of V .
- **dimension:** (page 113) The dimension of a vector space V is the number of vectors in a minimal spanning set.
- **basis definition 1:** (page 113) Any minimal spanning set of a vector space is called a *basis*.
- **quotient vector space:** (page 114) Given a vector space V and a subspace H , define the quotient vector space V/H , read “ V over H ” or “ V mod H ,” as the space where the vectors are simply shifts of H . That is,

$$V/H = \{v + H : v \in V\}.$$

The addition is defined as

$$(v + H) +_{V/H} (w + H) = (v + w) + H$$

and the action of a scalar k is defined as

$$k \cdot (v + H) = k \cdot v + H.$$

The additive identity $0_{V/H}$ is simply H itself. This type of vector space arises often.

- **Hom(D, C):** (page 116) The notation $\text{Hom}(D, C)$ is used to denote a vector space of functions $D \rightarrow C$ where C itself is a vector space.
- **vector space of functions:** (page 116) Suppose that $f : D \rightarrow C$ and $g : D \rightarrow C$. Suppose that C is a F -vector space. Then the following definitions turn the set $\text{Hom}(D, C)$ into a vector space:
 - The addition of functions $(f + g) : D \rightarrow C$ is defined by $x \mapsto f(x) + g(x)$.
 - Given a scalar $k \in F$, we can define $k \cdot f : D \rightarrow C$ as the function $x \mapsto k \cdot f(x)$.
 - The constant function $D \rightarrow C$ given by $x \mapsto 0_C$ is the additive identity element $0_{\text{Hom}(D, C)}$ of $\text{Hom}(D, C)$.

the set $\text{Hom}(D, C)$ becomes a vector space.

- **ring:** (page 117) A set R is called a ring if it meets all the criteria for being a field except it is not necessary to admit multiplicative inverses. For our purposes, we assume that rings are commutative in both addition and multiplication.
- **modules:** (page 118) A R -module is the exact same thing as a vector space except the scalars are taken in a (commutative) ring R . This simply means that rescaling may not be reversible.

2.1.7 Exercises

Computation Practice

1. Express the vector $(2, 4, -3)$ as a linear combination of the vectors $(1, 3, -1)$ and $(0, 2, 1)$.
2. The line $y = 2x$ is a line through the origin in $V = \mathbb{R}^2$. We can think of it as a subspace H of V .
 - (a) Find a vector $t \in \mathbb{R}^2$ so that $t + H$ describes the line $y = 2x - 3$ which is parallel to $y = 2x$. *Hint: the vectors in the line are solutions to the equation. Any vector t in the line works!*
 - (b) Find a vector $w \in \mathbb{R}^2$ so that $w + H$ describes the line $y = 2x + 5$ which is parallel to $y = 2x$.
 - (c) Find a vector $r \in \mathbb{R}^2$ so that $(t + H) +_{V/H} (w + H)$.
 - (d) What is an equation that describes the line $r + H$?
3. Suppose that H is a straight line through the origin in \mathbb{R}^3 . Describe what the quotient space \mathbb{R}^3/H looks like.
4. Suppose that we have a vector space V that is minimally spanned by the vectors a, b, c, d . Suppose that we would like to form a quotient V/H . The elements of the quotient vector space are simply subsets or rather chunks of V that partition V . Let's create our chunks so that a and b lie in the same chunk together—that is, $a + H = b + H$. Let's also say that we would like $c + H = d + H$. Determine how we should construct H . Can you express H as the span of 2 vectors?
5. The equation $x + y + 2z = 0$ is the equation of a plane through the origin in xyz coordinates. Let's call this plane H and let $V = \mathbb{R}^3$. Then, denote the plane $x + y + 2z = 3$ by a and the plane $x + y + 2z = 5$ by b . The planes a and b are parallel to the plane H . Therefore, $a, b \in V/H$.
 - (a) $a = t + H$. Find a vector t that makes this work. *Hint: the vectors in the plane are solutions to the equation. Any vector t in the plane works!*
 - (b) $b = w + H$. Find a vector w that makes this work.
 - (c) Perform the computation $a +_{V/H} b$. Describe the resulting plane as (a vector) + H : a shift of the plane H by a vector. *Hint: use the t and w you have already found. Do you know how to perform the following addition: $(t + H) +_{V/H} (w + H)$?*

- 6.** In this section, we defined finite fields \mathbb{F}_p where p is a prime number. Consider the finite field \mathbb{F}_7 . Its elements are described by the set $\{0, 1, 2, 3, 4, 5, 6\}$. In a field, every nonzero element has a multiplicative inverse. Hence, $3 \in \mathbb{F}_p$ has a multiplicative inverse in this set. That is, $3 \cdot_{\mathbb{F}_p} ? = 1$. What is this multiplicative inverse?

Notation Practice:

- 7.** Use proper notation to express the following:
- The vector v is a linear combination of the vectors v_1, v_2, \dots, v_n . The ambient vector space is V .
 - The span of v_1 and v_2 is contained in the span of v_3, v_4 , and v_5 . The ambient vector space is V .
- 8.** Write an expression that describes an arbitrary element of the span of the vectors v_1, v_2 , and v_3 . The ambient vector space is V which is a \mathbb{Q} -vector space.
- 9.** Write an expression that describes the intersection of two subspaces V_1 and V_2 of V .
- 10.** Write an expression that describes the collection of all ordered tuples that look like (a, b, c, d) where $a \in \mathbb{R}, b \in \mathbb{C}, c \in \mathbb{Z}, d \in \mathbb{Q}$. Use regular set builder notation and compact set builder notation.
- 11.** Write an expression that describes the collection of all sums that look like $a + b + c + d$ where $a \in \mathbb{R}, b \in \mathbb{C}, c \in \mathbb{Z}, d \in \mathbb{Q}$. Use regular set builder notation and compact set builder notation.
- 12.** Write an expression that represents all vectors outside the subspace A of the vector space B .
- 13.** Write an expression that represents the smallest subspace of the vector space V containing the subspaces A and B .
- 14.** Write an expression for the collection of all third degree polynomials with coefficients in \mathbb{C} .
- 15.** Suppose that $H \subset V$ and $a \in V$. Express the set $a + H$ in regular set builder notation.
- 16.** Suppose that v_1, v_2, \dots, v_n are vectors in a \mathbb{R} -vector space V . Write $\{\sum_{k=1}^n a_k v_k : a_1, a_2, \dots, a_n \in \mathbb{R}\}$ using vector span notation.
- 17.** Give notation for the vector space of ordered 4-tuples with entries in \mathbb{R} .
- 18.** Give notation for the vector space of ordered 3-tuples with entries in \mathbb{C} .
- 19.** Give notation for the vector space of ordered 5-tuples with entries in \mathbb{Q} .

Proof Practice

- 20.** Given any vector space V , prove that $\{0_V\}$ is a subspace which only has one element in it!
- 21.** Prove that $H = \{a \cdot (1, 2, 1) + b \cdot (1, 1, 0) : a, b \in \mathbb{R}\}$ is a subspace of \mathbb{R}^3 .
- 22.** Prove that the collection of third degree polynomials is not a vector space.
- 23.** Prove that the set of polynomials $\mathbb{R}[x]$ is a vector space that does not have a finite dimension. *Hint: consider a proof by contradiction to prove that $\mathbb{R}[x]$ cannot have finite dimension.*
- 24.** Prove that the dimension of the span of the following vectors which live in \mathbb{R}^4 is less than 3. (Find a contradiction.)
 $(1, 2, 3, 4), (1, 1, 1, 1), (2, 3, 4, 5), (5, 7, 9, 11)$
- 25.** Consider the vector space \mathbb{R}^3 . Prove that the span $\langle(1, 1, 1)\rangle$ is a subspace of the span $\langle(2, 3, 1), (-1, -2, 0)\rangle$.
- 26.** Suppose that $A, B \subset V$ are subspaces of the vector space V . Then prove that $A + B$ is also a subspace of V .
- 27.** Prove that for a subspace H of V , we have $H + H = H$.
- 28.** Let $H \subset V$ be a subspace of V . Suppose that $a \in H$. Then prove that $a + H = H$.
- 29.** Explain why $\mathbb{Z}[x]$ is both a ring and a \mathbb{Z} -module.

2.1.8 Solutions

1. $(2, 4, 3) = 2 \cdot (1, 3, -1) - (0, 2, 1)$

2. Solutions by parts:

- (a) $t = (0, -3)$ is an acceptable solution. There are others. Just make sure that it satisfies the equation $y = 2x - 3$.
- (b) $w = (0, 5)$ is an acceptable solution. There are others. Just make sure that it satisfies the equation $y = 2x + 5$.
- (c) $r = (0, -3) + (0, 5) = (0, 2)$.
- (d) Since $(0, 2)$ gives the y -intercept and line has slope 2, then the equation is $y = 2x + 2$.

3. This vector space looks like all lines that are parallel to H .

4. Taking a quotient by something or “modding out by something” means that we treat it like 0. We would like the difference of a and b to behave like 0 when we take the quotient. That is, we would like $\bar{a} - \bar{(b)} = \bar{0}_V$. This is the same as saying $a + H - (b + H) = H$. This is like saying $(a - b) + H + H = H$. So this would mean that $(a - b) + h_1 + h_2 = h_3$ for some $h_1, h_2, h_3 \in H$ which means that $(a - b) = h_3 - h_1 - h_2 \in H$. So, we would like $a - b \in H$. Similarly, we would like $c - d \in H$. Essentially what we are doing is making the difference between what we are “merging together” be zero. We have that $H = \langle a - b, c - d \rangle$

5. Solution by parts:

- (a) One simple choice for t is $(1, 0, 1)$ since this satisfies $x + y + 2z = 3$. There are many others that work.
- (b) One simple choice for w is $(3, 0, 1)$ since this satisfies $x + y + 2z = 5$. There are many others that work.
- (c) We know that $(t + H) +_{V/H} (w + H) = (t + w) + H$. Therefore, using our choices for t and w in this solution, we have that the sum of planes in this quotient is. $(4, 0, 2) + H$ In other words, it is a shift of the plane H by the vector $(4, 0, 2)$.

6. Notice that $3 \cdot 5 = 15$ which has remainder 1 when we divide by 7. Hence, $3 \cdot_{\mathbb{F}_p} 5 = 1$ so that 5 is the multiplicative inverse of 3 in \mathbb{F}_p .

7. Solutions by parts:

- (a) There is more than one way. We could write $H = \langle v_1, v_2, \dots, v_n \rangle \subset V$ and then say $v \in H$. We could also write: $v = \sum_{k=1}^n a_k v_k$ where $a_1, a_2, \dots, a_n \in \mathbb{R}$.

(b) $\langle v_1, v_2 \rangle \subset \langle v_3, v_4, v_5 \rangle \subset V$.

8. For $v_1, v_2, v_3 \in V$ where V is a \mathbb{Q} -vector space, elements in the span $\langle v_1, v_2, v_3 \rangle$ look like $a_1v_1 + a_2v_2 + a_3v_3$ where $a_1, a_2, a_3 \in \mathbb{Q}$.

9. $V_1 \subset V_2$

10. regular set builder notation: $\{(a, b, c, d) : a \in \mathbb{R}, b \in \mathbb{C}, c \in \mathbb{Z}, d \in \mathbb{Q}\}$. compact: $\mathbb{R} \times \mathbb{C} \times \mathbb{Z} \times \mathbb{Q}$.

11. regular set builder notation: $\{a + b + c + d : a \in \mathbb{R}, b \in \mathbb{C}, c \in \mathbb{Z}, d \in \mathbb{Q}\}$. compact: $\mathbb{R} + \mathbb{C} + \mathbb{Z} + \mathbb{Q}$.

12. $B \setminus A$

13. $A + B$

14. $P_3(\mathbb{C}) \setminus P_2(\mathbb{C})$.

15. Let $a \in V$. Then, $a + H = \{a + h : h \in H\}$.

16. $\langle v_1, v_2, v_3, \dots, v_n \rangle$

17. \mathbb{R}^4 or $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$

18. \mathbb{C}^3 or $\mathbb{C} \times \mathbb{C} \times \mathbb{C}$

19. \mathbb{Q}^5 or $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$

20. Notice that this subset is closed under addition: $0_V + 0_V = 0_V$. It is also closed under scalar multiplication: $k \cdot 0_V = 0_V$ for any scalar k .

21. The proof is exactly the same as in [example 8](#).

22. The set $P^3(\mathbb{R})$ is not closed under addition since $(x^3 + 1) + (-x^3 + x) = (x + 1)$. This is a degree 1 polynomial and is not in $P^3(\mathbb{R})$. Further, the additive identity 0 is not in $P^3(\mathbb{R})$. Any one reason will do for why any of the criteria in the definition of a vector space is not matched!

23. The set of polynomials $\mathbb{R}[x]$ is closed under addition and scalar multiplication by real numbers. The usual properties of addition and multiplication among polynomials transfer over to make $\mathbb{R}[x]$ a vector space. Suppose by way of contradiction that $\mathbb{R}[x]$ has a finite dimension so that it has a finite basis. Let n be the degree of the highest polynomial in that basis. Then x^{n+1} cannot be in the span of that basis since it is impossible to add two polynomials of degree less than $n + 1$ and get one of degree $n + 1$. But a basis is supposed to span the space. This contradicts that $\mathbb{R}[x]$ has a finite dimension.

24. Notice that $(1, 2, 3, 4) + (1, 1, 1, 1) = (2, 3, 4, 5)$ and that $(1, 2, 3, 4) + 2 \cdot (1, 1, 1, 1) = (5, 7, 9, 11)$. You could find this by inspection or by trying to solve a system of equations and then finding a dependency relation through the process. These two facts together contradict the idea that the dimension is greater than or equal to 3. This is because they show first that

$$\langle(1, 2, 3, 4), (1, 1, 1, 1), (2, 3, 4, 5), (5, 7, 9, 11)\rangle \subset \langle(1, 2, 3, 4), (1, 1, 1, 1)\rangle$$

since any linear combination

$$a \cdot (1, 2, 3, 4) + b \cdot (1, 1, 1, 1) + c \cdot (2, 3, 4, 5) + d \cdot (5, 7, 9, 11)$$

can be written as

$$\begin{aligned} & a \cdot (1, 2, 3, 4) + b \cdot (1, 1, 1, 1) + c \cdot \left((1, 2, 3, 4) + (1, 1, 1, 1) \right) + d \cdot \left((1, 2, 3, 4) + 2 \cdot (1, 1, 1, 1) \right) \\ &= (a + c + d) \cdot (1, 2, 3, 4) + (b + c + 2d) \cdot (1, 1, 1, 1) \in \langle(1, 2, 3, 4), (1, 1, 1, 1)\rangle \end{aligned}$$

It is already clear that

$$\langle(1, 2, 3, 4), (1, 1, 1, 1), (2, 3, 4, 5), (5, 7, 9, 11)\rangle \subset \langle(1, 2, 3, 4), (1, 1, 1, 1)\rangle$$

since any linear combination

$$a \cdot (1, 2, 3, 4) + b \cdot (1, 1, 1, 1)$$

can be written as

$$a \cdot (1, 2, 3, 4) + b \cdot (1, 1, 1, 1) + 0 \cdot (2, 3, 4, 5) + 0 \cdot (5, 7, 9, 11) \in \langle(1, 2, 3, 4), (1, 1, 1, 1), (2, 3, 4, 5), (5, 7, 9, 11)\rangle.$$

Therefore,

$$\langle(1, 2, 3, 4), (1, 1, 1, 1), (2, 3, 4, 5), (5, 7, 9, 11)\rangle = \langle(1, 2, 3, 4), (1, 1, 1, 1)\rangle$$

so that $\{(1, 2, 3, 4), (1, 1, 1, 1)\}$ is a spanning set for our span of four vectors which has size less than 3. Therefore, by the definition of dimension, the dimension of the span is less than 3.

25. Let $A = \langle(1, 1, 1)\rangle$ and $B = \langle(2, 3, 1), (-1, -2, 0)\rangle$. First, we need to show that $A \subset B$. This is clear since any linear combination of $(1, 1, 1)$ written as $a \cdot (1, 1, 1) = a \cdot (2, 3, 1) + a \cdot (-1, -2, 0) \in B$ since $(1, 1, 1) = (2, 3, 1) + (-1, -2, 0)$. Next, we need to show that A is closed under addition and scalar multiplication. Yet this is clear since any scalar multiple by $k \in \mathbb{R}$ of an element $a \cdot (1, 1, 1) \in A$ is in A : $(k \cdot a) \cdot (1, 1, 1) \in A$ and adding any two elements of A such as $a \cdot (1, 1, 1)$ and $b \cdot (1, 1, 1)$ is $(a + b) \cdot (1, 1, 1)$ which is again in A .

26. An arbitrary element of $A + B$ can be expressed as $a + b$ for $a \in A$ and $b \in B$. Notice that if we have two such elements in $x, y \in A + B$ —namely $x = a_1 + b_1$ and $y = a_2 + b_2$, then $x + y = (a_1 + a_2) + (b_1 + b_2) \in A + B$ because it matches the definition of what it means to be in $A + B$. Also, additive inverses such as $-x = -(a_1 + b_1) = (-a_1) + (-b_1)$ is again in $A + B$ because again it can be written as something in A added to something in B . These two facts in particular show that $\underbrace{x}_{\in A+B} + \underbrace{(-x)}_{\in A+B} = \underbrace{0_V}_{\in A+B}$. But since $0_V \in A$, B , we could have just written: $0_V = \underbrace{0_V}_{\in A+B} + \underbrace{0_V}_{\in A+B}$. Associativity is inherited from V . Therefore, $A + B$ is an additive group. Further, if k is a scalar, then $k \cdot x = k \cdot (a_1 + b_1) = \underbrace{(ka_1)}_{\in A} + \underbrace{kb_1}_{\in B}$. Since it is closed under scalar multiplication as well, we have that $A + B$ is a subgroup. *In fact, it is the smallest subspace that contains both A and B since any subspace must contain sums of things in A and B because it must be closed under addition.*

27. Look at the proof in the solution of the last exercise. According to the last statement in that proof, $H + H$ is the smallest subspace of V that contains H . Well that would be H itself. Therefore, $H + H = H$.

28. The set $a + H$ is simply $\{a + h : h \in H\}$. Notice that $-a + h \in H$ if $h \in H$ since H is closed under addition and scalar multiplication (specifically we have multiplied a by -1). So, for a given $h \in H$, let $w = -a + h$. Then $w \in H$. This means that $a + \underbrace{w}_{\in H} \in a + H$. Therefore, $a + w = a + \underbrace{(-a + h)}_w = h \in a + H$. Yet, this is true for all $h \in H$. Therefore, $H \subset a + H$. Also, since $a \in H$, then $a + h \in H$ for any $h \in H$ since H is closed under addition. This shows that $a + H \subset H$. Therefore, $a + H = H$.

29. The set $\mathbb{Z}[x]$ is the set of polynomials in the variable x with coefficients in \mathbb{Z} . They add by adding the coefficients together of like terms. Since \mathbb{Z} is closed under addition, $\mathbb{Z}[x]$ is then closed under addition. We take for granted that addition of polynomials in $\mathbb{Z}[x]$ is associative. The polynomial 0 is in $\mathbb{Z}[x]$ and given any $a(x) \in \mathbb{Z}[x]$, then $-a(x) \in \mathbb{Z}[x]$ so that $\mathbb{Z}[x]$ admits additive inverses. Therefore, $\mathbb{Z}[x]$ is a group under addition. The set $\mathbb{Z}[x]$ is closed under scalar multiplication by scalars in \mathbb{Z} . Scalar multiplication by integers distributes over this addition. Multiplication by scalars is associative. Therefore, $\mathbb{Z}[x]$ is a \mathbb{Z} -module. If you multiply two polynomials together, you again get a polynomial where the coefficients are just sums of products of the coefficients of the two polynomials. Again, we get something in $\mathbb{Z}[x]$. Hence, $\mathbb{Z}[x]$ is closed under multiplication. This multiplication is associative (inherited) and distributes over addition. Therefore, $\mathbb{Z}[x]$ is a ring. Essentially all we are doing is definition matching with the definition of a ring.

Linear Independence and

2.2

Bases

2.2.1 Linear Independence	128
2.2.2 More on Bases	132
2.2.3 Free Rank and Existence of a Basis	136
2.2.4 Exercises	139
2.2.5 Solutions	142

Questions to Guide Your Study:

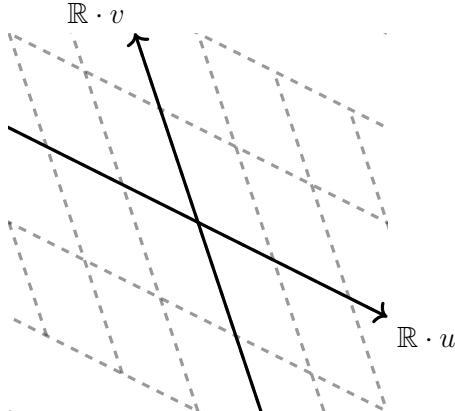
- *What does it mean for a collection of vectors to be linearly independent or linearly dependent?*
- *What are the different equivalent ways for thinking about linear independence?*
- *What are some strategies for deciding whether a collection of vectors is linearly independent or dependent?*
- *What are some ways for determining if a collection of vectors is a basis?*
- *How do you find the dimension of a vector space?*

2.2.1 Linear Independence

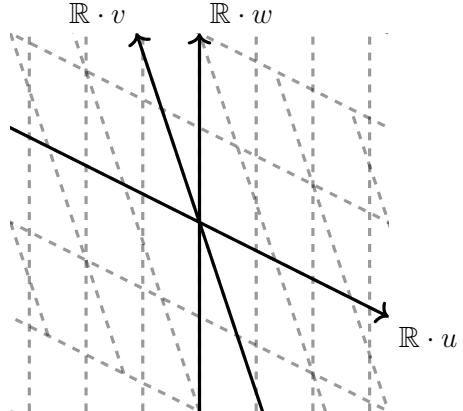
For vector spaces, there is an equivalent description of minimal spanning sets. It is called *linear independence*. If each vector in a set cannot be written as a linear combination of the others, then each vector is *independent* of the others and does not depend on them. Instead of saying that a set is a minimal spanning set, we could say that it is a spanning set which is linearly independent.

Another equivalent way of saying we have a minimal spanning set can be considered by an example. Suppose that $S = \{v, u, w\} \in \mathbb{R}^3$ spans a subspace $H \subset \mathbb{R}^3$. Then $\mathbb{R} \cdot v$, $\mathbb{R} \cdot u$, and $\mathbb{R} \cdot w$ are each lines in \mathbb{R}^3 contained in H . We can think of each of these lines as skewed axes. Adding a point (i.e. vector) from each of these axis lines gives us a linear combination. The vector described by this linear combination appears as a plot with respect to these skewed axes. If there is one and only one way to write the coordinates for each point

of H with respect to these skewed axes, then we say that the set S is a linearly independent set in \mathbb{R}^3 and that it is a minimal spanning set.



Good Axes: u and v are *linearly independent*. There is one and only one coordinate representation on the skewed axes for each point in the plane.



Bad Axes: u , v , and w are *linearly dependent*. There are **many** coordinate representations on the skewed axes for each point in the plane.

Let's look at a definition for linear independence of a set.

Linearly Independent Definition 1

A collection of vectors $\{v_1, v_2, v_3, \dots, v_n\}$ in a vector space V is called *linearly independent* if the only way for a linear combination $a_1v_1 + a_2v_2 + a_3v_3 + \dots + a_nv_n$ to equal the zero vector 0_V is for all of the scalars a_1 through a_n to be zero: $a_1 = a_2 = a_3 = \dots = a_n = 0$.

Linearly Independent Definition 2

Equivalently, we could say that a collection of vectors $\{v_1, v_2, v_3, \dots, v_n\}$ is linearly independent if and only if for any $v \in \langle v_1, v_2, v_3, \dots, v_n \rangle$, there is one and only one linear combination of $\{v_1, v_2, v_3, \dots, v_n\}$ that equals v . That is, there is exactly one set of coefficients a_1, a_2, \dots, a_n such that $v = a_1v_1 + a_2v_2 + \dots + a_nv_n$. The coefficients (a_1, a_2, \dots, a_n) themselves are the coordinates of v in the skewed coordinate system determined by the vectors $\{v_1, v_2, v_3, \dots, v_n\}$. There is only one skewed coordinate coordinate reading that yields v .

Linearly Independent Definition 3

A collection of vectors $B = \{v_1, v_2, v_3, \dots, v_n\}$ is linearly independent if and only if each vector in the collection is not in the span of the other vectors. That is, for any $v \in B$, then $v \notin \langle B \setminus \{v\} \rangle$.

Theorem 2.2.1 Linear independence: Definition Equivalence

All three definitions of linear independence are equivalent.

Proof. Notice that definition 1 is a special case of definition 2—when v is the zero vector. This means that definition 2 implies definition 1. We leave the implication that definition 1 implies definition 2 as an exercise! Do this by contradiction. Assume that a set is linearly independent if there is only one way to express the 0 vector as a linear combination of v_1, v_2, \dots, v_n . That is, all the scalar coefficients must be 0 to yield the zero vector. Suppose by way of contradiction that definition 2 does not hold so that

$$v = a_1v_1 + a_2v_2 + \cdots + a_nv_n = b_1v_1 + b_2v_2 + \cdots + b_nv_n$$

where $a_i \neq b_i$ for at least one index i . Can you contradict the fact that S is linearly independent according to definition 1?

That definition 3 is equivalent to definition 2 is also an exercise! Here is a hint:

$$v_1 = 1 \cdot v_1 + 0 \cdot v_2 + \cdots + 0 \cdot v_n.$$

□

Linearly Dependent

If a collection of vectors is not linearly independent, then it is linearly dependent.

Example 1. The set of vectors $\{(1, 0), (0, 1)\}$ is linearly independent. This is like saying that

$$a \cdot (1, 0) + b \cdot (0, 1) = (0, 0)$$

only when $a = b = 0$.

Example 2. The set of vectors $\{(1, 0), (2, 0)\}$ is linearly dependent since $-2 \cdot (1, 0) + (2, 0) = (0, 0)$. We can also see that $(2, 0) \in \langle(1, 0)\rangle$ so that by definition 3, the set cannot be linearly independent.

Example 3. Let's show that $(1, -1)$ and $(1, 1)$ are linearly independent using definition 1:

$$a \cdot (1, -1) + b \cdot (1, 1) = (a + b, -a + b) = (0, 0).$$

We are just solving the system of equations:

$$\begin{aligned} a + b &= 0 \\ a - b &= 0 \end{aligned}$$

You can verify that the only solution is $(0, 0)$. Therefore, the vectors are linearly independent.

Using definition 3, however, is probably the fastest way to show linear independence for \mathbb{R}^2 : since $(1, 1)$ is not a vector multiple of $(1, -1)$, we know that $(1, 1) \notin \langle(1, -1)\rangle$ and $(1, -1) \notin \langle(1, 1)\rangle$. Therefore, the collection $\{(1, 1), (1, -1)\}$ is linearly independent.



Example 4. A nice way of seeing if a set of vectors in \mathbb{R}^3 is linearly independent or dependent is to proceed as follows. We use definition 1. Suppose we want to consider if the vectors $(2, 3, -1)$, $(1, 2, 1)$ and $(3, 5, 0)$ are linearly independent. We line them up vertically as columns and write:

$$\begin{aligned} a \cdot \begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix} + b \cdot \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} + c \cdot \begin{pmatrix} 3 \\ 5 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 2a + b + 3c \\ 3a + 2b + 5c \\ -a + b \end{pmatrix} &= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \end{aligned}$$

We have a system of equations

$$\begin{aligned} 2a + b + 3c &= 0 \\ 3a + 2b + 5c &= 0 \\ -a + b &= 0 \end{aligned}$$

This is the same as finding the fiber $f^{-1}(0_{\mathbb{R}^3})$ where $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ is the function

$$(a, b, c) \mapsto (2a + b + 3c, 3a + 2b + 5c, -a + b).$$

If we get more than just the element $(0, 0, 0)$ in the fiber, we know a couple things. First, f is not injective and second, the columns of $\begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 5 \\ -1 & 1 & 0 \end{pmatrix}$ are not linearly independent. We will actually see very soon that these two ideas go hand in hand. *Linear independence and injectivity are friends!*

In solving the system, first notice that $b = a$ so that the first two equations become:

$$\begin{aligned} 3b + 3c &= 0 \\ 5b + 5c &= 0 \end{aligned}$$

Notice that these two equations are *really the same*: the second is just the first multiplied by $\frac{5}{3}$. The only information we gain from the first equation is that $b = -c$. This tells us that $a = -c$, $b = -c$ and c can be anything. For sure, the fiber $f^{-1}(0_{\mathbb{R}^3})$ has more than one element, is not injective and the vectors are not linearly independent. Therefore, they are linearly dependent.

Method for determining if a collection is linearly independent or dependent

Suppose that we have a vector collection $\{v_1, v_2, \dots, v_n\} \subset \mathbb{R}^m$. Then, create the function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ by the following rule:

$$(a_1, a_2, \dots, a_n) \mapsto a_1v_1 + a_2v_2 + \cdots + a_nv_n$$

If the function is injective, the vectors in the collection are independent. Otherwise, they are dependent. Since this function is additive, it suffices to check the size of $f^{-1}(0_{\mathbb{R}^m})$, which is the set of solutions to a system of equations. If it has only one element, then f is injective and so the collection is linearly independent. Otherwise, the collection is linearly dependent.

2.2.2 More on Bases

Recall that the first definition of a basis for a vector space is a *minimally sized spanning set*. The *dimension* of a vector space is defined to be the number of vectors in such a minimally sized spanning set. There is another equivalent characterization of what a basis is which is often used.

Basis Definition 2

A basis for a vector space V is a collection of vectors which is linearly independent and which spans all of V .

We will restrict ourselves primarily to vector spaces whose *dimensions are finite*. Hence, we prove the equivalence of our definitions of a basis in the *finite* case.

Theorem 2.2.2 Basis Definition Equivalence

The two definitions for a *finite* basis are equivalent.

Proof. That definition 2 implies definition 1 is an exercise—a proof by contradiction. Assume that a minimal spanning set is not linearly independent and then show how this assumption leads to a contradiction of minimality—meaning that the set that we assume to be minimal ends up not being minimal—we find a spanning set with fewer vectors. *You can do it!*

That definition 1 implies definition 2 relies on ideas that we develop in later sections. We will include

the proof here nonetheless. Skip this proof until you have read about **matrices** and **Smith normal form**.

First, assume definition 1. Suppose by way of contradiction that definition 2 does not hold. Namely, suppose that there is a linearly independent spanning set of a vector space V which is not minimal. This means that there are two differently sized linearly independent collections that span the space: say $S_1 = \{v_1, v_2, \dots, v_n\}$ and $S_2 = \{w_1, w_2, \dots, w_m\}$ where $m < n$.

Take a vector $v \in V$. Then v can uniquely be written with scalars $(a_1, a_2, \dots, a_n) \in \mathbb{R}^n$ as a linear combination $a_1v_1 + a_2v_2 + \dots + a_nv_n$ or uniquely with scalars $(b_1, b_2, \dots, b_m) \in \mathbb{R}^m$ as a linear combination $b_1v_1 + b_2v_2 + \dots + b_mv_m$. This dual representation creates a well-defined additive and “scalable” function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ called a *linear transformation*. It sends (a_1, a_2, \dots, a_n) to (b_1, b_2, \dots, b_m) . *The reader is invited to consider how just the uniqueness of the representation of the sum of two vectors in both representations turns this function into an additive one.*

Notice that the domain and codomain of this function are different vector spaces than V itself. They are spaces of tuples of coefficients. This function as a linear transformation has a unique matrix representation (under a column interpretation) where the i th column is the image of the standard basis vector e_i in the domain \mathbb{R}^n .

Because the linear independence of S_1 forces just one unique representation of the zero vector, this function f is injective (the fiber over the zero vector in the codomain is just the single zero vector of the domain). It’s Smith normal form however has a column of zeros just because $m < n$. This means that the Smith normal form has a nonzero kernel. This nonzero kernel pushed forward by the column operations map becomes the kernel of f . So, the kernel of f is nonzero. Yet this is a contradiction since f is injective. \square

Corollary 2.2.3 Dimension of \mathbb{R}^n

The dimension of \mathbb{R}^n is n .

Proof. Let $e_i \in \mathbb{R}^n$ be the n -tuple that has all zeros except for a 1 in position i . The vectors e_1, e_2, \dots, e_n clearly span \mathbb{R}^n and are linearly independent. Therefore, these vectors are a minimal spanning set so that the dimension is n . \square

Corollary 2.2.4 Condition for Linear Independence by Counting

If a collection of vectors is not a minimal spanning set, then it is not linearly independent.

Example 5. Suppose that we take a collection of vectors $\{(3, 4), (5, 6), (-10, 1)\} \subset \mathbb{R}^2$. We know that there exists a spanning set $\{(1, 0), (0, 1)\}$ of size 2. This is of size 3. Therefore, it is not a minimal spanning set and hence it is not linearly independent.

Example 6. We can see that the dimension of \mathbb{R}^2 is exactly 2. Take the spanning set $\{(1, 0), (0, 1)\}$. We just need to show that it is linearly independent. Then it will be a minimal spanning set. We can see that the only

scalars a and b that give

$$a \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

are $a = b = 0$. Hence, we are done. Note that the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by $f(a, b) = (a, b)$ is $\text{id}_{\mathbb{R}^2}$ which is clearly injective: there is only one element in $f^{-1}(0, 0)$.

Example 7. We can use this same technique to see if two vectors form a basis of \mathbb{R}^2 which has dimension 2. We start out by choosing only two vectors, because we already know the dimension of \mathbb{R}^2 . So, let's consider $(1, 2)$ and $(5, -1)$. We write these vectors as columns in a matrix: $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ and $\begin{pmatrix} 5 \\ -1 \end{pmatrix}$ to think of a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by

$$(x, y) \mapsto x \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} + y \cdot \begin{pmatrix} 5 \\ -1 \end{pmatrix} = \begin{pmatrix} x + 5y \\ 2x - y \end{pmatrix}.$$

To see if this function is injective, we simply check the fiber $f^{-1}(0_{\mathbb{R}^2})$ which is $f^{-1}(0, 0)$. To do this, we solve the system:

$$\begin{aligned} x + 5y &= 0 \\ 2x - y &= 0 \end{aligned}$$

Notice that from the bottom equation, $y = 2x$. Substituting in the top equation gives $x + 5(2x) = 0$ or simply $11x = 0$ so that $x = 0$. If $x = 0$, both equations force $y = 0$ so that $f^{-1}(0, 0) = \{(0, 0)\}$. Since the fiber only has one element, f is injective. Therefore, the set of vectors $(1, 2)$ and $(5, -1)$ is a basis for \mathbb{R}^2 .

Proving that a set is or is not a basis

Suppose that we are working in \mathbb{R}^3 which has dimension 3 and are considering the set of vectors

$$\{(a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3)\}.$$

To see if these vectors are a basis or not, we form an *additive* function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ given by

$$(x, y, z) \mapsto x \cdot (a_1, b_1, c_1) + y \cdot (a_2, b_2, c_2) + z \cdot (a_3, b_3, c_3)$$

which can also be written as:

$$(x, y, z) \mapsto (a_1x + a_2y + a_3z, b_1x + b_2y + b_3z, c_1x + c_2y + c_3z).$$

If this function is injective, the set of vectors is a basis. If not, then it is not a basis. Injectivity is checked right at the fiber $f^{-1}(0, 0, 0)$.



Example 8. Take the vectors $\{(1, 1), (1, 0), (2, 5)\}$. These are linearly dependent in \mathbb{R}^2 even though they span all of \mathbb{R}^2 . Let's find two different linear combinations of $(1, -1) \in \mathbb{R}^2$ using these vectors. We can write

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix} = a \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + b \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + c \cdot \begin{pmatrix} 2 \\ 5 \end{pmatrix}$$

and we have

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} a+b+2c \\ a+5c \end{pmatrix}$$

We just need to find two examples of a , b , and c that make this happen. If we let $c = 0$, then we need $1 = a + b$ and $-1 = a$ so that $b = 2$. This would give one linear combination:

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix} = -1 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 2 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 2 \\ 5 \end{pmatrix}$$

If we let $a = 0$, then the bottom equation would tell us $5c = -1$ so that $c = -\frac{1}{5}$. Therefore, in the top equation we would have $b - \frac{2}{5} = 1$ so that $b = \frac{7}{5}$. So we could have the linear combination:

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix} = 0 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \frac{7}{5} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{1}{5} \cdot \begin{pmatrix} 2 \\ 5 \end{pmatrix}$$

When a collection of vectors is not linearly independent as in the last example, there is more than one way to represent a vector as a linear combination of the collection.

Theorem 2.2.5 Subspace Dimension

Given a vector space V and a subspace W , suppose that $\dim(W) = \dim(V)$. This means that $W = V$.

Proof. Let $n = \dim(W) = \dim(V)$. Suppose by way of contradiction that $V \neq W$. Then, there exists $v \in V \setminus W$. This means that $v \in V$ but $v \notin W$. This means that v added to any basis of W must be linearly independent by definition 3 of linear independence. Yet any linearly independent spanning set by basis definition 1 is a basis. Hence, we have a basis for V of size $n + 1$. Since the basis definitions are equivalent, this basis is a minimal spanning set—yet we already assumed that $\dim(V) = n$ so that all minimal spanning sets must have size n . This is a contradiction. \square

Example 9. Since $(1, 2)$ and $(2, 1)$ are linearly independent in \mathbb{R}^2 , their span is a subspace V of \mathbb{R}^2 of dimension 2. Since the dimension of \mathbb{R}^2 is 2, this means that the $V = \mathbb{R}^2$. That is, $\mathbb{R}^2 = \langle(1, 2), (2, 1)\rangle$

2.2.3 Free Rank and Existence of a Basis

Linear *independence* is kind of like *freedom*—freedom from having two different representations that are the same with respect to a basis. Hence, we will be using the word *free* to describe situations that deal with linear independence. For modules, finding linear independence is not always as easy and *freedom is more precious!*

Free Rank

Let R be a ring. The Free rank of an R -module M is the least number of R -linearly independent elements whose span is all of M . Such a minimal collection is called a free basis for the R -module. The free rank of a vector space is simply its dimension.

Example 10. \mathbb{Z}^3 is a \mathbb{Z} -module of free-rank 3. It has a basis of $(1, 0, 0)$, $(0, 1, 0)$, and $(0, 0, 1)$.

Example 11. $\mathbb{F}_3 \times \mathbb{F}_3$ is a \mathbb{Z} -module since $k \in \mathbb{Z}$ acts on elements nicely by $k \cdot (a, b) = (\bar{k} \cdot a, \bar{k} \cdot b)$ where \bar{k} is the remainder of $k \div 3$ and multiplication is given in the field \mathbb{F}_3 . But, it has no \mathbb{Z} -basis nor even free \mathbb{Z} -rank! This is because no collection of elements can ever be \mathbb{Z} -linearly independent—not even one element. That is because $3 \cdot (a, b) = (0, 0)$ for any $(a, b) \in \mathbb{F}_3^3$ and $3 \neq 0$. But if we change our scalars to \mathbb{F}_3 , then it does have a \mathbb{F}_3 -basis of $(1, 0)$ and $(0, 1)$ and a \mathbb{F}_3 -dimension of 2.

We never run into the problem of the last example if our set of scalars is a field. To emphasize this point, we include a result about finitely generated vector spaces—we say that a vector space is *finitely generated* if it is the span of a finite number of vectors.

Theorem 2.2.6 Finitely Generated Vector Spaces have Bases

Every finitely generated vector space has a basis and a dimension.

Proof. Every finitely generated vector space has a minimal spanning set since it has a finite spanning set. Just choose a spanning set of the smallest size. This set is linearly independent since it is minimal—it is a basis. \square

Key Concepts from this Section

- **linearly independent definition 1:** (page 129) A collection of vectors $\{v_1, v_2, v_3, \dots, v_n\}$ in a vector space V is called *linearly independent* if the only way for a linear combination $a_1v_1 + a_2v_2 + a_3v_3 + \dots + a_nv_n$ to equal the zero vector 0_V is for all of the scalars a_1 through a_n to be zero: $a_1 = a_2 = a_3 = \dots = a_n = 0$.
- **linearly independent definition 2:** (page 129) Equivalently, we could say that a collection of vectors $\{v_1, v_2, v_3, \dots, v_n\}$ is linearly independent if and only if for any $v \in \langle v_1, v_2, v_3, \dots, v_n \rangle$,

there is one and only one linear combination of $\{v_1, v_2, v_3, \dots, v_n\}$ that equals v . That is, there is exactly one set of coefficients a_1, a_2, \dots, a_n such that $v = a_1v_1 + a_2v_2 + \dots + a_nv_n$. The coefficients (a_1, a_2, \dots, a_n) themselves are the coordinates of v in the skewed coordinate system determined by the vectors $\{v_1, v_2, v_3, \dots, v_n\}$. There is only one skewed coordinate coordinate reading that yields v .

- **linearly independent definition 3:** (page 129) A collection of vectors $B = \{v_1, v_2, v_3, \dots, v_n\}$ is linearly independent if and only if each vector in the collection is not in the span of the other vectors. That is, for any $v \in B$, then $v \notin \langle B \setminus \{v\} \rangle$.
- **theorem 2.2.1 linear independence: definition equivalence:** (page 130) All three definitions of linear independence are equivalent.
- **linearly dependent:** (page 130) If a collection of vectors is not linearly independent, then it is linearly dependent.
- **method for determining if a collection is linearly independent or dependent:** (page 132) Suppose that we have a vector collection $\{v_1, v_2, \dots, v_n\} \subset \mathbb{R}^m$. Then, create the function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ by the following rule:

$$(a_1, a_2, \dots, a_n) \mapsto a_1v_1 + a_2v_2 + \dots + a_nv_n$$

If the function is injective, the vectors in the collection are independent. Otherwise, they are dependent. Since this function is additive, it suffices to check the size of $f^{-1}(0_{\mathbb{R}^m})$, which is the set of solutions to a system of equations. If it has only one element, then f is injective and so the collection is linearly independent. Otherwise, the collection is linearly dependent.

- **basis definition 2:** (page 132) A basis for a vector space V is a collection of vectors which is linearly independent and which spans all of V .
- **theorem 2.2.2 basis definition equivalence:** (page 132) The two definitions for a *finite* basis are equivalent.
- **corollary 2.2.3 dimension of \mathbb{R}^n :** (page 133) The dimension of \mathbb{R}^n is n .
- **corollary 2.2.4 condition for linear independence by counting:** (page 133) If a collection of vectors is not a minimal spanning set, then it is not linearly independent.
- **proving that a set is or is not a basis:** (page 134) Suppose that we are working in \mathbb{R}^3 which has dimension 3 and are considering the set of vectors

$$\{(a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3)\}.$$

To see if these vectors are a basis or not, we form an *additive* function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ given by

$$(x, y, z) \mapsto x \cdot (a_1, b_1, c_1) + y \cdot (a_2, b_2, c_2) + z \cdot (a_3, b_3, c_3)$$

which can also be written as:

$$(x, y, z) \mapsto (a_1x + a_2y + a_3z, b_1x + b_2y + b_3z, c_1x + c_2y + c_3z).$$

If this function is injective, the set of vectors is a basis. If not, then it is not a basis. Injectivity is checked right at the fiber $f^{-1}(0, 0, 0)$.

- **theorem 2.2.5 subspace dimension:** (page 135) Given a vector space V and a subspace W , suppose that $\dim(W) = \dim(V)$. This means that $W = V$.
- **free rank:** (page 136) Let R be a ring. The Free rank of an R -module M is the least number of R -linearly independent elements whose span is all of M . Such a minimal collection is called a free basis for the R -module. The free rank of a vector space is simply its dimension.
- **finitely generated:** (page 136) A vector space is finitely generated if it is the span of a finite number of vectors.
- **theorem 2.2.6 finitely generated vector spaces have bases:** (page 136) Every finitely generated vector space has a basis and a dimension.

2.2.4 Exercises

Computation Practice

- 1.** Given the following collection of vectors in \mathbb{R}^4 , determine whether or not these vectors are linearly independent:

$$\{(1, 0, 1, 1), (1, 1, 1, 1), (0, 1, 1, 1)\}$$

- 2.** Find a subcollection of the collection $\{(1, 3, 0), (1, 0, 2), (1, -1, 1), (0, 1, 1)\}$ vectors which is a basis for \mathbb{R}^3 .

- 3.** Suppose that there is a collection of 8 vectors in \mathbb{C}^5 . Explain why this collection must be linearly dependent.

- 4.** Explain why the following set of vectors in \mathbb{R}^2 is linearly dependent:

$$v = (1, 1), \quad u = (1, 0), \quad w = (1, 2)$$

Suppose that $av + bu + cw = (0, 0)$. Find an example of a , b , and c that makes this work such that at least one of a , b , and c is nonzero.

- 5.** Given the following collection of vectors in \mathbb{R}^3 , show that they are linearly dependent:

$$\{(1, 0, -2), (1, 1, 1), (1, 2, 4)\}$$

- 6.** Explain why \mathbb{F}_5^2 has no free \mathbb{Z} -basis as a \mathbb{Z} -module.

Proof Practice

- 7.** Prove the statement: *A (finite) minimal spanning set S in a vector space V is linearly independent.* See the hints given for [Theorem 2.2.2](#) in the text.

- 8.** Prove: *If V is the span of a set of linearly independent vectors $S = \{v_1, v_2, \dots, v_n\}$, then if $v \in V$, there*

is one and only one way to represent v as a linear combination $v = a_1v_1 + a_2v_2 + \cdots + a_nv_n$. See the hints given for [Theorem 2.2.1](#) in the text.

- 9.** Prove that the following collection of vectors in \mathbb{R}^3 is linearly dependent:

$$(1, 4, 2), (1, 0, 1), (-6, -8, -8)$$

- 10.** Prove that $\mathbb{F}_2 \times \mathbb{F}_2$ is a vector space with scalars in \mathbb{F}_2 of dimension 2.

Extra Computation Practice

Determine if the following sets of vectors in \mathbb{R}^3 are linearly independent or linearly dependent

11. $(2, 4, 3), (0, -4, 4), (-8, -6, -13)$

12. $(1, 1, -1), (-3, -2, -1), (3, -1, 4)$

13. $(1, -1, 1), (-4, -3, 4), (-9, 6, 6)$

14. $(-5, -3, 2), (2, 2, -5), (22, 14, -13)$

15. $(-2, 3, 4), (2, 2, 2), (-4, -4, -32)$

16. $(4, 0, -2), (0, -5, -4), (-16, -20, -8)$

17. $(-2, -4, 2), (1, 3, 4), (4, 4, -24)$

18. $(1, -3, -3), (1, -3, -5), (0, 0, 6)$

19. $(-1, 2, 1), (3, -4, -2), (-5, 4, 3)$

20. $(1, 2, 3), (-2, -1, -4), (-7, -6, -10)$

21. $(1, 0, 3), (4, 4, -3), (-3, 1, -1)$

22. $(2, -1, 1), (1, 2, 2), (3, 3, -2)$

23. $(3, 4, -5), (-4, -4, 2), (-24, -16, 32)$

24. $(-1, -5, -2), (-1, -3, -3), (0, 2, -1)$

25. $(-1, -3, 0), (-3, 2, -5), (-1, -3, 0)$

26. $(-3, -4, 3), (-5, -1, 1), (0, -3, -4)$

27. $(3, 1, -2), (-3, 1, -3), (0, 0, -2)$

28. $(2, 4, -4), (-5, 2, -1), (-14, -4, 4)$

29. $(2, 2, -3), (1, -1, 2), (-6, -6, 9)$

30. $(1, -3, -2), (-3, 3, -2), (-5, 13, 2)$

31. $(-4, -1, -4), (3, 1, -4), (3, -2, 4)$

32. $(0, -5, -1), (-1, 2, 2), (-6, 13, -1)$

33. $(-5, -2, -2), (-3, -2, 4), (7, 7, 4)$

34. $(-4, -3, 4), (3, 3, -5), (-2, -9, 8)$

35. $(-4, 2, 1), (4, 0, -4), (-4, -4, 10)$

36. $(4, 3, 4), (-2, 3, 4), (2, -2, -1)$

37. $(4, -1, -3), (-1, 3, 1), (-5, 4, -5)$

38. $(-2, 1, -2), (-3, 2, 2), (-14, 8, -4)$

39. $(-5, -2, -2), (0, 4, -4), (-2, 3, -2)$

40. $(1, -4, -2), (-3, 4, 1), (4, 1, -2)$

41. $(-1, -5, -2), (-1, 3, 2), (3, -7, -4)$

42. $(-3, -3, 2), (1, 4, 1), (-12, -12, 8)$

43. $(4, -1, -3), (1, 2, -3), (-9, -1, 10)$

44. $(4, 1, -1), (-1, 4, 4), (1, 0, -2)$

45. $(3, 1, -5), (4, -2, 1), (-19, -3, 24)$

46. $(-2, 4, -5), (-5, -4, -1), (-2, -24, 18)$

47. $(2, 3, -1), (3, 3, 3), (-12, -7, -3)$

48. $(2, -2, 2), (1, 2, 3), (-7, 1, -4)$

49. $(0, -4, -4), (1, 0, 1), (4, -8, -7)$

50. $(3, -2, 2), (4, -3, -2), (-9, 6, -6)$

2.2.5 Solutions

1. We consider linear combinations $a \cdot (1, 0, 1, 1) + b \cdot (1, 1, 1, 1) + c \cdot (0, 1, 1, 1) = (a+b, b+c, a+b+c, a+b+c)$. We just check to see if the additive function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^4$ given by $f(a, b, c) = (a+b, b+c, a+b+c, a+b+c)$ is injective. We consider the preimage of $(0, 0, 0, 0)$ which amounts to solving the system of equations:

$$\begin{aligned} a + b &= 0 \\ b + c &= 0 \\ a + b + c &= 0 \\ a + b + c &= 0 \end{aligned}$$

The first equation with $a + b = 0$ changes the third equation $\underbrace{a + b + c}_= 0 = 0$ so that $c = 0$. Then the second equation becomes $b = 0$ which then forces $a = 0$ from the first equation. Hence, the only point in the fiber is $(0, 0, 0)$. Hence, f is injective and the three vectors are linearly independent.

2. Since the dimension of \mathbb{R}^3 is 3, then we need exactly 3 vectors that are linearly independent. Consider the linear combinations

$$a \cdot (1, 3, 0) + b \cdot (1, 0, 2) + c \cdot (1, -1, 1) + d \cdot (0, 1, 1) = (a + b + c, 3a - c + d, 2b + c + d).$$

Let's start with a function $f : \mathbb{R}^4 \rightarrow \mathbb{R}^3$ given by $(a, b, c, d) \mapsto (a + b + c, 3a - c + d, 2b + c + d)$. Consider the fiber $f^{-1}(0, 0, 0)$. Which of the values a, b, c , or d can we ignore so that the fiber only has one element in it? Consider

$$\begin{aligned} a + b + c &= 0 \\ 3a - c + d &= 0 \\ 2b + c + d &= 0 \end{aligned}$$

If we ignore a , then the first equation would tell us $b = -c$ so that the third equation would become $-c + d = 0$ which would be the same as the second equation. This would allow there to be more than one solution. *so we cannot ignore a.* Let's try ignoring d . Then the third equation would tell us that $c = -2b$ so that the first equation is $a - b = 0$ so that $a = b$. Hence, with these two equalities, the second equation becomes $3b + 2b = 0$ so that $b = 0$. Therefore, the third equation would tell us $c = 0$. This implies that $a = 0$. Hence, if we ignore d , that is enough! Specifically, the function $g : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ given by $g(a, b, c) = (a + b + c, 3a - c, 2b + c)$ has only $(0, 0, 0)$ in the fiber $g^{-1}(0, 0, 0)$. Consequently, the first three vectors are linearly independent and therefore make up a basis of \mathbb{R}^3 .

3. The dimension of \mathbb{C}^5 is 5. That means that the collection is not a minimal spanning set. Hence, it is not linearly dependent.

4. The set of vectors is dependent because there is more than 2 and the dimension of \mathbb{R}^2 is 2. There are many solutions for a , b , and c . You can think:

$$a \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + b \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + c \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Then,

$$\begin{aligned} a + b + c &= 0 \\ a + 2c &= 0 \end{aligned}$$

Just assume one of the variables is equal to 1 and solve for the others. Then, check to make sure the linear combination holds. For instance, if $c = 1$, then $a = -2$. This forces $b = 1$. You can check that this works!

5. Consider the function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ given by $(a, b, c) \mapsto (a + b + c, b + 2c, -2a + b + 4c)$ and consider $f^{-1}(0, 0, 0)$. We get a system of equations

$$\begin{aligned} a + b + c &= 0 \\ b + 2c &= 0 \\ -2a + b + 4c &= 0 \end{aligned}$$

The second equation tells us that $b = -2c$ so that the first equation becomes $a - c = 0$ so that $a = c$. Using these two equalities gives that the third equation is true no matter what c is since it reduces to $0 = 0$. Therefore, anything that looks like $(c, -2c, c)$ is a solution. In particular, $(1, -2, 1)$ and $(0, 0, 0)$ are both in $f^{-1}(0, 0, 0)$. Therefore, the vectors are linearly dependent.

6. Note that a linear combination with all the scalars being 5 is the same as a linear combination with all of the scalars being 0 for *any* collection of zeros because multiplication by 5 and then division by 5 always gives a remainder of 0. For a non-vector space module, linear independence must be checked in order for a minimal spanning set to be a basis!

7. Let's first prove that a minimal spanning set is linearly independent. Suppose that $S = \{v_1, v_2, \dots, v_n\}$ is a minimal spanning set. Then by way of contradiction, let's assume that it is not linearly independent. This means that there exist scalars a_1, a_2, \dots, a_n not all zero such that $a_1v_1 + a_2v_2 + \dots + a_nv_n = 0$. This means that at least one of the scalars a_1, a_2, \dots, a_n is nonzero. By reordering our list, we can assume without loss of generality that $a_1 \neq 0$. This means that

$$a_1v_1 + a_2v_2 + \dots + a_nv_n = 0$$

$$a_1v_1 = -a_2v_2 - \dots - a_nv_n$$

$$v_1 = -\frac{a_2}{a_1}v_2 - \dots - \frac{a_n}{a_1}v_n$$

Therefore, $v_1 \in \langle v_2, \dots, v_n \rangle$ which means that V can be spanned by $n - 1$ vectors instead of n . But we had assumed that S which has n vectors was a minimal spanning set. This is a contradiction.

8. Suppose that

$$v = a_1v_1 + a_2v_2 + \cdots + a_nv_n = b_1v_1 + b_2v_2 + \cdots + b_nv_n.$$

where $a_i \neq b_i$ for some $i \in \{1, 2, \dots, n\}$. Without loss of generality, we can reorder the indices so that $a_1 \neq b_1$. Then if we subtract both one representation for v from the other, we obtain:

$$(a_1 - b_1)v_1 + (a_2 - b_2)v_2 + \cdots + (a_n - b_n)v_n = 0.$$

But since S is linearly independent, then $(a_1 - b_1) = 0, (a_2 - b_2) = 0, \dots, (a_n - b_n) = 0$. This contradicts the fact that $a_1 \neq b_1$. Hence, we cannot have two distinct representations of any vector v as a linear combination of the vectors in S .

9. All we need to do is to show that the collection does not satisfy the criterion in the definition of being linearly independent. Either by inspection or by trying to solve a system of equations to find a dependency, we find that $-2 \cdot (1, 4, 2) - 4 \cdot (1, 0, 1) = (-6, -8, -8)$. This means that

$$-2 \cdot (1, 4, 2) - 4 \cdot (1, 0, 1) - 1 \cdot (-6, -8, -8) = 0$$

so that a nonzero linear combination of these vectors is zero. This means that the vectors cannot be linearly independent. Therefore, they are linearly dependent.

10. The vectors $(1, 0)$ and $(0, 1)$ are linearly independent since $a \cdot (1, 0) + b \cdot (0, 1) = (a, b) = (0, 0)$ with $a, b \in \mathbb{F}_2$ can only happen when $a = b = 0$. They are a minimal spanning set and so the dimension is 2. Since \mathbb{F}^2 is an additive group in each component, it is an additive group. It is closed under rescaling the same way that \mathbb{R}^2 is with scalars in \mathbb{R} . *Just definition match!*

11. linearly independent

12. linearly independent

13. linearly independent

14. linearly dependent

15. linearly independent

16. linearly dependent

17. linearly dependent

18. linearly dependent

19. linearly independent

20. linearly independent

21. linearly independent

22. linearly independent

23. linearly independent

24. linearly dependent

25. linearly dependent

26. linearly independent

27. linearly independent

28. linearly independent

29. linearly dependent

30. linearly independent

31. linearly independent

32. linearly independent

33. linearly independent

34. linearly independent

35. linearly dependent

36. linearly independent

37. linearly independent

38. linearly dependent

39. linearly independent

40. linearly independent

41. linearly independent

42. linearly dependent

43. linearly dependent

44. linearly independent

45. linearly dependent

46. linearly dependent

47. linearly independent

48. linearly independent

49. linearly independent

50. linearly dependent

Matrix Functions: Linear Transformations

2.3

2.3.1 Linear Transformations	147
2.3.2 Matrices are Just Functions of Column Vectors	149
2.3.3 Matrices are Functions of Row Vectors	154
2.3.4 Matrix Multiplication From a Column Interpretation	156
2.3.5 Matrix Multiplication From a Row Interpretation	158
2.3.6 Fast Matrix Squaring	161
2.3.7 Exercises	167
2.3.8 Solutions	171

Questions to Guide Your Study:

- *How can you think of a matrix as a function? What role does linear independence play?*
- *What is a linear transformation? What does it mean for a function to be scalable?*
- *How can you determine the range, domain and codomain of a linear transformation determined by a matrix?*
- *What is the row interpretation versus the column interpretation of multiplying matrices?*

2.3.1 Linear Transformations

We have talked about vector spaces and even see some additive functions between them. Functions between vector spaces that are additive and also *scalable* are called *linear transformations*.

Scalable Function

A function $f : D \rightarrow C$ such that both D and C admit a scalar multiplication by elements in \mathbb{R} is called *scalable* if scaling is preserved. That is, if we scale before we apply the function or after, the final result in the codomain is the same:

$$f(\underbrace{r \cdot v}_{\text{scale before}}) = \underbrace{r \cdot f(v)}_{\text{scale after}}$$

Linear Transformation

A *linear transformation* is a function $f : V \rightarrow W$ between vector spaces V and W that is both:

- additive
- scalable

This simply means that a linear transformation will preserve addition and scaling—the two major components of a vector space. In fact, even more is true, it preserves the vector space structure:

Theorem 2.3.1 Linear Transformations Preserve Structure

Given a linear transformation $f : V \rightarrow W$, then:

- $f(0_V) = 0_W$. *The additive identity of the domain is sent to the additive identity of the codomain.*
- $f(-v) = -f(v)$. *Additive inverses in the domain are sent to additive inverses in the codomain.*

In particular, because linear transformations preserve addition, they preserve parallelograms. A linear transformation is like a morphing of one space into another: it is like a change of coordinates and/or dimensions in a way that preserves parallelograms. But before we explore some examples, let's discuss one interpretation of how they work.

2.3.2 Matrices are Just Functions of Column Vectors



We are going to explain how all we need is a matrix, an array of numbers, to describe a linear transformation between vector spaces. The key ingredient that we will use is:

Theorem 2.3.2 Linear Transformations and Linear Combinations

A linear transformation $f : V \rightarrow W$ will preserve linear combinations. That is,

$$f(a_1v_1 + a_2v_2 + \cdots + a_nv_n) = a_1f(v_1) + a_2f(v_2) + \cdots + a_nf(v_n).$$

What we first need is a nice linearly independent set of vectors that spans the domain—a choice of basis. For now, let's focus our attention on vector spaces that look like \mathbb{R}^n for some $n \in \mathbb{N}$. In this case, we have a very nice **standard basis**:

Standard Basis Vectors

In the vector space \mathbb{R}^n , we have the *standard basis*:

$$\underbrace{(1, 0, 0, \dots, 0)}_{e_1}, \underbrace{(0, 1, 0, \dots, 0)}_{e_2}, \underbrace{(0, 0, 1, \dots, 0)}_{e_3}, \dots, \underbrace{(0, 0, 0, \dots, 1)}_{e_n}$$

where e_i is the n -tuple that has a 1 in position i and zeros elsewhere.

Because a basis is linearly independent, there is one and only one way to represent a vector as a linear combination of that basis. This gives us a way to make a well-defined function *by just knowing where to send the basis elements*:

$$\begin{aligned} (2, 3, 4) &= 2 \cdot (1, 0, 0) + 3 \cdot (0, 1, 0) + 4 \cdot (0, 0, 1) \\ f((2, 3, 4)) &= 2 \cdot (2, 1, 0) + 3 \cdot (-1, 0, 1) + 4 \cdot (2, 1, 0) \end{aligned}$$

Suppose that we are constructing a function $\mathbb{R}^3 \rightarrow \mathbb{R}^3$. To construct the function, all we do is determine where the function will send the standard basis elements e_1 , e_2 , and e_3 . Then, we can send an arbitrary vector $v = (a, b, c) = a \cdot e_1 + b \cdot e_2 + c \cdot e_3$ to $a \cdot f(e_1) + b \cdot f(e_2) + c \cdot f(e_3)$. This process produces a well-defined function since we cannot represent v as $a_1 \cdot e_1 + b_1 \cdot e_2 + c_1 \cdot e_3$ for coefficients a_1 , b_1 , c_1 which are different from a , b , c by the linear independence of e_1 , e_2 , and e_3 . If we could, then we would be confused about

which representation to use in finding the image of v :

$$a \cdot e_1 + b \cdot e_2 + c \cdot e_3 \stackrel{?}{=} a_1 \cdot e_1 + b_1 \cdot e_2 + c_1 \cdot e_3$$

only if $a = a_1$, $b = b_1$, $c = c_1$

We do not need to worry about obtaining $a \cdot f(e_1) + b \cdot f(e_2) + c \cdot f(e_3)$ versus $a_1 \cdot f(e_1) + b_1 \cdot f(e_2) + c_1 \cdot f(e_3)$ because there is *only one* set of scalars a , b , and c that actually works. This type of function is a *linear transformation*. How do we write such a function? With a matrix:

$$\begin{pmatrix} 2 & -1 & 2 \\ 1 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \begin{matrix} f(e_1) & f(e_2) & f(e_3) \end{matrix}$$

Then, to compute $f(2, 3, 4)$, we write $(2, 3, 4)$ as a column on the right and turn its entries into scalars that multiply to corresponding columns:

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

$$2 \cdot f(e_1) \quad 3 \cdot f(e_2) \quad 4 \cdot f(e_3)$$

This correspondence changes one linear combination into another which uses the same scalars 2, 3, and 4:

$$(2, 3, 4) = 2 \cdot e_1 + 3 \cdot e_2 + 4 \cdot e_3 \mapsto 2 \cdot f(e_1) + 3 \cdot f(e_2) + 4 \cdot f(e_3)$$

$$\begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix} + \begin{pmatrix} -3 \\ 0 \\ -3 \end{pmatrix} + \begin{pmatrix} 8 \\ 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 7 \\ 6 \\ -3 \end{pmatrix}$$

$$2 \cdot f(e_1) + 3 \cdot f(e_2) + 4 \cdot f(e_3) = f(2, 3, 4)$$

The process just illustrated is called **matrix multiplication**—but really, it is just plugging a vector into a function determined by a matrix. We call this the *column interpretation of a matrix function*:

Column Interpretation of Matrix Input

Suppose that we have a matrix

$$\begin{pmatrix} c_1 & c_2 & \cdots & c_n \end{pmatrix}$$

where $c_1, c_2, \dots, c_n \in \mathbb{R}^m$ represent its columns. Then, the matrix represents a linear transformation $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ such that $f(e_1) = c_1, f(e_2) = c_2, \dots, f(e_n) = c_n$. To compute $f(a_1, a_2, \dots, a_n)$, simply take the following linear combination:

$$a_1 \cdot c_1 + a_2 \cdot c_2 + \cdots + a_n \cdot c_n$$

- The domain is $\mathbb{R}^{\text{Number of Columns}}$.
- The codomain is $\mathbb{R}^{\text{Number of Rows}}$.

Column Space

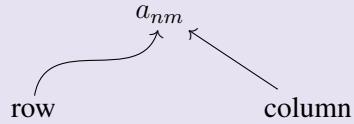
The range of a matrix

$$\begin{pmatrix} c_1 & c_2 & \cdots & c_n \end{pmatrix}$$

under the column interpretation is the span of the columns of the matrix $\langle c_1, c_2, \dots, c_n \rangle$. If the columns $c_1, c_2, \dots, c_n \in \mathbb{R}^m$, then this span is a subspace of \mathbb{R}^m . We call it the *column space* of the matrix.

Matrix Labeling Notation

A matrix is a *table* or an *array* of numbers. If we use a capital letter A to represent the matrix, then we use a lowercase letter a with subscripts to represent the entries in the array. In particular, we use the convention:



to write:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix}$$

We say that the matrix A is a $m \times n$ matrix where m is the number of rows and n is the number of columns.

Example 1. With the column interpretation, the following matrix is an example of a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$:

$$\mathbb{R}^3 \leftarrow \left\{ \begin{pmatrix} 1 & 2 \\ 0 & -1 \\ 3 & 1 \end{pmatrix} \right.$$

\mathbb{R}^2

The range of the matrix is the column space of the matrix—the span of the vectors $(1, 0, 3)$ and $(2, -1, 1)$. This span $\langle (1, 0, 3) (2, -1, 1) \rangle$ is a subspace of the codomain \mathbb{R}^3 .

If this matrix is labeled as A , then its entries are:

$$\begin{pmatrix} a_{11} = 1 & a_{12} = 2 \\ a_{21} = 0 & a_{22} = -1 \\ a_{31} = 3 & a_{32} = 1 \end{pmatrix}.$$

The matrix is a 3×2 matrix with 3 rows and 2 columns.



Example 2. *A matrix as a function.* Consider the following *matrix multiplication*. The matrix on

the left represents a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ and the one on the right represents an input vector $(1, 2)$:

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

Then, the result of the matrix multiplication is

$$f(1, 2) = 1 \cdot (1, 3, 0) + 2 \cdot (2, 1, 1) = (5, 5, 2).$$

Example 3. A matrix as a function.

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

The matrix on the left represents a function $f : \mathbb{R}^4 \rightarrow \mathbb{R}$. The result of the matrix multiplication is:

$$f(1, 2, 1, 0) = 1 \cdot (1) + 2 \cdot (5) + 1 \cdot (3) + 0 \cdot (2).$$

2.3.3 Matrices are Functions of Row Vectors

The following diagram shows how we can think of a matrix as being a function where the input is a vector written as a row on the left and the output is a corresponding linear combination of the rows of a matrix:

We have been viewing linear transformations from a column point of view. now, let's look at a row point of view. Suppose that we have a linear transformation f such that

$$f(e_1) = (2, -1, 2) \quad f(e_2) = (1, 0, 1) \quad f(e_3) = (0, -1, 0).$$

We can express this idea in the rows of a matrix:

$$\left(\begin{array}{ccc} 2 & -1 & 2 \\ 1 & 0 & 1 \\ 0 & -1 & 0 \end{array} \right) \begin{array}{l} f(e_1) \\ f(e_2) \\ f(e_3) \end{array}$$

Just as for the column interpretation, fixing the destinations of e_1 , e_2 , and e_3 , fixes the destinations of all other vectors in the domain. For example,

$$(2, 3, 4) = 2 \cdot e_1 + 3 \cdot e_2 + 4 \cdot e_3 \longmapsto 2 \cdot f(e_1) + 3 \cdot f(e_2) + 4 \cdot f(e_3)$$

In particular, we write the input *on the left as a row vector itself*. We input a row and we output a row as a linear combination of the rows that appear in the matrix itself.

$$\begin{pmatrix} 2 & 3 & 4 \end{pmatrix} \cdot \left(\begin{array}{ccc} 2 & -1 & 2 \\ 1 & 0 & 1 \\ 0 & -1 & 0 \end{array} \right) \begin{array}{l} 2 \cdot f(e_1) \\ + \\ 3 \cdot f(e_2) \\ + \\ 4 \cdot f(e_3) \\ \parallel \\ f(2, 3, 4) \end{array}$$

The diagram illustrates the mapping of the input row $(2, 3, 4)$ to the output row $f(2, 3, 4)$ through the matrix $\begin{pmatrix} 2 & -1 & 2 \\ 1 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$. Arrows show the components of the input row being distributed across the columns of the matrix. Specifically, the first component '2' is multiplied by the first column of the matrix, the second component '3' by the second column, and the third component '4' by the third column. These results are then summed to produce the final output row $f(2, 3, 4)$.

$$\begin{aligned}
 & 2 \cdot f(e_1) \quad \left(\begin{array}{ccc} 4 & -2 & 4 \end{array} \right) \\
 & + \\
 & 3 \cdot f(e_2) \quad \left(\begin{array}{ccc} 3 & 0 & 3 \end{array} \right) \\
 & + \\
 & 4 \cdot f(e_3) \quad \left(\begin{array}{ccc} 0 & -4 & 0 \end{array} \right) \\
 & \| \qquad \qquad \| \\
 & f(2, 3, 4) \quad \left(\begin{array}{ccc} 7 & -6 & 7 \end{array} \right)
 \end{aligned}$$

Row Interpretation of Matrix Input

Suppose that we have a $n \times m$ matrix

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}$$

where $r_1, r_2, \dots, r_n \in \mathbb{R}^m$ represent the columns of the matrix. Then, the matrix represents a linear transformation $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ such that $f(e_1) = r_1, f(e_2) = r_2, \dots, f(e_n) = r_n$. To compute $f(a_1, a_2, \dots, a_n)$, simply take the following linear combination:

$$a_1 \cdot r_1 + a_2 \cdot r_2 + \cdots + a_n \cdot r_n$$

- The domain is $\mathbb{R}^{\text{Number of Rows}}$.
- The codomain is $\mathbb{R}^{\text{Number of Columns}}$.

Row Space

The range of a matrix

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}$$

under the row interpretation is the span of the rows of the matrix $\langle r_1, r_2, \dots, r_n \rangle$. If the rows $r_1, r_2, \dots, r_n \in \mathbb{R}^m$, then this span is a subspace of \mathbb{R}^m . We call it the *row space* of the matrix.

Example 4. With the row interpretation, the following matrix is an example of a function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$:

$$\mathbb{R}^3 \longrightarrow \left\{ \begin{pmatrix} 1 & 2 \\ 0 & -1 \\ 3 & 1 \end{pmatrix} \right. \downarrow \left. \begin{array}{c} \\ \\ \end{array} \right\} \mathbb{R}^2$$

The range of the matrix is the row space of the matrix—the span of the vectors $(1, 2)$, $(0, -1)$, and $(3, 1)$. This span $\langle (1, 2), (0, -1), (3, 1) \rangle$ is a subspace of the codomain \mathbb{R}^2 .



Example 5. *Matrix function by a row interpretation.* The following computes $f(1, 2, -1)$ for the matrix function f described by the matrix on the right according to the row interpretation:

$$\underbrace{\begin{pmatrix} 1 & 2 & -1 \end{pmatrix}}_{\text{input}} \cdot \underbrace{\begin{pmatrix} 2 & 1 \\ 0 & 1 \\ 1 & -1 \end{pmatrix}}_f$$

We compute:

$$f(1, 2, -1) = 1 \cdot (2, 1) + 2 \cdot (0, 1) - 1 \cdot (1, -1) = (1, 4).$$

2.3.4 Matrix Multiplication From a Column Interpretation

With the column interpretation of matrix functions, *input to output* is the same as *right to left*: just as it is with standard function notation:

$$\underbrace{f(x)}_{\leftarrow}$$

When we compose two matrix functions f and g together as $f \circ g$, we can find a matrix that represents $f \circ g$ simply by finding:

$$\left(\begin{array}{cccc} & \textcolor{pink}{|} & \textcolor{pink}{|} & \textcolor{pink}{|} & \cdots & \end{array} \right) \quad \begin{array}{cccc} (f \circ g)(e_1) & (f \circ g)(e_2) & (f \circ g)(e_3) & \cdots \end{array}$$

We know how to plug e_1 into the matrix function for g . We get out a vector $g(e_1)$. Now plug this vector $g(e_1)$ into the matrix function f . We arrive at $(f \circ g)(e_1)$.

Matrix Function Multiplication/Composition (Column Interpretation)

Suppose we have two matrix functions f and g represented by the matrices A and B respectively.

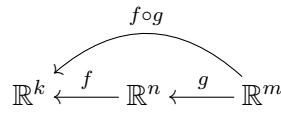
Suppose that the *columns* of A and the *columns* of B are notated as $A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}$ and $B = \begin{pmatrix} b_1 & b_2 & \cdots & b_m \end{pmatrix}$. Then, the matrix product $A \cdot B$ is the same as the matrix function for $f \circ g$. That is, the columns of $A \cdot B$ read as:

$$A \cdot B = \begin{pmatrix} (f \circ g)(e_1) & (f \circ g)(e_2) & \cdots & (f \circ g)(e_m) \end{pmatrix}$$

Notice that $g(e_1) = b_1$ so that $f(g(e_1)) = f(b_1) = A \cdot b_1$. Hence:

$$A \cdot B = \begin{pmatrix} A \cdot b_1 & A \cdot b_2 & \cdots & A \cdot b_m \end{pmatrix}.$$

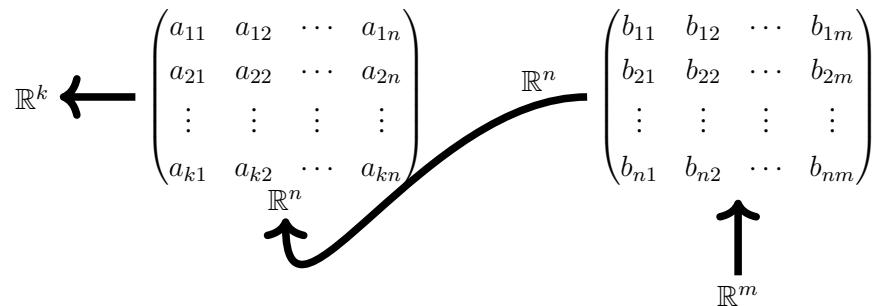
The codomain of g must match the domain \mathbb{R}^n of f . We have:



where k is the number of rows of A . The matrix A is a $k \times n$ matrix and the matrix B is a $n \times m$ matrix. The matrix $A \cdot B$ is a matrix with size:

$$(k \times n)(n \times m) = k \times m.$$

The following diagram depicts the flow of domain to codomain in a matrix multiplication with a column interpretation:

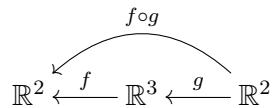


Example 6. *Matrix multiplication as composition.* Let's perform the following matrix multiplica-

tion:

$$\begin{pmatrix} 1 & 0 & 2 \\ 1 & 2 & 3 \\ f & & \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 4 & 2 \\ 0 & 1 \\ g & \end{pmatrix}$$

First notice that the multiplication is possible *since the composition is possible*: the codomain \mathbb{R}^3 of g matches the domain \mathbb{R}^3 of f :



Since $f \circ g$ has domain \mathbb{R}^2 and codomain \mathbb{R}^2 , it will be a 2×2 matrix. We just need to compute $(f \circ g)(e_1)$ and $(f \circ g)(e_2)$. The first of these is: $f(g(e_1)) = f(1, 4, 0) = 1 \cdot (1, 1) + 4 \cdot (0, 2) + 0 \cdot (2, 3) = (1, 9)$. This will be the first column.

Next, we compute $f(g(e_2)) = f(1, 2, 1) = 1 \cdot (1, 1) + 2 \cdot (0, 2) + 1 \cdot (2, 3) = (3, 8)$. Hence, turning these into columns, we arrive at the matrix:

$$\begin{pmatrix} 1 & 3 \\ 9 & 8 \end{pmatrix}.$$

2.3.5 Matrix Multiplication From a Row Interpretation

With the **row interpretation** of matrix functions, *input to output* is the same as *left to right*: the **right** way to read in English. Now finally, function composition can go in a sensible direction! *But notationally*, if we write $f \circ g$, we still mean that the function g acts first—what is different is how we write the matrix multiplication. If A is the matrix for g and B the matrix for f , then $\underbrace{A}_g \cdot \underbrace{B}_f$ corresponds to $f \circ g$. We'll get used to this.

But first, let's consider the mechanics of what it means to use the row interpretation to get a matrix for the composition of $f \circ g$:

$$(f \circ g)(e_1) \left(\begin{array}{c} \text{pink bar} \\ \text{pink bar} \\ \text{pink bar} \\ \vdots \end{array} \right)$$

$$(f \circ g)(e_2) \left(\begin{array}{c} \text{pink bar} \\ \text{pink bar} \\ \text{pink bar} \\ \vdots \end{array} \right)$$

$$(f \circ g)(e_3) \left(\begin{array}{c} \text{pink bar} \\ \text{pink bar} \\ \text{pink bar} \\ \vdots \end{array} \right)$$

We know how to plug e_1 into the matrix function for g . We get out a vector $g(e_1)$. Now plug this vector $g(e_1)$ into the matrix function f . We arrive at $(f \circ g)(e_1)$.

Matrix Function Multiplication/Composition (Row Interpretation)

Suppose we have a matrix function g represented by a matrix A and a matrix function f represented by the matrix B . Suppose that the *rows* of A and the *rows* of B are notated as

$A = \underbrace{\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}}_g$ and $B = \underbrace{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}}_f$. Then, the matrix product $\underbrace{A}_g \cdot \underbrace{B}_f$ is the same as the matrix function for $f \circ g$. That is, the rows of $A \cdot B$ read as:

$$A \cdot B = \begin{pmatrix} (f \circ g)(e_1) \\ (f \circ g)(e_2) \\ \vdots \\ (f \circ g)(e_n) \end{pmatrix}$$

Notice that $g(e_1) = a_1$ so that $f(g(e_1)) = f(a_1) = a_1 \cdot B$. Hence:

$$A \cdot B = \begin{pmatrix} a_1 \cdot B \\ a_2 \cdot B \\ \vdots \\ a_n \cdot B \end{pmatrix}.$$

The codomain of g must match the domain \mathbb{R}^m of f . We have:

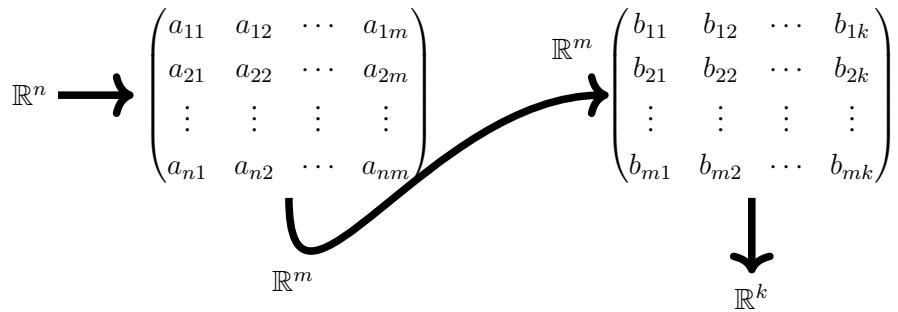
$$\mathbb{R}^n \xrightarrow{g} \mathbb{R}^m \xrightarrow{f} \mathbb{R}^k$$

$\nearrow^{f \circ g}$

where k is the number of columns of B . The matrix A is a $n \times m$ matrix and the matrix B is a $m \times k$ matrix. The matrix $A \cdot B$ is a matrix with size:

$$(n \times m)(m \times k) = n \times k.$$

The following diagram depicts the flow of domain to codomain in a matrix multiplication with a row interpretation:



Example 7. Video *Matrix multiplication by rows.* Consider the following matrix multiplication with a row interpretation:

$$\underbrace{\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}}_g \cdot \underbrace{\begin{pmatrix} 4 & 1 & 0 \\ 2 & 0 & -1 \end{pmatrix}}_f$$

First notice that the multiplication is possible *since the composition is possible*: the codomain \mathbb{R}^2 of g matches the domain \mathbb{R}^2 of f :

$$\mathbb{R}^2 \xrightarrow{g} \mathbb{R}^2 \xrightarrow{f} \mathbb{R}^3$$

$f \circ g$

Since $f \circ g$ has domain \mathbb{R}^2 and codomain \mathbb{R}^3 , it will be a 2×3 matrix. We compute:

$$\begin{pmatrix} (f \circ g)(e_1) \\ (f \circ g)(e_2) \end{pmatrix}$$

The first row is:

$$f(g(e_1)) = f(1, 2) = \begin{pmatrix} 1 \cdot (4, 1, 0) \\ + \\ 2 \cdot (2, 0, -1) \end{pmatrix} = (8, 1, -2).$$

This will be the first row. Next, we compute $f(g(e_2)) = f(0, 1) = \begin{pmatrix} 0 \cdot (4, 1, 0) \\ + \\ 1 \cdot (2, 0, -1) \end{pmatrix} = (2, 0, -1)$. Hence,

stacking these results, we arrive at the matrix:

$$\begin{pmatrix} 8 & 1 & -2 \\ 2 & 0 & -1 \end{pmatrix}.$$

Theorem 2.3.3 Row and Column Interpretations Give Same Product

Whether we use a column interpretation or a row interpretation for matrix multiplication, the result will be the same.

Proof. We will soon talk about matrix multiplication by partitioning (i.e. blocking). Coming up with the partitioning works equally in both interpretations since partitioning the “output” columns in the column interpretation or the “output” rows in the row interpretation *must be done in exactly the same way*. Further, every partitioning just divides up the process to yield the same result. That is, *it does not matter what partition we use*—the result is always the same as long as we stick to one of our interpretations for matrix multiplication. Suppose that we use the column interpretation the whole time we matrix multiply. If we use the smallest sizes of blocks—namely 1×1 blocks, it is clear that if used the row interpretation instead, the results would be the same! The sums of 1×1 multiplied to 1×1 matrices is equivalent in both interpretations. \square

2.3.6 Fast Matrix Squaring

Suppose that we have

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

Let's compute $A^2 = A \cdot A$ according to a column interpretation. To get the first column of A^2 , we think:

$$A \cdot A \cdot e_1 = A \cdot (A \cdot e_1) = A \cdot (\text{first column of } A)$$

$$\left(\begin{array}{ccc} 2 & 0 & -1 \\ 1 & 1 & 0 \\ 0 & 3 & 1 \end{array} \right) \cdot \left(\begin{array}{c} 2 \\ 1 \\ 0 \end{array} \right)$$

This comes out to:

$$2 \cdot \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix} + 0 \cdot \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \\ 3 \end{pmatrix}$$

Similarly, to compute the second column:

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

$\uparrow e_2$

$$0 \cdot \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix} + 3 \cdot \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -3 \\ 1 \\ 6 \end{pmatrix}$$

We continue for the third column:

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

$\uparrow e_3$

$$-1 \cdot \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix} + 1 \cdot \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -3 \\ -1 \\ 1 \end{pmatrix}$$

Hence,

$$A^2 = \begin{pmatrix} 4 & -3 & -3 \\ 3 & 1 & -1 \\ 3 & 6 & 1 \end{pmatrix}$$

We could have done the same thing with rows under a row interpretation.

We can square a matrix when we can compose the matrix thought of as a function with itself. *This means that the domain and the codomain must be the same.* Hence, there should be the same number of rows as columns in the matrix. The matrix would then look like a square. Wait!

We can square a matrix if it is square!

Square Matrix

A square matrix is a matrix that has the same number of rows as columns. If a matrix A is a square matrix, then we say that it is a $n \times n$ matrix for some positive integer n .

Fast Matrix Squaring

Suppose that A is a square matrix.

- The j th column of A^2 is the result of plugging in the j th column of A into the matrix A thought of as a function under a column interpretation.
- The j th row of A^2 is the result of plugging in the j th row of A into the matrix A thought of as a function under a row interpretation.

Key Concepts from this Section

- **scalable function:** (page 147) A function $f : D \rightarrow C$ such that both D and C admit a scalar multiplication by elements in \mathbb{R} is called *scalable* if scaling is preserved. That is, if we scale before we apply the function or after, the final result in the codomain is the same:

$$f(\underbrace{r \cdot v}_{\text{scale before}}) = \underbrace{r \cdot f(v)}_{\text{scale after}}$$

- **linear transformation:** (page 148) A *linear transformation* is a function $f : V \rightarrow W$ between vector spaces V and W that is both:
 - additive
 - scalable
 - **theorem 2.3.1 linear transformations preserve structure:** (page 148) Given a linear transformation $f : V \rightarrow W$, then:
 - $f(0_V) = 0_W$. *The additive identity of the domain is sent to the additive identity of the codomain.*
 - $f(-v) = -f(v)$. *Additive inverses in the domain are sent to additive inverses in the codomain.*
 - **theorem 2.3.2 linear transformations and linear combinations:** (page 149) A linear transformation $f : V \rightarrow W$ will preserve linear combinations. That is,
- $$f(a_1v_1 + a_2v_2 + \cdots + a_nv_n) = a_1f(v_1) + a_2f(v_2) + \cdots + a_nf(v_n).$$
- **standard basis:** (page 149) This is the basis of standard basis vectors for the vector space \mathbb{R}^n for $n \in \mathbb{N}$.

- **standard basis vectors:** (page 149) In the vector space \mathbb{R}^n , we have the *standard basis*:

$$\underbrace{(1, 0, 0, \dots, 0)}_{e_1}, \underbrace{(0, 1, 0, \dots, 0)}_{e_2}, \underbrace{(0, 0, 1, \dots, 0)}_{e_3}, \dots, \underbrace{(0, 0, 0, \dots, 1)}_{e_n}$$

where e_i is the n -tuple that has a 1 in position i and zeros elsewhere.

- **matrix multiplication:** (page 150) This is the process of composing two matrix functions (i.e. linear transformations represented by matrices).
- **column interpretation of matrix input:** (page 150) Suppose that we have a matrix

$$\begin{pmatrix} c_1 & c_2 & \cdots & c_n \end{pmatrix}$$

where $c_1, c_2, \dots, c_n \in \mathbb{R}^m$ represent its columns. Then, the matrix represents a linear transformation $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ such that $f(e_1) = c_1, f(e_2) = c_2, \dots, f(e_n) = c_n$. To compute $f(a_1, a_2, \dots, a_n)$, simply take the following linear combination:

$$a_1 \cdot c_1 + a_2 \cdot c_2 + \cdots + a_n \cdot c_n$$

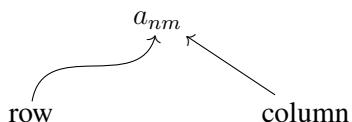
- The domain is $\mathbb{R}^{\text{Number of Columns}}$.
- The codomain is $\mathbb{R}^{\text{Number of Rows}}$.

- **column space:** (page 151) The range of a matrix

$$\begin{pmatrix} c_1 & c_2 & \cdots & c_n \end{pmatrix}$$

under the column interpretation is the span of the columns of the matrix $\langle c_1, c_2, \dots, c_n \rangle$. If the columns $c_1, c_2, \dots, c_n \in \mathbb{R}^m$, then this span is a subspace of \mathbb{R}^m . We call it the *column space* of the matrix.

- **matrix labeling notation:** (page 151) A matrix is a *table* or an *array* of numbers. If we use a capital letter A to represent the matrix, then we use a lowercase letter a with subscripts to represent the entries in the array. In particular, we use the convention:



to write:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix}$$

We say that the matrix A is a $m \times n$ matrix where m is the number of rows and n is the number of columns.

- **row interpretation of matrix input:** (page 155) Suppose that we have a $n \times m$ matrix

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}$$

where $r_1, r_2, \dots, r_n \in \mathbb{R}^m$ represent the columns of the matrix. Then, the matrix represents a linear transformation $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ such that $f(e_1) = r_1, f(e_2) = r_2, \dots, f(e_n) = r_n$. To compute $f(a_1, a_2, \dots, a_n)$, simply take the following linear combination:

$$a_1 \cdot r_1 + a_2 \cdot r_2 + \cdots + a_n \cdot r_n$$

- The domain is $\mathbb{R}^{\text{Number of Rows}}$.
- The codomain is $\mathbb{R}^{\text{Number of Columns}}$.

- **row space:** (page 155) The range of a matrix

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}$$

under the row interpretation is the span of the rows of the matrix $\langle r_1, r_2, \dots, r_n \rangle$. If the rows $r_1, r_2, \dots, r_n \in \mathbb{R}^m$, then this span is a subspace of \mathbb{R}^m . We call it the *row space* of the matrix.

- **matrix function multiplication/composition (column interpretation):** (page 156) Suppose we have two matrix functions f and g represented by the matrices A and B respectively. Suppose that the *columns* of A and the *columns* of B are notated as $A = (a_1 \ a_2 \ \cdots \ a_n)$ and $B = (b_1 \ b_2 \ \cdots \ b_m)$. Then, the matrix product $A \cdot B$ is the same as the matrix function for $f \circ g$. That is, the columns of $A \cdot B$ read as:

$$A \cdot B = ((f \circ g)(e_1) \ (f \circ g)(e_2) \ \cdots \ (f \circ g)(e_m))$$

- **matrix function multiplication/composition (row interpretation):** (page 158) Suppose we have a matrix function g represented by a matrix A and a matrix function f represented by the matrix B .

Suppose that the *rows* of A and the *rows* of B are notated as $A = \underbrace{\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}}_g$ and $B = \underbrace{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}}_f$. Then, the matrix product $\underbrace{A}_g \cdot \underbrace{B}_f$ is the same as the matrix function for $f \circ g$. That is, the rows of $A \cdot B$ read as:

$$A \cdot B = \begin{pmatrix} (f \circ g)(e_1) \\ (f \circ g)(e_2) \\ \vdots \\ (f \circ g)(e_n) \end{pmatrix}$$

- **theorem 2.3.3 row and column interpretations give same product:** (page 161) Whether we use a column interpretation or a row interpretation for matrix multiplication, the result will be the same.
- **square matrix:** (page 162) A square matrix is a matrix that has the same number of rows as columns. If a matrix A is a square matrix, then we say that it is a $n \times n$ matrix for some positive integer n .
- **fast matrix squaring:** (page 163) Suppose that A is a square matrix.
 - The j th column of A^2 is the result of plugging in the j th column of A into the matrix A thought of as a function under a column interpretation.
 - The j th row of A^2 is the result of plugging in the j th row of A into the matrix A thought of as a function under a row interpretation.

2.3.7 Exercises

Column Interpretation of Matrix Multiplication

Use the column interpretation to multiply the matrices and then determine what the domain and codomain are of the resulting matrix. Assume that the matrices are maps between \mathbb{R} -vector spaces of the form \mathbb{R}^n .

$$1. \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 & -1 \end{pmatrix}$$

$$2. \begin{pmatrix} 1 & -2 \\ 1 & -2 \\ -2 & -2 \\ -2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 & -1 & 0 \\ -2 & 0 & -1 & 2 \end{pmatrix}$$

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

$$4. \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \end{pmatrix}$$

$$5. \begin{pmatrix} 1 & 2 & -2 & 1 \\ 2 & -2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 & -1 \\ -2 & 0 \\ -1 & -2 \\ 2 & -2 \end{pmatrix}$$

$$6. \begin{pmatrix} -1 \\ -2 \\ 2 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \end{pmatrix}$$

$$7. \begin{pmatrix} 1 \end{pmatrix} \cdot \begin{pmatrix} -2 & -2 & -2 \end{pmatrix}$$

$$8. \begin{pmatrix} 2 \end{pmatrix} \cdot \begin{pmatrix} -1 \end{pmatrix}$$

$$9. \begin{pmatrix} 1 & 2 & 0 \\ 1 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & -2 \\ -1 & 2 & -1 \\ 2 & -1 & 0 \end{pmatrix}$$

$$10. \begin{pmatrix} 2 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \end{pmatrix}$$

$$11. \begin{pmatrix} 2 \\ 0 \\ 2 \\ -1 \end{pmatrix} \cdot \begin{pmatrix} 2 \end{pmatrix}$$

$$12. \begin{pmatrix} -1 & 2 & 0 & -2 \\ 2 & 0 & -1 & 1 \\ 1 & 2 & 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & -1 & 1 & 0 \\ -1 & 2 & -1 & -1 \\ -1 & 1 & 2 & -2 \\ -1 & 1 & -2 & 0 \end{pmatrix}$$

$$13. \begin{pmatrix} 2 & 1 & -1 & -1 \\ -1 & -1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 1 \\ 2 & 0 & 0 \\ 2 & -2 & 1 \end{pmatrix}$$

$$14. \begin{pmatrix} 2 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 & 0 \end{pmatrix}$$

$$15. \begin{pmatrix} 1 & -2 & 2 \end{pmatrix} \cdot \begin{pmatrix} -1 & -1 \\ 1 & -1 \\ 0 & -1 \end{pmatrix}$$

$$16. \begin{pmatrix} -1 & 1 & -2 \\ -2 & -2 & 2 \\ 2 & 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} -1 & -2 & -1 \\ 2 & 0 & 1 \\ -2 & 0 & 0 \end{pmatrix}$$

$$17. \begin{pmatrix} 0 & -2 & -2 & 0 \\ -2 & 0 & 0 & 0 \\ -2 & 0 & 2 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 \\ 1 & -2 \\ 1 & 2 \\ 2 & 0 \end{pmatrix}$$

$$18. \begin{pmatrix} -2 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 \end{pmatrix}$$

$$19. \begin{pmatrix} -1 \\ 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & -2 \end{pmatrix}$$

$$20. \begin{pmatrix} -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & -2 \end{pmatrix}$$

Row Interpretation of Matrix Multiplication

Use the row interpretation to multiply the matrices and then determine what the domain and codomain are of the resulting matrix. Assume that the matrices are maps between \mathbb{R} -vector spaces of the form \mathbb{R}^n .

$$21. \begin{pmatrix} 1 & -1 \\ -2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & -2 \\ -2 & 1 \end{pmatrix}$$

$$22. \begin{pmatrix} 2 & 1 \\ 2 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -2 \\ 2 & 1 \end{pmatrix}$$

$$23. \begin{pmatrix} -1 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} -1 & -1 & 1 \\ -1 & -2 & -1 \\ -2 & -2 & 0 \end{pmatrix}$$

$$24. \begin{pmatrix} 1 & -2 & 2 \\ 0 & 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -1 \\ -2 \end{pmatrix}$$

$$25. \begin{pmatrix} 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 & -1 \\ 2 & 0 & 1 \end{pmatrix}$$

$$26. \begin{pmatrix} 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 & 1 \end{pmatrix}$$

27. $\begin{pmatrix} 2 & 2 & 1 & 2 \\ -2 & 0 & 0 & -1 \\ 0 & 2 & 0 & 1 \\ -2 & -1 & -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & -2 \\ -2 & 0 \\ 0 & 1 \\ -1 & -2 \end{pmatrix}$

29. $\begin{pmatrix} -2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 2 & -1 \\ 0 & 0 & 0 & -2 \end{pmatrix}$

31. $\begin{pmatrix} -2 & 1 \\ 2 & 0 \\ 0 & -2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -2 \\ -1 & -2 \end{pmatrix}$

33. $\begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & -2 & 1 & 0 \\ 1 & 1 & 0 & -2 \end{pmatrix}$

35. $\begin{pmatrix} 2 & -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$

37. $\begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 & -2 \end{pmatrix}$

39. $\begin{pmatrix} 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & -1 & 2 & 0 \end{pmatrix}$

28. $\begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} -1 \end{pmatrix}$

30. $\begin{pmatrix} 1 & -1 & 1 & 0 \\ -1 & 0 & 1 & -1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & -2 & 0 & 0 \\ 2 & 2 & 1 & 2 \\ 1 & 1 & -1 & 2 \\ 1 & 2 & 1 & -2 \end{pmatrix}$

32. $\begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \\ 2 & 0 & -1 \\ -2 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}$

34. $\begin{pmatrix} -2 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & -1 & 1 & 2 \\ 0 & 2 & -2 & -1 \end{pmatrix}$

36. $\begin{pmatrix} 2 & 2 \\ 2 & -2 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 0 \end{pmatrix}$

38. $\begin{pmatrix} 2 & 2 & 2 & 0 \\ -1 & 0 & -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & -2 \\ 2 & -1 \\ 1 & -1 \\ 0 & -1 \end{pmatrix}$

40. $\begin{pmatrix} 0 & 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 & -1 \\ 2 & -2 & -1 \\ 2 & 0 & 2 \end{pmatrix}$

Matrix Squaring

Compute A^2 by using the technique in the section. You can do so by columns or rows.

$$\mathbf{41.} A = \begin{pmatrix} 0 & 0 & 2 \\ -2 & -2 & 2 \\ -1 & 1 & 0 \end{pmatrix}$$

$$\mathbf{42.} A = \begin{pmatrix} 0 & 0 \\ -2 & 2 \end{pmatrix}$$

$$\mathbf{43.} A = \begin{pmatrix} 0 & 0 & 2 & -1 \\ -2 & -2 & -2 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathbf{44.} A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ -1 & 0 & 2 & 0 \\ 0 & 0 & -2 & 2 \\ 1 & 1 & 1 & -2 \end{pmatrix}$$

$$\mathbf{45.} A = \begin{pmatrix} -2 & -1 \\ -1 & 2 \end{pmatrix}$$

$$\mathbf{46.} A = \begin{pmatrix} 0 & 2 & -1 & 0 \\ -2 & -1 & 0 & 1 \\ 0 & -2 & -1 & -1 \\ -2 & -2 & 0 & 2 \end{pmatrix}$$

$$\mathbf{47.} A = \begin{pmatrix} 0 & 0 & -1 & -2 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 2 \end{pmatrix}$$

$$\mathbf{48.} A = \begin{pmatrix} -2 & -2 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{49.} A = \begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix}$$

$$\mathbf{50.} A = \begin{pmatrix} 0 & -2 & 1 \\ 2 & -1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\mathbf{51.} A = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\mathbf{52.} A = \begin{pmatrix} 2 & 1 & -2 & -2 \\ 1 & 2 & 0 & -1 \\ -1 & 0 & 0 & 2 \\ 2 & -1 & 0 & 0 \end{pmatrix}$$

2.3.8 Solutions

1. $\begin{pmatrix} 4 & -2 & 2 \\ -2 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix} \quad f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

2. $\begin{pmatrix} 6 & 2 & 1 & -4 \\ 6 & 2 & 1 & -4 \\ 0 & -4 & 4 & -4 \\ -4 & -4 & 2 & 0 \end{pmatrix} \quad f : \mathbb{R}^4 \rightarrow \mathbb{R}^4$

3. $\begin{pmatrix} 1 \\ 2 \\ 2 \\ 0 \end{pmatrix} \quad f : \mathbb{R}^1 \rightarrow \mathbb{R}^4$

4. $\begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

5. $\begin{pmatrix} -1 & 1 \\ 1 & -4 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

6. $\begin{pmatrix} -2 \\ -4 \\ 4 \\ 2 \end{pmatrix} \quad f : \mathbb{R}^1 \rightarrow \mathbb{R}^4$

7. $\begin{pmatrix} -2 & -2 & -2 \end{pmatrix} \quad f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

8. $\begin{pmatrix} -2 \end{pmatrix} \quad f : \mathbb{R}^1 \rightarrow \mathbb{R}^1$

9. $\begin{pmatrix} -2 & 4 & -4 \\ -3 & 3 & -3 \end{pmatrix} \quad f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$

10. $\begin{pmatrix} 4 \\ 2 \end{pmatrix} \quad f : \mathbb{R}^1 \rightarrow \mathbb{R}^2$

11. $\begin{pmatrix} 4 \\ 0 \\ 4 \\ -2 \end{pmatrix} \quad f : \mathbb{R}^1 \rightarrow \mathbb{R}^4$

12. $\begin{pmatrix} 1 & 3 & 1 & -2 \\ -2 & -2 & -2 & 2 \\ -4 & 4 & 5 & -6 \end{pmatrix} \quad f : \mathbb{R}^4 \rightarrow \mathbb{R}^3$

13. $\begin{pmatrix} -2 & 1 & 2 \\ 1 & -2 & -1 \end{pmatrix} \quad f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$

14. $\begin{pmatrix} -2 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$

15. $\begin{pmatrix} -3 & -1 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

16. $\begin{pmatrix} 7 & 2 & 2 \\ -6 & 4 & 0 \\ -2 & -4 & 0 \end{pmatrix} \quad f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

17. $\begin{pmatrix} -4 & 0 \\ -4 & 2 \\ -6 & 6 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$

18. $\begin{pmatrix} 4 & -2 \\ 0 & 0 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

19. $\begin{pmatrix} 0 & 2 \\ 0 & -4 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

20. $\begin{pmatrix} 1 & 2 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

21. $\begin{pmatrix} 4 & -3 \\ -4 & 4 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

22. $\begin{pmatrix} 2 & -3 \\ -2 & -5 \\ 2 & 1 \end{pmatrix} \quad f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$

23. $\begin{pmatrix} -3 & -5 & -3 \\ -4 & -4 & 0 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$

24. $\begin{pmatrix} -1 \\ 3 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

25. $\begin{pmatrix} 6 & -2 & -1 \end{pmatrix} \quad f : \mathbb{R}^1 \rightarrow \mathbb{R}^3$

26. $\begin{pmatrix} 2 & -4 & 2 \end{pmatrix} \quad f : \mathbb{R}^1 \rightarrow \mathbb{R}^3$

27. $\begin{pmatrix} -10 & -7 \\ 5 & 6 \\ -5 & -2 \\ 6 & 3 \end{pmatrix} \quad f : \mathbb{R}^4 \rightarrow \mathbb{R}^2$

28. $\begin{pmatrix} -2 \\ 2 \\ -1 \end{pmatrix} \quad f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

29. $\begin{pmatrix} -4 & 0 & -4 & 4 \end{pmatrix} \quad f : \mathbb{R}^1 \rightarrow \mathbb{R}^4$

30. $\begin{pmatrix} 1 & -3 & -2 & 0 \\ -2 & 1 & -2 & 4 \\ 2 & 2 & 1 & 2 \end{pmatrix} \quad f : \mathbb{R}^3 \rightarrow \mathbb{R}^4$

31. $\begin{pmatrix} -1 & 2 \\ 0 & -4 \\ 2 & 4 \\ -1 & -2 \end{pmatrix} \quad f : \mathbb{R}^4 \rightarrow \mathbb{R}^2$

32. $\begin{pmatrix} 2 & 1 \\ 3 & 2 \\ 4 & 2 \\ -4 & -2 \end{pmatrix} \quad f : \mathbb{R}^4 \rightarrow \mathbb{R}^2$

33. $\begin{pmatrix} -1 & 3 & -1 & -2 \\ 2 & -2 & 1 & 0 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^4$

34. $\begin{pmatrix} 2 & 6 & -6 & -6 \\ -1 & 1 & -1 & 1 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^4$

35. $\begin{pmatrix} 2 \end{pmatrix} \quad f : \mathbb{R}^1 \rightarrow \mathbb{R}^1$

36. $\begin{pmatrix} 4 \\ 4 \\ -2 \end{pmatrix} \quad f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

37. $\begin{pmatrix} 1 & -2 & -2 \\ 2 & -4 & -4 \\ 0 & 0 & 0 \\ 1 & -2 & -2 \end{pmatrix} \quad f : \mathbb{R}^4 \rightarrow \mathbb{R}^3$

38. $\begin{pmatrix} 10 & -8 \\ -3 & 4 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

39. $\begin{pmatrix} -1 & -1 & 2 & 0 \end{pmatrix} \quad f : \mathbb{R}^1 \rightarrow \mathbb{R}^4$

40. $\begin{pmatrix} -2 & -2 & -5 \end{pmatrix} \quad f : \mathbb{R}^1 \rightarrow \mathbb{R}^3$

41. $\begin{pmatrix} -2 & 2 & 0 \\ 2 & 6 & -8 \\ -2 & -2 & 0 \end{pmatrix}$

42. $\begin{pmatrix} 0 & 0 \\ -4 & 4 \end{pmatrix}$

43. $\begin{pmatrix} 2 & 0 & -1 & 0 \\ 2 & 4 & 2 & -2 \\ 0 & 0 & 2 & -1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$

44. $\begin{pmatrix} 0 & 0 & -2 & 2 \\ 0 & 0 & -5 & 4 \\ 2 & 2 & 6 & -8 \\ -3 & -2 & -1 & 6 \end{pmatrix}$

45. $\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$

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

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

48. $\begin{pmatrix} 4 & 2 \\ 0 & 1 \end{pmatrix}$

49. $\begin{pmatrix} 4 & 0 \\ 2 & 0 \end{pmatrix}$

50. $\begin{pmatrix} -4 & 2 & 2 \\ -2 & -3 & 3 \\ 0 & 0 & 0 \end{pmatrix}$

51. $\begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$

52. $\begin{pmatrix} 3 & 6 & -4 & -9 \\ 2 & 6 & -2 & -4 \\ 2 & -3 & 2 & 2 \\ 3 & 0 & -4 & -3 \end{pmatrix}$

Matrix Block Multiplication

2.4

2.4.1 Column-Row Partition Blocks for Multiplication	174
2.4.2 Mixing Column-Row Partitions with Row-Column Partitions	177
2.4.3 Block Diagonal Matrices	182
2.4.4 The Standard Definition of Matrix Multiplication	185
2.4.5 Exercises	189
2.4.6 Solutions	193

Questions to Guide Your Study:

- *What is a matching column-row partition?*
- *What is a (possibly non-matching) column-row partition?*
- *What kinds of partitions are allowed for matrix block multiplication?*
- *Once you have a good partition, how do you use the blocks to matrix multiply?*
- *What is a block diagonal matrix?*
- *Why is multiplication of block diagonal matrices so simple?*

2.4.1 Column-Row Partition Blocks for Multiplication

Think about matrix multiplication under the column interpretation where we are taking a linear combination of columns. The columns are in the matrix on the left and the the scalars we multiply to the columns are in the matrix on the right:

$$\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \cdot \left(\begin{array}{cc} 1 & -1 \\ 1 & 0 \end{array} \right) = 1 \cdot \left(\begin{array}{c} 1 \\ 0 \end{array} \right) + 1 \cdot \left(\begin{array}{c} 1 \\ 1 \end{array} \right) + 1 \cdot \left(\begin{array}{c} -1 \\ 0 \end{array} \right)$$

Yet, we can organize our work in chunks as shown:

$$\left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right)_A \cdot \left(\begin{array}{cc} -1 & 0 \\ 0 & 1 \end{array} \right)_B = \left(\begin{array}{c} 1 \\ 1 \\ 1 \end{array} \right)_{C,D} = 1 \cdot \left(\begin{array}{c} 1 \\ 0 \end{array} \right) + 1 \cdot \left(\begin{array}{c} 1 \\ 1 \end{array} \right) + 1 \cdot \left(\begin{array}{c} -1 \\ 0 \end{array} \right)$$

$A \cdot C + B \cdot D$

Doing the same split up for each column, thinking that C has the *first scalars* and D has the *last scalars*, we can enlarge our matrix on the right and proceed as follows:

$$\left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right)_A \cdot \left(\begin{array}{cc} -1 & 0 \\ 0 & 1 \end{array} \right)_B = \left(\begin{array}{ccc} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{array} \right)_{C,D} = A \cdot C + B \cdot D$$

Matching Column-Row Partition

Suppose that we are multiplying two matrices A and B . Suppose that the columns of A are given by a_1, a_2, \dots, a_n and that the rows of B are given by b_1, b_2, \dots, b_n . Then, a matching column-row partition is a partition of these rows and columns which takes the same shape. For instance, if $n = 4$, then the partitions

$$A = \left(\begin{array}{c|cc|c} a_1 & a_2 & a_3 & a_4 \end{array} \right)$$

and

$$B = \left(\begin{array}{c} b_1 \\ b_2 \\ b_3 \\ b_4 \end{array} \right)$$

together make up a matching column-row partition with shape $(* | * \ * | *)$.

Column-Row Partition Multiplication

Suppose that we are multiplying two matrices A and B with a matching column-row partition. Call the chunks of the column partition of A as A_1, A_2, \dots, A_k and chunks of the row partition of B as B_1, B_2, \dots, B_k . Then:

$$A \cdot B = A_1 \cdot B_1 + A_2 \cdot B_2 + \cdots + A_k \cdot B_k.$$



Example 1. A simple partition blocking. Consider the matrix multiplication:

$$\left(\begin{array}{cccc} 1 & 0 & -1 & 1 \end{array} \right) \cdot \left(\begin{array}{c} 1 \\ 1 \\ 0 \\ 1 \end{array} \right).$$

We use the partition $\star \mid \star \star \mid \star$ on the rows and the columns:

$$\left(\begin{array}{c|cc|c} 1 & 0 & -1 & 1 \end{array} \right) \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 1 \cdot 1 + (0 \ -1) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 1 \cdot 1 = 2.$$



Example 2. Comparing two column-row partitions. We use two different column-row partitions.

First, let's use the partition $\star \mid \star \star \mid \star \star$:

$$\left(\begin{array}{c|cc|c} 1 & -1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{array} \right) \cdot \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \\ \hline 1 & 1 & -1 \end{pmatrix}$$

The result is:

$$\begin{aligned} & \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot (1 \ 1 \ 0) + \begin{pmatrix} -1 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot (1 \ 1 \ -1) \\ &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} -1 & 0 & -1 \\ 1 & 2 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & -1 \\ 2 & 3 & 0 \end{pmatrix}. \end{aligned}$$

Next, let's use the partition $\star \star \mid \star \star \star$:

$$\left(\begin{array}{cc|cc} 1 & -1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{array} \right) \cdot \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \\ \hline 1 & 1 & -1 \end{pmatrix}$$

The result is:

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

2.4.2 Mixing Column-Row Partitions with Row-Column Partitions

Consider the following diagram depicting a matching column-row partition $\star \star \mid \star \star$:

$$\left(\begin{array}{cc|c} 2 & 1 & -1 \\ 3 & 1 & 0 \end{array} \right) \cdot \left(\begin{array}{c} -2 \\ 4 \\ -3 \end{array} \right) = -2 \cdot \left(\begin{array}{c} 2 \\ 3 \end{array} \right) + 4 \cdot \left(\begin{array}{c} 1 \\ 1 \end{array} \right) - 3 \cdot \left(\begin{array}{c} -1 \\ 0 \end{array} \right)$$

We can divide up the result of the matrix multiplication by thinking of the top entry of each column separately from the lower entry by drawing horizontal lines as shown:

$$\left(\begin{array}{cc|c} 2 & 1 & -1 \\ 3 & 1 & 0 \end{array} \right) \cdot \left(\begin{array}{c} -2 \\ 4 \\ -3 \end{array} \right) = \frac{-2 \cdot \left(\begin{array}{c} 2 \\ 3 \end{array} \right) + 4 \cdot \left(\begin{array}{c} 1 \\ 1 \end{array} \right) - 3 \cdot \left(\begin{array}{c} -1 \\ 0 \end{array} \right)}{-2 \cdot \left(\begin{array}{c} 3 \\ 0 \end{array} \right) + 4 \cdot \left(\begin{array}{c} 1 \\ 0 \end{array} \right) - 3 \cdot \left(\begin{array}{c} 0 \\ 0 \end{array} \right)}$$

Now, if we add another column to the second matrix, we can similarly split up the left part of the result versus the right part of the result as follows:

$$\left(\begin{array}{cc|c} 2 & 1 & -1 \\ 3 & 1 & 0 \end{array} \right) \cdot \left(\begin{array}{c} -2 \\ 4 \\ -3 \\ | \\ 1 \\ 3 \\ -1 \end{array} \right) = \left(-2 \cdot \left(\begin{array}{c} 2 \\ 3 \end{array} \right) + 4 \cdot \left(\begin{array}{c} 1 \\ 1 \end{array} \right) - 3 \cdot \left(\begin{array}{c} -1 \\ 0 \end{array} \right) \quad \left| \quad 1 \cdot \left(\begin{array}{c} 2 \\ 3 \end{array} \right) + 3 \cdot \left(\begin{array}{c} 1 \\ 1 \end{array} \right) - 1 \cdot \left(\begin{array}{c} -1 \\ 0 \end{array} \right) \right) \right)$$

$$\left(\begin{array}{cc|c} 2 & 1 & -1 \\ 3 & 1 & 0 \end{array} \right) \cdot \left(\begin{array}{c|c} -2 & 1 \\ 4 & 3 \\ -3 & -1 \end{array} \right) = \left(-2 \cdot \left(\begin{array}{c} 2 \\ 3 \end{array} \right) + 4 \cdot \left(\begin{array}{c} 1 \\ 1 \end{array} \right) - 3 \cdot \left(\begin{array}{c} -1 \\ 0 \end{array} \right) \quad \left| \quad 1 \cdot \left(\begin{array}{c} 2 \\ 3 \end{array} \right) + 3 \cdot \left(\begin{array}{c} 1 \\ 1 \end{array} \right) - 1 \cdot \left(\begin{array}{c} -1 \\ 0 \end{array} \right) \right) \right)$$

Row-Column Partition (non-matching)

Suppose that we are multiplying two matrices A and B as $A \cdot B$. Suppose that the rows of A are given by a_1, a_2, \dots, a_m and that the rows of B are given by b_1, b_2, \dots, b_k . Then, a row-column partition *any* partition of the rows of A and *any* partition of the columns of B . For instance, if $m = 4$ and $k = 5$, then the partitions

$$A = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

and

$$B = \left(\begin{array}{c|ccccc} b_1 & b_2 & b_3 & b_4 & b_5 \end{array} \right)$$

together make up a *non-matching* row-column partition.

Matrix Partitioning Principle for Multiplication

As long as we keep the matching column-row partition, we can use *any not necessarily matching* “row-column” partition.

- The matching column-row partition reorganizes *the addition* that gives us the result.
- The row-column partition organizes *where we see* specific results.

Matrix Block Multiplication

Suppose that we have divided our matrices into blocks which follow a matching column-row partition and any kind of row-column partition.

We can just matrix multiply pretending that the blocks themselves are matrix entries.

Yet we must be careful on the order of multiplying matrix chunks! If a matrix chunk comes from the original left matrix, then it always goes on the left whenever we are multiplying with it among the blocks. If a matrix chunk comes from the original right matrix, then it always goes on the right whenever we are multiplying with it among the blocks.

Example 3. Mixed Blocking. Consider the multiplication of two matrices where we have used the column-row partition $(* | * * | *)$. We use a row-column partition such that the rows of the first matrix are all one

chunk together, but the columns of the second matrix are partitioned as follows:

$$\left(\begin{array}{c|cc|c} 1 & 0 & 1 & -1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & -1 & 0 \end{array} \right) \cdot \left(\begin{array}{c|cc} 1 & 1 & 1 \\ \hline 1 & 0 & 1 \\ 1 & 1 & 0 \\ \hline 1 & 0 & 1 \end{array} \right)$$

We label the chunks as follows and matrix multiply according to a row interpretation (both interpretations give the same result):

$$\begin{pmatrix} A & B & C \end{pmatrix} \cdot \begin{pmatrix} D & E \\ F & G \\ H & I \end{pmatrix} = \begin{pmatrix} AD & AE \\ BF & BG \\ CH & CI \end{pmatrix}$$

+
+
+

We get:

$$\begin{pmatrix} AD & AE \end{pmatrix} = \left(\begin{array}{c|c} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \cdot 1 & \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \end{pmatrix} \end{array} \right) = \left(\begin{array}{c|cc} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{array} \right)$$

$$\begin{pmatrix} BF & BG \end{pmatrix} = \left(\begin{array}{c|c} \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array} \right) = \left(\begin{array}{c|cc} 1 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & -1 & 1 \end{array} \right)$$

$$\begin{pmatrix} CH & CI \end{pmatrix} = \left(\begin{array}{c|c} \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \cdot 1 & \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \end{pmatrix} \end{array} \right) = \left(\begin{array}{c|cc} -1 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{array} \right)$$

Now, we add these results together:

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



Example 4. *Mixed blocking.* We repeat the last example but with a different row-column partition

(in the matrix on the left). The column-row partition of the multiplication $(\star | \star \star | \star)$ is the same.

$$\left(\begin{array}{c|cc|c} 1 & 0 & 1 & -1 \\ \hline 1 & 1 & 1 & 0 \\ \hline 0 & 1 & 0 & 1 \\ 1 & 1 & -1 & 0 \end{array} \right) \cdot \left(\begin{array}{c|cc} 1 & 1 & 1 \\ \hline 1 & 0 & 1 \\ \hline 1 & 1 & 0 \\ 1 & 0 & 1 \end{array} \right)$$

We label the chunks as follows and matrix multiply according to a row interpretation (both interpretations give the same result):

$$\left(\begin{array}{ccc} A & B & C \\ J & K & L \\ M & N & P \end{array} \right) \cdot \left(\begin{array}{cc} D & E \\ F & G \\ H & I \end{array} \right) = \left(\begin{array}{c|cc} \begin{array}{c} (AD \ AE) \\ + \\ (BF \ BG) \\ + \\ (CH \ CI) \end{array} & \hline & \begin{array}{c} (JD \ JE) \\ + \\ (KF \ KG) \\ + \\ (LH \ LI) \end{array} \\ \hline \begin{array}{c} (MD \ ME) \\ + \\ (NF \ NG) \\ + \\ (PH \ PI) \end{array} & \end{array} \right)$$

We get:

$$(AD \ AE) = (1 \cdot 1 | 1 \cdot (1 \ 1)) = (1 | 1 \ 1)$$

$$(BF \ BG) = \left((0 \ 1) \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \middle| (0 \ 1) \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right) = (1 | 1 \ 0)$$

$$(CH \ CI) = (-1 \cdot 1 | -1 \cdot (0 \ 1)) = (-1 | 0 \ -1)$$

So,

$$(AD \ AE) + (BF \ BG) + (CH \ CI) = (1 \ 2 \ 0)$$

$$\left(\begin{array}{cc} JD & JE \end{array} \right) = \left(\begin{array}{c|cc} 1 \cdot 1 & 1 \cdot (1 & 1) \end{array} \right) = \left(\begin{array}{c|cc} 1 & 1 & 1 \end{array} \right)$$

$$\left(\begin{array}{cc} KF & KG \end{array} \right) = \left(\begin{array}{c|cc} (1 & 1) \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} & (1 & 1) \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array} \right) = \left(\begin{array}{c|cc} 2 & 1 & 1 \end{array} \right)$$

$$\left(\begin{array}{cc} LH & LI \end{array} \right) = \left(\begin{array}{c|cc} 0 \cdot 1 & 0 \cdot (0 & 1) \end{array} \right) = \left(\begin{array}{c|cc} 0 & 0 & 0 \end{array} \right)$$

So,

$$\left(\begin{array}{cc} JD & JE \end{array} \right) + \left(\begin{array}{c|cc} KF & KG \end{array} \right) + \left(\begin{array}{c|cc} LH & LI \end{array} \right) = \left(\begin{array}{c} 3 & 2 & 2 \end{array} \right)$$

$$\left(\begin{array}{cc} MD & ME \end{array} \right) = \left(\begin{array}{c|cc} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot 1 & \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot (1 & 1) \end{array} \right) = \left(\begin{array}{c|cc} 0 & 0 & 0 \\ 1 & 1 & 1 \end{array} \right)$$

$$\left(\begin{array}{cc} NF & NG \end{array} \right) = \left(\begin{array}{c|cc} \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array} \right) = \left(\begin{array}{c|cc} 1 & 0 & 1 \\ 0 & -1 & 1 \end{array} \right)$$

$$\left(\begin{array}{cc} PH & PI \end{array} \right) = \left(\begin{array}{c|cc} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot 1 & \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot (0 & 1) \end{array} \right) = \left(\begin{array}{c|cc} 1 & 0 & 1 \\ 0 & 0 & 0 \end{array} \right)$$

So,

$$\left(\begin{array}{cc} MD & ME \end{array} \right) + \left(\begin{array}{cc} NF & NG \end{array} \right) + \left(\begin{array}{cc} PH & PI \end{array} \right) = \left(\begin{array}{c} 2 & 0 & 2 \\ 1 & 0 & 2 \end{array} \right)$$

Stacking the results on top of each other, we again arrive at:

$$\left(\begin{array}{ccc} 1 & 2 & 0 \\ 3 & 2 & 2 \\ \hline 2 & 0 & 2 \\ 1 & 0 & 2 \end{array} \right)$$

2.4.3 Block Diagonal Matrices

Matrix block multiplication makes the multiplication of what are called “block diagonal matrices” very simple.

Block Diagonal Matrix

A block diagonal matrix is one made up of square blocks down the diagonal starting in the upper left and going to the lower right. All other blocks in the matrix are filled with zeros. We could have:

$$\begin{pmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & C \end{pmatrix}$$

where the blocks A , B , and C are square matrices each of any size and the zeros simply *stand for blocks* of many 0's.

Example 5. The following is an example of a block diagonal matrix:

$$\left(\begin{array}{ccccccc} 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 5 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 7 \end{array} \right)$$

If we would like to multiply two block diagonal matrices together according to the partition the blocks give, *the corresponding blocks on the diagonal need to be the same size*. This is to ensure a matching column-row partition.

Theorem 2.4.1

To multiply two block diagonal matrices where corresponding blocks have the same size, simply multiply corresponding blocks.

Proof. We give an illustration which could be turned into a rigorous argument. Suppose that we are multiplying

the following two block diagonal matrices:

$$\begin{pmatrix} A & 0 & 0 & \cdots \\ 0 & B & 0 & \cdots \\ 0 & 0 & C & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \cdot \begin{pmatrix} D & 0 & 0 & \cdots \\ 0 & E & 0 & \cdots \\ 0 & 0 & F & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

If we use a column interpretation, the first column of the product will be:

$$\begin{pmatrix} A & 0 & 0 & \cdots \\ 0 & B & 0 & \cdots \\ 0 & 0 & C & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \cdot \begin{pmatrix} D \\ 0 \\ 0 \\ \vdots \end{pmatrix} = \begin{pmatrix} A \\ 0 \\ 0 \\ \vdots \end{pmatrix} \cdot D = \begin{pmatrix} AD \\ 0 \\ 0 \\ \vdots \end{pmatrix}$$

What is on the right, stays on the right in the multiplication. *This is especially true when we are dealing with blocks instead of just scalar entries.* A similar computation will show that the second column of the product is

$$\begin{pmatrix} 0 \\ BE \\ 0 \\ \vdots \end{pmatrix}$$

Continuing on, we see that we are simply multiplying the diagonal blocks across. □

Example 6. Let's multiply the following two block diagonal matrices together:

$$\left(\begin{array}{ccccc} 2 & 1 & 0 & 0 & \text{multiply } 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{array} \right) \cdot \left(\begin{array}{ccccc} 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{array} \right)$$

multiply multiply multiply

$$= \begin{pmatrix} 3 & -2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 10 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix}$$

2.4.4 The Standard Definition of Matrix Multiplication

Standard Definition of Matrix Multiplication

The way that matrix multiplication is commonly defined is simply by using a row-column partition *only* (which can be non-matching). Suppose that we are multiplying matrices A and B together as $A \cdot B$.

- Every row of A is a block.
- Every column of B is a block.

With this definition it suffices to know how to multiply a single row matrix to a single column matrix and how to arrange all of these products. We will use our current knowledge of row and column interpretations to complete these tasks.

Example 7. Let's use the standard definition to perform the following multiplication:

$$\begin{pmatrix} 1 & 0 & 1 \\ 2 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}$$

We simply take rows of the first matrix as blocks and the columns of the second matrix as blocks:

$$\left(\begin{array}{ccc} 1 & 0 & 1 \\ 2 & -1 & 0 \\ \hline 0 & 1 & 0 \end{array} \right) \cdot \left(\begin{array}{c|c} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{array} \right)$$

We could label these blocks to have:

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \cdot \begin{pmatrix} d & e \end{pmatrix}$$

In either interpretation, we obtain:

$$\begin{pmatrix} ad & ae \\ bd & be \\ cd & ce \end{pmatrix}$$

and remember that the d and e happen on the right of each multiplication. Note that all of these products of blocks are 1×1 matrices since

$$(\text{row}) \cdot \begin{pmatrix} \text{column} \end{pmatrix} = (1 \times 1 \text{ matrix}).$$

Hence, our resulting final matrix *will be a 3×2 matrix!* Let's just look at one of the multiplications via a row interpretation:

$$ad = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{matrix} 1 \cdot (1) \\ + \\ 0 \cdot (1) \\ + \\ 1 \cdot (0) \end{matrix} = 1$$

Working through all of these we obtain:

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

This standard definition is not usually as efficient or convenient as using a row or a column interpretation.

Key Concepts from this Section

- **matching column-row partition:** (page 175) Suppose that we are multiplying two matrices A and B . Suppose that the columns of A are given by a_1, a_2, \dots, a_n and that the rows of B are given by b_1, b_2, \dots, b_n . Then, a matching column-row partition is a partition of these rows and columns which

takes the same shape. For instance, if $n = 4$, then the partitions

$$A = \left(\begin{array}{c|cc|c} a_1 & a_2 & a_3 & a_4 \end{array} \right)$$

and

$$B = \left(\begin{array}{c} \frac{b_1}{b_2} \\ \frac{b_2}{b_3} \\ \frac{b_3}{b_4} \end{array} \right)$$

together make up a matching column-row partition with shape $(* | * \ * | *)$.

- **column-row partition multiplication:** (page 176) Suppose that we are multiplying two matrices A and B with a matching column-row partition. Call the chunks of the column partition of A as A_1, A_2, \dots, A_k and chunks of the row partition of B as B_1, B_2, \dots, B_k . Then:

$$A \cdot B = A_1 \cdot B_1 + A_2 \cdot B_2 + \dots + A_k \cdot B_k.$$

- **row-column partition (non-matching):** (page 178) Suppose that we are multiplying two matrices A and B as $A \cdot B$. Suppose that the rows of A are given by a_1, a_2, \dots, a_m and that the rows of B are given by b_1, b_2, \dots, b_k . Then, a row-column partition *any* partition of the rows of A and *any* partition of the columns of B . For instance, if $m = 4$ and $k = 5$, then the partitions

$$A = \left(\begin{array}{c} a_1 \\ a_2 \\ a_3 \\ a_4 \end{array} \right)$$

and

$$B = \left(\begin{array}{c|cc|cc} b_1 & b_2 & b_3 & b_4 & b_5 \end{array} \right)$$

together make up a *non-matching* row-column partition.

- **matrix partitioning principle for multiplication:** (page 179) As long as we keep the matching column-row partition, we can use *any not necessarily matching* “row-column” partition.
 - The matching column-row partition reorganizes *the addition* that gives us the result.
 - The row-column partition organizes *where we see* specific results.
- **matrix block multiplication:** (page 179) Suppose that we have divided our matrices into blocks which follow a matching column-row partition and any kind of row-column partition.

We can just matrix multiply pretending that the blocks themselves are matrix entries.

Yet we must be careful on the order of multiplying matrix chunks! If a matrix chunk comes from the original left matrix, then it always goes on the left whenever we are multiplying with it among the blocks. If a matrix chunk comes from the original right matrix, then it always goes on the right whenever we are multiplying with it among the blocks.

- **block diagonal matrix:** (page 182) A block diagonal matrix is one made up of square blocks down the diagonal starting in the upper left and going to the lower right. All other blocks in the matrix are filled with zeros. We could have:

$$\begin{pmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & C \end{pmatrix}$$

where the blocks A , B , and C are square matrices each of any size and the zeros simply *stand for blocks* of many 0's.

- **theorem 2.4.1 :** (page 183) To multiply two block diagonal matrices where corresponding blocks have the same size, simply multiply corresponding blocks.
- **standard definition of matrix multiplication:** (page 185) The way that matrix multiplication is commonly defined is simply by using a row-column partition *only* (which can be non-matching). Suppose that we are multiplying matrices A and B together as $A \cdot B$.
 - Every row of A is a block.
 - Every column of B is a block.

2.4.5 Exercises

Block Matrix Multiplication

Compute the matrix products. If one matrix has a partition given, create a compatible partition in the other matrix. Then, use the partitions in both matrices to perform the matrix multiplication.

$$1. \begin{pmatrix} -1 \\ 2 \end{pmatrix} \cdot \left(\begin{array}{c|cc|c} 1 & -2 & 2 & 0 \end{array} \right)$$

$$2. \begin{pmatrix} 1 & -1 & 2 & 0 \end{pmatrix} \cdot \left(\begin{array}{cccc} -2 & -1 & 0 & 1 \\ -1 & -1 & 0 & 2 \\ \hline 2 & 1 & -2 & 0 \\ \hline 2 & 0 & 2 & -2 \end{array} \right)$$

$$3. \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \cdot \left(\begin{array}{cc|c} -1 & -1 & 1 \\ 1 & 2 & -1 \\ \hline 0 & 2 & 0 \end{array} \right)$$

$$4. \begin{pmatrix} 0 \\ 2 \end{pmatrix} \cdot \left(\begin{array}{c|c} 1 & -1 \\ \hline -2 & 1 \\ \hline -1 & 0 \end{array} \right) \cdot \begin{pmatrix} 2 & -2 & 1 \\ -2 & 1 & -2 \\ -1 & -1 & 0 \end{pmatrix}$$

$$5. \begin{pmatrix} 0 & -1 & -2 & -2 \\ 0 & 1 & 2 & -2 \end{pmatrix} \cdot \left(\begin{array}{c|c|c} 1 & 2 & -1 \\ \hline -2 & -2 & 2 \\ \hline -2 & 2 & -2 \\ \hline 2 & -2 & -1 \end{array} \right)$$

$$6. \begin{pmatrix} -1 \\ -2 \end{pmatrix} \cdot \begin{pmatrix} -1 \\ -2 \end{pmatrix}$$

$$7. \begin{pmatrix} -1 \\ -1 \end{pmatrix} \cdot \left(\begin{array}{c|cc} 2 & 0 & -2 \\ \hline 0 & -2 & 0 \end{array} \right)$$

$$8. \begin{pmatrix} -1 & -2 \\ -2 & 1 \end{pmatrix} \cdot \left(\begin{array}{c|cc|c} 2 & 2 & 2 & 1 \\ \hline -1 & 1 & 0 & -2 \end{array} \right)$$

$$9. \begin{pmatrix} -2 \end{pmatrix} \cdot \begin{pmatrix} -2 \end{pmatrix}$$

$$10. \begin{pmatrix} 2 \\ -1 \\ -2 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} -2 & 2 & -2 \\ 0 & 0 & 2 \end{pmatrix}$$

$$11. \left(\begin{array}{cc|c} -2 & 1 & 1 \\ 0 & -1 & -2 \\ \hline 0 & -1 & -1 \end{array} \right) \cdot \begin{pmatrix} 1 & 1 & -2 \\ 2 & -1 & -2 \\ -1 & -1 & 0 \end{pmatrix}$$

$$12. \begin{pmatrix} 2 & -2 & -2 \end{pmatrix} \cdot \left(\begin{array}{c|cc} 2 & 2 & -1 \\ \hline -1 & -1 & -1 \\ \hline -2 & -1 & -2 \end{array} \right)$$

$$13. \begin{pmatrix} -2 & 1 & 2 \\ 0 & 1 & 2 \\ -2 & 1 & 1 \end{pmatrix} \cdot \left(\begin{array}{c|cc|c} -1 & 2 & 1 \\ \hline -2 & 2 & -1 \\ 0 & 2 & -1 \end{array} \right)$$

$$14. \begin{pmatrix} -1 & 1 & 1 \\ 2 & 1 & 0 \\ 1 & 2 & -2 \end{pmatrix} \cdot \left(\begin{array}{c|cc} -2 & 2 \\ \hline 2 & 2 \\ 1 & 1 \end{array} \right)$$

$$15. \begin{pmatrix} -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ -2 \end{pmatrix}$$

$$16. \begin{pmatrix} 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & -2 \\ -1 & 0 \end{pmatrix}$$

$$17. \begin{pmatrix} 2 & -2 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

$$18. \left(\begin{array}{c|cc} -1 & 2 \\ \hline -2 & 1 \\ 0 & 1 \\ \hline 1 & -2 \end{array} \right) \cdot \begin{pmatrix} -1 \\ -2 \end{pmatrix}$$

$$19. \begin{pmatrix} -1 & 1 \\ -1 & 2 \\ 0 & -1 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}$$

$$20. \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \cdot \left(\begin{array}{c|cc} 1 & 0 & 1 & 2 \\ \hline 0 & -1 & -2 & -2 \end{array} \right)$$

Multiplication with Block Diagonal Matrices

Determine how you should think of the following as products of block diagonal matrices. Then, multiply the matrices together using the block diagonal technique.

$$21. \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 2 & -1 \end{pmatrix}$$

$$22. \begin{pmatrix} 1 & -2 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 \end{pmatrix}$$

23.
$$\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

24.
$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

25.
$$\begin{pmatrix} -2 & -2 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & -2 \\ 0 & 0 & 0 & 0 & -2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

26.
$$\begin{pmatrix} 2 & 1 & 0 & 0 \\ -2 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

27.
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & -2 & 2 \end{pmatrix}$$

28.
$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & -2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

29.
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

30.
$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

2.4.6 Solutions

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

2. $\begin{pmatrix} 3 & 2 & -4 & -1 \end{pmatrix}$

3. $\begin{pmatrix} -1 & -1 & 1 \end{pmatrix}$

4. $\begin{pmatrix} -1 & 2 & -2 \\ 7 & -7 & 6 \end{pmatrix}$

5. $\begin{pmatrix} 2 & 2 & 4 \\ -10 & 6 & 0 \end{pmatrix}$

6. $\begin{pmatrix} 3 \\ 0 \end{pmatrix}$

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

8. $\begin{pmatrix} 0 & -4 & -2 & 3 \\ -5 & -3 & -4 & -4 \end{pmatrix}$

9. $\begin{pmatrix} 4 \end{pmatrix}$

10. $\begin{pmatrix} -4 & 4 & -2 \\ 2 & -2 & 0 \\ 4 & -4 & 0 \\ -2 & 2 & -4 \end{pmatrix}$

11. $\begin{pmatrix} -1 & -4 & 2 \\ 0 & 3 & 2 \\ -1 & 2 & 2 \end{pmatrix}$

12. $\begin{pmatrix} 10 & 8 & 4 \end{pmatrix}$

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

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

15. $\begin{pmatrix} -4 \end{pmatrix}$

16. $\begin{pmatrix} -3 & -4 \end{pmatrix}$

17. $\begin{pmatrix} -4 \\ 2 \end{pmatrix}$

18. $\begin{pmatrix} -3 \\ 0 \\ -2 \\ 3 \end{pmatrix}$

19.
$$\begin{pmatrix} -1 & 2 \\ 0 & 4 \\ -1 & -2 \\ -3 & 2 \end{pmatrix}$$

20.
$$\begin{pmatrix} 1 & 1 & 3 & 4 \\ 2 & 1 & 4 & 6 \end{pmatrix}$$

21.
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & -4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

22.
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 6 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 \end{pmatrix}$$

23.
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

24.
$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

25.
$$\begin{pmatrix} 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

26.
$$\begin{pmatrix} 1 & -2 & 0 & 0 \\ -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

27.
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -3 & 2 \\ 0 & 0 & 0 & 2 & -2 \end{pmatrix}$$

28.
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$29. \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$30. \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Chapter 2 Selected Review Questions

Section 2.1

Do you understand what dimension means in relation to minimal spanning sets? Do you know what a linear combination and a span are?

1. Prove that the dimension of the span of the following vectors which live in \mathbb{R}^4 is less than 3.

$$(1, 2, 3, 4), (1, 1, 1, 1), (2, 3, 4, 5), (5, 7, 9, 11)$$

Do you should understand what makes a vector space a vector space? In particular, can you verify that a subspace of a vector space satisfies all of the properties of a vector space? Can you show that something is a subspace?

2. Consider the vector space \mathbb{R}^3 . The span $W = \langle (1, 1, 1) \rangle$ is a subspace of the span $V = \langle (2, 3, 1), (-1, -2, 0) \rangle$. Complete the following:

- Show that W is a *subset* of V .
- What conditions are necessary to ensure that a subset of a vector space is a subspace?
- Give examples of these conditions being satisfied in this example.

Can you identify the elements in a quotient vector space and add them together?

3. The points on the line $4x + y = 0$ defines a vector subspace of \mathbb{R}^2 . Call this subspace H .

- Express the line $4x + y = 5$ as a shift of H . That is, this line is $(a, b) + H$ for some (a, b) . Find (a, b) .
- Express the line $4x + y = 7$ as a shift of H . That is, this line is $(c, d) + H$ for some (c, d) . Find (c, d) .
- The two shifts $(a, b) + H$ and $(c, d) + H$ are examples of vectors in the quotient vector space \mathbb{R}^2/H . What is the sum of these two vectors in the quotient?

4. The equation $x + y + z = 0$ is the equation of a plane through the origin in xyz coordinates. Let's call this plane H and let $V = \mathbb{R}^3$. Then, denote the plane $x + y + z = 1$ by a and the plane $x + y + z = 2$ by b . The planes a and b are parallel to the plane H . Therefore, $a, b \in V/H$.

- (a) $a = t + H$. Find a vector t that makes this work. *Hint: the vectors in the plane are solutions to the equation. Any vector t in the plane works!*
- (b) $b = w + H$. Find a vector w that makes this work.
- (c) Perform the computation $a +_{V/H} b$. Describe the resulting plane as (a vector) + H : a shift of the plane H by a vector. *Hint: use the t and w you have already found. Do you know how to add $(t + H) +_{V/H} (w + H)$?*

Section 2.2

Can you find a nonzero linear combination which verifies a collection of vectors is linearly independent?

5. Prove that the following collection of vectors in \mathbb{R}^3 is linearly dependent:

$$(1, 4, 2), (1, 0, 1), (-6, -8, -8)$$

Can you use the “zero fiber for injectivity” idea to see if a collection of vectors is linearly independent or dependent?

6. Linearly independent or dependent?
 $(1, -1, 1), (-4, -3, 4), (-9, 6, 6)$

7. Linearly independent or dependent?
 $(-5, -3, 2), (2, 2, -5), (22, 14, -13)$

Section 2.3

Do you understand and can you use row and column interpretation to multiply two matrices together?

- 8.** Column Interpretation of Matrix Multiplication and what is the domain and codomain of the result?

$$\begin{pmatrix} 0 & -2 & -2 & 0 \\ -2 & 0 & 0 & 0 \\ -2 & 0 & 2 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 \\ 1 & -2 \\ 1 & 2 \\ 2 & 0 \end{pmatrix}$$

- 9.** Row Interpretation of Matrix Multiplication and what is the domain and codomain of the result?

$$\begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \\ 2 & 0 & -1 \\ -2 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}$$

Section 2.4

Can you correctly create and use blocks to multiply two matrices together?

- 10.** Block Matrix Multiplication. Find a partition of the other matrix that is compatible and use it multiply the matrices:

$$\begin{pmatrix} -2 & 1 & 2 \\ 0 & 1 & 2 \\ -2 & 1 & 1 \end{pmatrix} \cdot \left(\begin{array}{c|cc} -1 & 2 & 1 \\ \hline -2 & 2 & -1 \\ 0 & 2 & -1 \end{array} \right)$$

Solutions/Hints

1. Notice that $(1, 2, 3, 4) + (1, 1, 1, 1) = (2, 3, 4, 5)$ and that $(1, 2, 3, 4) + 2 \cdot (1, 1, 1, 1) = (5, 7, 9, 11)$. This means that only two vectors can be used to span. Hence, the dimension is less than 3.

2. Solutions by part:

(a) This comes from $(1, 1, 1) = (2, 3, 1) + (-1, -2, 0) \in V$.

(b) We need W to be closed with respect to vector addition and scalar multiplication.

(c) A possible example of W being closed with respect to addition:

$$\underbrace{2 \cdot (1, 1, 1)}_{\in W} + \underbrace{3 \cdot (1, 1, 1)}_{\in W} = 5 \cdot (1, 1, 1) \in W$$

A possible example of W being closed with respect to scalar multiplication:

$$2 \cdot \underbrace{(3, 3, 3)}_{\in W} = (6, 6, 6) = 6 \cdot (1, 1, 1) \in W$$

3. Solutions by part:

(a) One possible way to express this shift is as $(1, 1) + H$. You can choose any (a, b) on the line $4x + y = 5$ and it will work.

(b) One possible way to express this shift is as $(1, 3) + H$. You can choose any (c, d) on the line $4x + y = 7$ and it will work.

(c) We add vectors in the quotient as follows:

$$\left((1, 1) + H \right) + \left((1, 3) + H \right) = \left((2, 4) + H \right)$$

We just add the shift representatives together.

4. Solution by parts:

(a) One simple choice for t is $(0, 0, 1)$ since this satisfies $x + y + z = 1$. There are many others that work.

(b) One simple choice for w is $(0, 0, 2)$ since this satisfies $x + y + z = 2$. There are many others that work.

- (c) We know that $(t + H) +_{V/H} (w + H) = (t + w) + H$. Therefore, using our choices for t and w in this solution, we have that the sum of planes in this quotient is. $(0, 0, 3) + H$ In other words, it is a shift of the plane H by the vector $(0, 0, 3)$.

- 5.** All we need to do is to show that the collection does not satisfy the criterion in the definition of being linearly independent. Either by inspection or by trying to solve a system of equations to find a dependency, we find that $-2 \cdot (1, 4, 2) - 4 \cdot (1, 0, 1) = (-6, -8, -8)$. This means that

$$-2 \cdot (1, 4, 2) - 4 \cdot (1, 0, 1) - 1 \cdot (-6, -8, -8) = 0$$

so that a nonzero linear combination of these vectors is zero. This means that the vectors cannot be linearly independent. Therefore, they are linearly dependent.

- 6.** We set

$$a \cdot (1, -1, 1) + b \cdot (-4, -3, 4) + c \cdot (-9, 6, 6) = (0, 0, 0)$$

which turns into

$$(a - b4 - 9c, -a - 3b + 6c, a + 4b + 6c) = (0, 0, 0)$$

or rather

$$\begin{aligned} a - b4 - 9c &= 0 \\ -a - 3b + 6c &= 0 \\ a + 4b + 6c &= 0 \end{aligned}$$

Solving this system, the only solution is $(0, 0, 0)$ so that the collection of vectors is linearly independent.

- 7.** Follow the same procedure as in the solution of the last exercise. Since there is more than one solution, the vectors are linearly dependent.

$$\textbf{8. } \begin{pmatrix} -4 & 0 \\ -4 & 2 \\ -6 & 6 \end{pmatrix} \quad f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$$

$$\textbf{9. } \begin{pmatrix} 2 & 1 \\ 3 & 2 \\ 4 & 2 \\ -4 & -2 \end{pmatrix} \quad f : \mathbb{R}^4 \rightarrow \mathbb{R}^2$$

- 10.** Since the row partition of the second matrix is: $\left(\begin{array}{c|c} * & * \\ * & * \\ \hline * & * \end{array} \right)$, we should use a column partition $\left(\begin{array}{c|c|c} * & * & * \end{array} \right)$ for the first matrix. You can row partition the first matrix any way you would like. One possibility is to have blocks:

$$(a \ b) \cdot \begin{pmatrix} c & d & e \\ f & g & h \end{pmatrix} = (ac \ ad \ ae) + (bf \ bg \ bh)$$

The result is:

$$\begin{pmatrix} 0 & 2 & -5 \\ -2 & 6 & -3 \\ 0 & 0 & -4 \end{pmatrix}$$

Linear Trans-

formation

3

Examples

Rotating and Stretching the Plane

3.1

3.1.1 Building Matrices for Plane Transformations	204
3.1.2 The Equation of a Transformed Graph	206
3.1.3 Exercises	209
3.1.4 Solutions	213

Questions to Guide Your Study:

- *How do you write a matrix that describes a basic transformation in the plane?*
- *How can you use matrices to write the equation of a rotated graph?*

3.1.1 Building Matrices for Plane Transformations

Think about what the domain of a matrix function could be. It could be the line \mathbb{R} , or the plane \mathbb{R}^2 , or 3-dimensional space \mathbb{R}^3 , or any higher dimensional analog. The range can be a subspace of any of these as well. The effect of a matrix function is to *transform* its domain into its range. That is, it could take all of 3-space and squash it to a plane. Or it could squash 3-space or 2-space to a line. It also could take a line and insert it into a larger space. It could take \mathbb{R}^2 and picture it as a plane passing through the origin in \mathbb{R}^3 .

Indeed, matrix functions do cause transformations. *But these transformations are nice!* Remember that they are *additive* and *scalable*. Being additive means that the tip-to-tail addition of vectors is preserved. This is equivalent to saying that *parallelograms are preserved*.

See the SageMath activity at



in order to explore some 3-dimensional models of linear transformations.

Some Basic Examples of Linear Transformations

- Rotating about an axis.
- Rescaling certain coordinates.
- Perpendicular (usually termed *orthogonal* in higher than 2 dimensions) projection onto a subspace of \mathbb{R}^n .

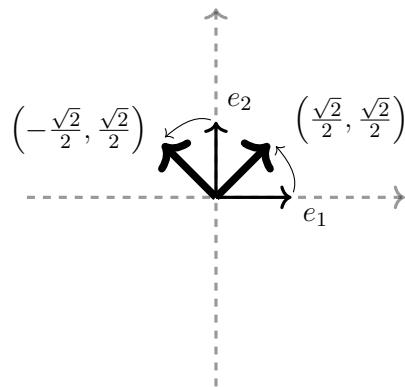
In order to build a matrix which describes one or more of these types of transformations in sequence, we simply use the idea that just knowing where standard basis vectors go, we know where everything goes.

Matrix Formation Principle

Just knowing the destination of standard basis vectors is enough to build a matrix that describes a linear transformation. If we list the destinations as rows, the linear transformation acts via a row interpretation matrix multiplication. If we list the destinations as columns, the linear transformation acts via a column interpretation matrix multiplication.



Example 1. *Example of using a linear transformation to describe rotation.* Suppose that we spin the plane \mathbb{R}^2 about the origin counterclockwise by 45° . This is a linear transformation and can be described by a matrix function. Just consider where $e_1 = (1, 0)$ and $e_2 = (0, 1)$ go in order to write down the matrix:



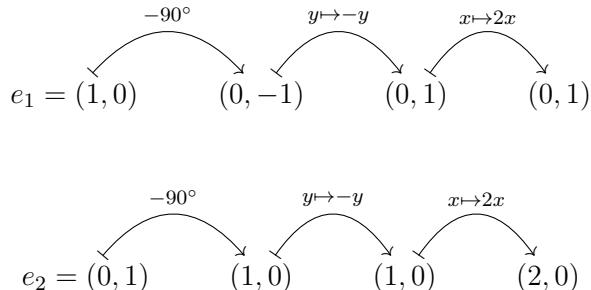
Therefore, with a column interpretation, the matrix is:

$$\begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} = \frac{\sqrt{2}}{2} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

Example 2. *Example of a rotation, stretch, and reflection* Suppose that we would like to write down a matrix function f with a row interpretation for the result of two consecutive transformations:

1. rotate clockwise by 90°
2. reflect over the x -axis
3. stretch x coordinates by a factor of 2

We think:



Hence, we have the matrix:

$$\begin{matrix} f(e_1) & \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \\ f(e_2) & \end{matrix}$$

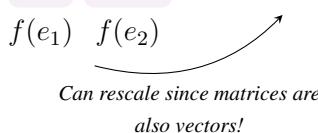
3.1.2 The Equation of a Transformed Graph

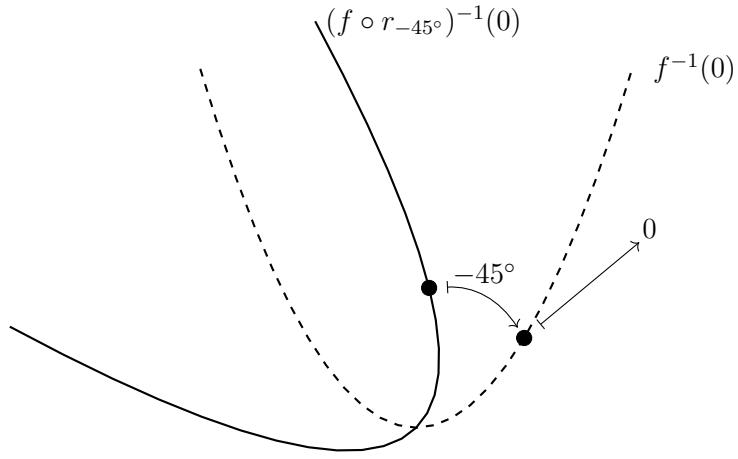
We have discussed how to write the matrix for a transformation. Now, how do we change the equation that describes a graph to which that we apply a transformation? We illustrate how via an example.



Example 3. *Example of rotating a graph with a linear transformation.*

Let's start with the graph of $y = x^2$ and try to come up with an equation that represents this curve rotated by 45° *counterclockwise*. First, we look at the graph of $y = x^2$ all coordinate points (x, y) such that $y - x^2 = 0$. That is, if $f(x, y) = y - x^2$. We are considering the fiber $f^{-1}(0)$. Let $r_\theta(x, y)$ represent the function $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ that rotates points in the plane by an angle of θ . Then the following picture tells us that the graph we are interested in is the set of points $(f \circ r_{-45^\circ})^{-1}(0) \subset \mathbb{R}^2$:





These points are the solutions to the equation:

$$(f \circ r_{-45^\circ})(x, y) = 0$$

Using a **row interpretation**, we can write $r_{-45^\circ} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ as:

$$\begin{aligned} r_{-45^\circ}(e_1) &= \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{pmatrix} \\ r_{-45^\circ}(e_2) &= \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \end{aligned}$$

Therefore,

$$r_{-45^\circ}(x, y) = \begin{pmatrix} x & y \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \cdot \frac{\sqrt{2}}{2} = (x + y, -x + y) \cdot \frac{\sqrt{2}}{2}$$

Then, using $f(x, y) = y - x^2$, the equation for the rotated parabola is

$$f\left(\frac{\sqrt{2}}{2} \cdot (x + y), \frac{\sqrt{2}}{2} \cdot (-x + y)\right) = 0$$

Using $\frac{\sqrt{2}}{2} = \frac{1}{\sqrt{2}}$:

$$\underbrace{\frac{1}{\sqrt{2}}(-x + y)}_{\text{replace } y} - \underbrace{\frac{1}{2}(x + y)^2}_{\text{replace } x^2} = 0$$

Multiplying the equation by 2 and then expanding:

$$-\sqrt{2}x + \sqrt{2}y - x^2 - 2xy - y^2 = 0$$

or simply:

$$x^2 + \sqrt{2}x - \sqrt{2}y + 2xy + y^2 = 0$$

The Equation of a Transformed Graph

Suppose that we wish to perform a particular transformation (i.e. function) $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ to a graph which is given as a fiber $f^{-1}(c)$ of a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ for some $c \in \mathbb{R}$. Further suppose that the function T has an inverse function T^{-1} . Then, the new resulting graph is the fiber $(f \circ T^{-1})^{-1}(c)$. That is, the original equation is $f(x, y) = c$ and the equation that represents the transformed graph is $f \circ T^{-1}(x, y) = c$.

Key Concepts from this Section

- **some basic examples of linear transformations:** (page 204)
 - Rotating about an axis.
 - Rescaling certain coordinates.
 - Perpendicular (usually termed *orthogonal* in higher than 2 dimensions) projection onto a subspace of \mathbb{R}^n .
- **matrix formation principle:** (page 205) Just knowing the destination of standard basis vectors is enough to build a matrix that describes a linear transformation. If we list the destinations as rows, the linear transformation acts via a row interpretation matrix multiplication. If we list the destinations as columns, the linear transformation acts via a column interpretation matrix multiplication.
- **the equation of a transformed graph:** (page 208) Suppose that we wish to perform a particular transformation (i.e. function) $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ to a graph which is given as a fiber $f^{-1}(c)$ of a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ for some $c \in \mathbb{R}$. Further suppose that the function T has an inverse function T^{-1} . Then, the new resulting graph is the fiber $(f \circ T^{-1})^{-1}(c)$.

That is, the original equation is $f(x, y) = c$ and the equation that represents the transformed graph is $f \circ T^{-1}(x, y) = c$.

3.1.3 Exercises

Finding the Matrix of a Linear Transformation

Find the matrix (according to the indicated interpretation) for the one function $\mathbb{R}^2 \rightarrow \mathbb{R}$ that performs all of transformations listed in the order indicated on \mathbb{R}^2 .

1. Column interpretation:

- Reflect across x axis.

2. Column interpretation:

- Reflect across x axis.
- Rotate by 135° .

3. Column interpretation:

- Reflect across x axis.
- Rotate by -60° .
- y values : Stretch by a factor of 2.

4. Column interpretation:

- Rotate by -45° .

5. Column interpretation:

- Reflect across x axis.
- Rotate by -60° .

6. Row interpretation:

- Rotate by 135° .

7. Row interpretation:

- Reflect across x axis.
- y values : Compress by a factor of 2.

8. Column interpretation:

- Rotate by 120° .
- Reflect across y axis.

9. Row interpretation:

- Rotate by 45° .
- Reflect across y axis.
- x values : Stretch by a factor of 3.

10. Column interpretation:

- x values : Compress by a factor of 3.
- Rotate by 120° .

11. Column interpretation:

- Reflect across y axis.

12. Column interpretation:

- Reflect across x axis.
- Rotate by -60° .

13. Row interpretation:

- x and y values: Compress by a factor of 2.

14. Column interpretation:

- Reflect across y axis.
- y values : Compress by a factor of 2.

15. Column interpretation:

- Rotate by 120° .

16. Row interpretation:

- Reflect across x axis.
- y values : Stretch by a factor of 2.
- Rotate by -30° .

17. Column interpretation:

- Rotate by 30° .

18. Column interpretation:

- Reflect across y axis.
- Rotate by 150° .

19. Column interpretation:

- Reflect across y axis.
- Rotate by 150° .

20. Column interpretation:

- Reflect across x axis.
- Rotate by -45° .

Equations of Rotated Graphs

If we rotate the graph of the given equation by the angle indicated, then find the equation for that new rotated graph:

21. Rotate by 60° :

$$9x^2 - 4y^2 - 36 = 0$$

22. Rotate by 90° :

$$-x^2 + y = 0$$

23. Rotate by -60° :

$$9x^2 - 4y^2 - 36 = 0$$

24. Rotate by -60° :

$$x^2 + 4y^2 - 4 = 0$$

25. Rotate by -45° :

$$x^2 + 4y^2 - 4 = 0$$

26. Rotate by -60° :

$$9x^2 - 4y^2 - 36 = 0$$

27. Rotate by -60° :

$$-x^2 + y = 0$$

28. Rotate by -90° :

$$9x^2 - 4y^2 - 36 = 0$$

29. Rotate by -90° :

$$9x^2 - 4y^2 - 36 = 0$$

30. Rotate by -60° :

$$-x^2 + y = 0$$

31. Rotate by -90° :

$$x^2 + 4y^2 - 4 = 0$$

32. Rotate by 90° :

$$9x^2 - 4y^2 - 36 = 0$$

33. Rotate by -60° :

$$-x^2 + y = 0$$

34. Rotate by 90° :

$$-x^2 + y = 0$$

35. Rotate by -45° :

$$-x^2 + y = 0$$

36. Rotate by -30° :

$$-x^2 + y = 0$$

Proof Practice

37. Prove the two sum formulas from trigonometry:

- $\cos(a + b) = \cos(a)\cos(b) - \sin(a)\sin(b)$
- $\sin(a + b) = \sin(a)\cos(b) + \cos(a)\sin(b)$

by multiplying the matrix that represents rotation by an angle of a to the matrix that represents rotation by an angle of b . Should not the matrix product as a composition of two rotation functions simply be rotation by $a + b$? Remember that cos gives a x -coordinate on the unit circle and sin gives a y -coordinate.

3.1.4 Solutions

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

2. $\begin{pmatrix} -\frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \end{pmatrix}$

3. $\begin{pmatrix} \frac{1}{2} & -\frac{1}{2}\sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}$

4. $\begin{pmatrix} \frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \\ -\frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \end{pmatrix}$

5. $\begin{pmatrix} \frac{1}{2} & -\frac{1}{2}\sqrt{3} \\ -\frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$

6. $\begin{pmatrix} -\frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \\ -\frac{1}{2}\sqrt{2} & -\frac{1}{2}\sqrt{2} \end{pmatrix}$

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

8. $\begin{pmatrix} \frac{1}{2} & \frac{1}{2}\sqrt{3} \\ \frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$

9. $\begin{pmatrix} -\frac{3}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \\ \frac{3}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \end{pmatrix}$

10. $\begin{pmatrix} -\frac{1}{6} & -\frac{1}{2}\sqrt{3} \\ \frac{1}{6}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$

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

12. $\begin{pmatrix} \frac{1}{2} & -\frac{1}{2}\sqrt{3} \\ -\frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$

13. $\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$

14. $\begin{pmatrix} -1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$

15. $\begin{pmatrix} -\frac{1}{2} & -\frac{1}{2}\sqrt{3} \\ \frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$

16. $\begin{pmatrix} \frac{1}{2}\sqrt{3} & -\frac{1}{2} \\ -1 & -\sqrt{3} \end{pmatrix}$

17. $\begin{pmatrix} \frac{1}{2}\sqrt{3} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2}\sqrt{3} \end{pmatrix}$

18. $\begin{pmatrix} \frac{1}{2}\sqrt{3} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2}\sqrt{3} \end{pmatrix}$

19. $\begin{pmatrix} \frac{1}{2}\sqrt{3} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2}\sqrt{3} \end{pmatrix}$

20. $\begin{pmatrix} \frac{1}{2}\sqrt{2} & -\frac{1}{2}\sqrt{2} \\ -\frac{1}{2}\sqrt{2} & -\frac{1}{2}\sqrt{2} \end{pmatrix}$

21. $-\left(\sqrt{3}x - y\right)^2 + \frac{9}{4}\left(\sqrt{3}y + x\right)^2 - 36 = 0$

22. $-y^2 - x = 0$

23. $-\left(\sqrt{3}x + y\right)^2 + \frac{9}{4}\left(\sqrt{3}y - x\right)^2 - 36 = 0$

24. $\left(\sqrt{3}x + y\right)^2 + \frac{1}{4}\left(\sqrt{3}y - x\right)^2 - 4 = 0$

25. $\left(\sqrt{2}x + \sqrt{2}y\right)^2 + \frac{1}{4}\left(\sqrt{2}x - \sqrt{2}y\right)^2 - 4 = 0$

26. $-\left(\sqrt{3}x + y\right)^2 + \frac{9}{4}\left(\sqrt{3}y - x\right)^2 - 36 = 0$

27. $-\frac{1}{4}\left(\sqrt{3}y - x\right)^2 + \frac{1}{2}\sqrt{3}x + \frac{1}{2}y = 0$

28. $-4x^2 + 9y^2 - 36 = 0$

29. $-4x^2 + 9y^2 - 36 = 0$

30. $-\frac{1}{4}\left(\sqrt{3}y - x\right)^2 + \frac{1}{2}\sqrt{3}x + \frac{1}{2}y = 0$

31. $4x^2 + y^2 - 4 = 0$

32. $-4x^2 + 9y^2 - 36 = 0$

33. $-\frac{1}{4}\left(\sqrt{3}y - x\right)^2 + \frac{1}{2}\sqrt{3}x + \frac{1}{2}y = 0$

34. $-y^2 - x = 0$

35. $-\frac{1}{4}\left(\sqrt{2}x - \sqrt{2}y\right)^2 + \frac{1}{2}\sqrt{2}x + \frac{1}{2}\sqrt{2}y = 0$

36. $-\frac{1}{4}\left(\sqrt{3}x - y\right)^2 + \frac{1}{2}\sqrt{3}y + \frac{1}{2}x = 0$

37. In a column interpretation, thinking about the destinations of e_1 and e_2 , we can build the matrices for rotations by a and b and then multiply them:

$$\underbrace{\begin{pmatrix} \cos(b) & -\sin(b) \\ \sin(b) & \cos(b) \end{pmatrix}}_{\text{rotation by } b} \cdot \underbrace{\begin{pmatrix} \cos(a) & -\sin(a) \\ \sin(a) & \cos(a) \end{pmatrix}}_{\text{rotation by } a} = \underbrace{\begin{pmatrix} \cos(a)\cos(b) - \sin(a)\sin(b) & -\sin(a)\cos(b) - \cos(a)\sin(b) \\ \sin(a)\cos(b) + \cos(a)\sin(b) & \cos(a)\cos(b) - \sin(a)\sin(b) \end{pmatrix}}_{\text{rotation by } a+b}$$

This result should be rotation by $a + b$. Let's also build a matrix for rotation by $a + b$ another way—this time using the same technique that we built the matrices for rotation by a and rotation by b :

$$\underbrace{\begin{pmatrix} \cos(a+b) & -\sin(a+b) \\ \sin(a+b) & \cos(a+b) \end{pmatrix}}_{\text{rotation by } a+b}$$

We know that:

$$\underbrace{\begin{pmatrix} \cos(a+b) & -\sin(a+b) \\ \sin(a+b) & \cos(a+b) \end{pmatrix}}_{\text{rotation by } a+b} = \underbrace{\begin{pmatrix} \cos(a)\cos(b) - \sin(a)\sin(b) & -\sin(a)\cos(b) - \cos(a)\sin(b) \\ \sin(a)\cos(b) + \cos(a)\sin(b) & \cos(a)\cos(b) - \sin(a)\sin(b) \end{pmatrix}}_{\text{rotation by } a+b}$$

Upon equating matrix entries, we get the two sum formulas. So really, the sum formulas come from assuming that rotation is a linear map describable by a matrix.

Derivatives as Matrices

3.2

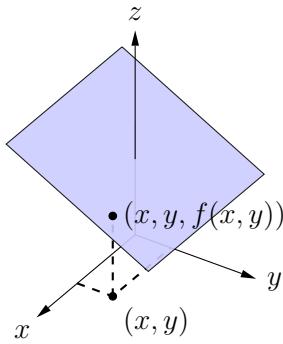
3.2.1 Graphing Shifts of Linear Transformations	216
3.2.2 Derivatives	218
3.2.3 Chain Rule	225
3.2.4 Machine Learning	226
3.2.5 Exercises	231
3.2.6 Solutions	238

Questions to Guide Your Study:

- Given an equation which describes a graph, how do you find a function for which the graph is one of its fibers and vice versa?
- What is the derivative of a function with multiple inputs and outputs? What does it mean?
- How do you find the derivative matrix for a function?
- What are partial derivatives and how and why do we use them?
- What is the chain rule?
- Why does it make sense that the chain rule works like matrix multiplication?

3.2.1 Graphing Shifts of Linear Transformations

Linear transformations are functions. Can we graph them? Perhaps not all of them have nice visualizations. But some do. A function $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ can be graphed with \mathbb{R}^2 (the xy -plane) as its domain and \mathbb{R} (the z -axis) as its codomain. Let's look at an example of a function f which is not a linear transformation—but is a shift of one. Suppose that $f(x, y) = \frac{1}{8}x - \frac{1}{8}y + 1$. Then, the graph of f can be depicted as:



What we see is a graphed relationship between codomain and domain. We will see that the graph of this function is actually a fiber of a linear transformation. Fibers of linear transformations *are always shifts of the fiber over the 0 vector*. The fiber over the 0 vector *is a vector space*: it is a span of vectors so it looks like a point, line, plane, or some n -dimensional space through the origin.

Notice that what we are looking at is a plane: *it is a shift of a plane through the origin—i.e. a shift of a vector space*. So, it really can be thought of as a fiber according to this description! Let's see if we can build a linear transformation h such that the graph of f is a fiber for it! We know that planes parallel to this one fill out all of \mathbb{R}^3 and fibers partition the domain. Hence, the domain must be \mathbb{R}^3 . Further, we know that elements of the range are indexed uniquely by fibers. We can stack the parallel planes along a one-dimensional line and get all of them. Hence, the range has dimension 1. We could build a surjective function so that the range is equal to the codomain. So perhaps $h : \mathbb{R}^3 \rightarrow \mathbb{R}$ would be a good choice. Now let's look at the actual formula for f and play with it:

$$\underbrace{f(x, y)}_z = \frac{1}{8}x - \frac{1}{8}y + 1$$

$$-1 = \frac{1}{8}x - \frac{1}{8}y - z$$

If $h(x, y, z) = \frac{1}{8}x - \frac{1}{8}y - z$, then the solutions to this equation would simply be described by the fiber $h^{-1}(-1)$.

Lines and Planes are Fibers

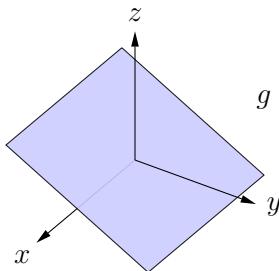
Lines and planes are fibers of linear transformations.

There is an essential difference between a *graph* of a function and a function itself. Let's go back to the function f . Aside from its graph being a fiber of a linear transformation, the function f is related to another linear transformation. Suppose that we take the $+1$ out of the formula for f to form a new function g . Then, we are left with $g(x, y) = \frac{1}{8}x - \frac{1}{8}y$ which represents a linear transformation $\mathbb{R}^2 \rightarrow \mathbb{R}$ given by the matrix $\begin{pmatrix} \frac{1}{8} & -\frac{1}{8} \end{pmatrix}$. The output z -values of f are just *shifts* by $+1$ of the outputs of the linear transformation g . That is, our plane is the graph of a *shift of a linear transformation function*.

Lines and Planes are Graphs of Shifts

Lines and planes can be thought of as graphs (i.e. fibers) of functions. Those functions themselves are shifts of linear transformations.

The graph of our linear transformation g as a fiber of h is actually a fiber over the 0-vector so is itself a vector space—*a plane through the origin*:



Example 1. Let's find a matrix under a column interpretation for which the graph of $f(x, y) = 2x + y - 7$ is a fiber. We think:

$$z = 2x + y - 7 \implies 7 = \underbrace{2x + y - z}_{h(x,y,z)}$$

So, if we define $h : \mathbb{R}^3 \rightarrow \mathbb{R}$ by $h(x, y, z) = 2x + y - z$, then the graph of f is $h^{-1}(7)$. The matrix representing h under a column interpretation is a 1×3 matrix: $\begin{pmatrix} 2 & 1 & -1 \end{pmatrix}$. Indeed, we can use the formula $h(x, y, z) = 2x + y - z$ to find the images of e_1 , e_2 , and e_3 to build our matrix if we desire: $h(e_1) = 2 \cdot 1 + 0 - 0 = 2$, $h(e_2) = 2 \cdot 0 + 1 - 0 = 1$, and $h(e_3) = 2 \cdot 0 + 0 - 1 = -1$. These also are just the coefficients of x , y , and z in our formula.

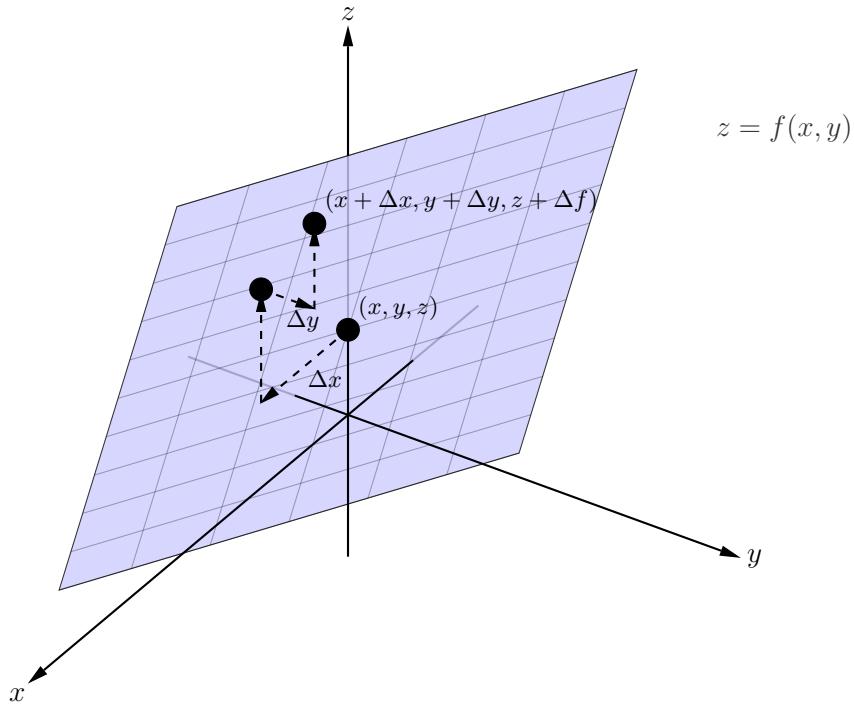
Example 2. Suppose that $h : \mathbb{R}^2 \rightarrow \mathbb{R}$ is given by the matrix $\begin{pmatrix} 1 & 4 \end{pmatrix}$ under a column interpretation then let's find the function f such that $h^{-1}(5)$ is the graph of f . We think:

$$\begin{pmatrix} 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = 5 \implies x + 4y = 5 \implies \underbrace{y}_{f(x)} = -\frac{1}{4}x + \frac{5}{4}.$$

Hence, we find that $f : \mathbb{R} \rightarrow \mathbb{R}$ with $f(x) = -\frac{1}{4}x + \frac{5}{4}$ is the desired function.

3.2.2 Derivatives





Derivative of a Function $\mathbb{R}^2 \rightarrow \mathbb{R}$

Consider the figure above. Assume that the graph of $z = f(x, y)$ looks approximately flat like a plane at the point (x, y, z) on its graph. Suppose further that we would like to measure the change of f (notated as Δf) as the input moves from (x, y) to $(x + \Delta x, y + \Delta y)$. Computationally, we have:

$$\Delta f = f(x + \Delta x, y + \Delta y) - f(x, y).$$

Notice that this is a vertical distance between two points on the graph. Then, the derivative (notated $Df(x, y)$) of f at (x, y) is a linear transformation $\mathbb{R}^2 \rightarrow \mathbb{R}$ that tells us precisely what Δf would be *if the function f were actually flat like a plane itself*. That is, $Df(x, y)$ is described as:

$$(\Delta x, \Delta y) \mapsto \Delta f$$

So, the derivative $Df(x, y)$ of a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ is a linear transformation and can be described as a matrix! Let's see how to make such a matrix with a column interpretation. ***In our calculations, we assume that the graph of f is a plane.***

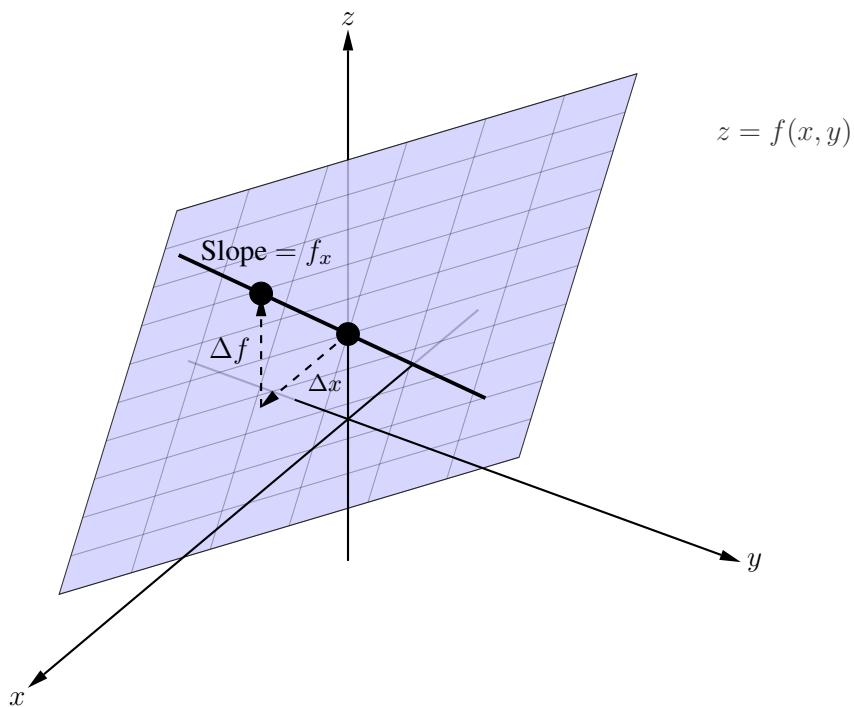
$$\left(\begin{array}{c} \Delta f \text{ with } (\Delta x, \Delta y) = e_1 \\ \Delta f \text{ with } (\Delta x, \Delta y) = e_2 \end{array} \right)$$

e_1 e_2
 || ||
 $\left(\underbrace{1}_{\Delta x}, \underbrace{0}_{\Delta y} \right)$ $\left(\underbrace{0}_{\Delta x}, \underbrace{1}_{\Delta y} \right)$

To help us know what the images of e_1 and e_2 are, we introduce some notation:

 f_x

Assume that the graph of $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ given by $(x, y) \mapsto z$ is *approximated* by a plane through a point (x, y, z) . All the points on the plane that have the same y value as this point form a line. We call the slope of this line f_x . This emphasizes that along this line, f is a function of x . The variable x is the only one changing.

 **f_y**

Assume that the graph of $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ given by $(x, y) \mapsto z$ is *approximated* by a plane through a point (x, y, z) . All the points on the plane that have the same x value as this point form a line. We call the slope of this line f_y . This emphasizes that along this line, f is a function of y . The variable y is the only one changing.

Then, for $(\Delta x, \Delta y) = (1, 0)$, we have that $\frac{\Delta f}{\Delta x} = f_x$ so that $\Delta f = f_x \cdot \underbrace{\Delta x}_{=1}$ so that $\Delta f = f_x$. Similarly, for $(\Delta x, \Delta y) = (0, 1)$, then $\Delta f = f_y$. Consequently, we have that the matrix for the derivative $Df(x, y)$ is:

$$\begin{pmatrix} f_x & f_y \end{pmatrix}$$

Now, f_x is the slope of f assuming that only x is changing and that for fixed y , f is a straight line. In other words, f_x is the slope of the *tangent line* in the x direction at the point (x, y, z) on the graph of f . We

compute it by taking the derivative of the formula of $f(x, y)$ assuming that y is constant and only x is variable. Similarly, we compute f_y by taking the derivative of $f(x, y)$ assuming that x is constant and only y is variable.

Example 3. Suppose that $f(x, y) = x^2 + 2xy$. Then, f_x is found by pretending that y is a constant and then just taking a derivative of $x^2 + 2xy$. The result is: $f_x = 2x + 2y$. Likewise, we compute f_y and find that $f_y = 2x$. So in this case:

$$Df(x, y) : \begin{pmatrix} 2x + 2y & 2x \end{pmatrix}$$

Example 4. Let's compute an approximation for Δf in the last example assuming that the input changes from the point $(-1, 1)$ by the amount: $(\Delta x, \Delta y) = (.1, .2)$. We simply compute:

$$Df(-1, 1)(.1, .2) = \begin{pmatrix} 2(-1) + 2(1) & 2(-1) \end{pmatrix} \cdot \begin{pmatrix} .1 \\ .2 \end{pmatrix} = \begin{pmatrix} 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} .1 \\ .2 \end{pmatrix} = -.4$$

This means that the z value of the surface described by f has approximately fallen .4 units as the input changes from $(-1, 1)$ to $(-1 + .1, 1 + .2) = (-.9, 1.2)$. The only reason why this is approximate is because the derivative calculation assumes that the function f is a plane (*which it is not*).

Example 5. Let's compute $Df(x, y)$ if $f(x, y) = \cos(x) + \sin(y)$. We calculate:

$$Df(x, y) : \begin{pmatrix} f_x & f_y \end{pmatrix} = \begin{pmatrix} -\sin(x) & \cos(y) \end{pmatrix}.$$

The derivative assumes that a function *is flat* at a point and measures how much the output of the function should change based on such an assumption. Let's build on this idea of "flat." Another way of saying this is that the graph of f looks approximately like a *shift of a linear transformation* nearby a point.

Smooth Function

A function is smooth if it at every point in its domain, it is approximated by a shift of a linear transformation. Which transformation we consider changes as we move from point to point.

Precise Definition of Smooth Function—Optional

To make this precise, we assume that we know how to take distances in the domain and codomain of the function. Then we say that a function f is smooth at an input vector v if and only if given $\epsilon > 0$, there exists δ such that if the distance from v to another vector w is less than δ , then there exists a linear transformation given by a matrix A such that the distance from $f(v) + A \cdot (w - v)$ to $f(w)$ is less than ϵ .

Derivative

The derivative of a smooth function f at an input point is the linear transformation such that *when shifted* approximates that function f near that point. In the precise definition, it is the linear transformation given by the matrix A .

Any function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ given by formulas for which we can take derivatives with respect to any variable while keeping the others constant is smooth. *Any surface, line, etc. that looks flat up close—as opposed to jagged—is describable by a smooth function.*

The matrix of the derivative is given in a column interpretation by

$$\begin{pmatrix} \underbrace{f_x}_{\hat{e}_1} & \underbrace{f_y}_{\hat{e}_2} & \underbrace{f_z}_{\hat{e}_3} & \cdots \end{pmatrix}.$$

Partial Derivatives

We call the expression f_x the partial derivative of f with respect to x .

There are n columns f_x, f_y, f_z, \dots , and there are m rows since each of these columns represent how much the output of f is changing. Such a change lives in the codomain. Yet this should be clear: a shift of the derivative mimics the function itself.

Consequently, the derivative as a linear transformation should have the same domain and codomain as the function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$.

Example 6. Let's take the derivative of $f : \mathbb{R}^3 \rightarrow \mathbb{R}$ given by $f(x, y, z) = xy + yz^3$. We should get a 1×3

matrix in the column interpretation since the derivative should be a linear transformation *also* with $\mathbb{R}^3 \rightarrow \mathbb{R}$.

$$Df(x, y) : \begin{pmatrix} f_x & f_y & f_z \end{pmatrix} = \begin{pmatrix} y & x + z^3 & 3yz^2 \end{pmatrix}$$

Example 7. Let's compute the derivative of $f : \mathbb{R}^3 \rightarrow \mathbb{R}$ given by $f(x, y, z) = \cos(xyz^3)$. We should get a 1×3 matrix in the column interpretation since the derivative should be a linear transformation *also* with $\mathbb{R}^3 \rightarrow \mathbb{R}$. We have:

$$Df(x, y) : \begin{pmatrix} f_x & f_y & f_z \end{pmatrix} = \begin{pmatrix} -yz^3 \sin(xyz^3) & -xz^3 \sin(xyz^3) & -3xyz^2 \sin(xyz^3) \end{pmatrix}$$

where we have used the chain rule with respect to each variable one at a time.

Example 8. Let's compute the derivative of $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by $f(x, y) = (x + y, x^2 - 3y)$. We should get a 2×2 matrix in the column interpretation since the derivative should be a linear transformation *also* with $\mathbb{R}^2 \rightarrow \mathbb{R}^2$.

$$Df(x, y) : \begin{pmatrix} f_x & f_y \end{pmatrix}$$

Now, notice that the columns f_x and f_y should live in \mathbb{R}^2 . We compute:

$$f_x = (x + y, x^2 - 3y)_x = (1, 2x)$$

where we have taken the derivative with respect to x only in each component of the function output. Likewise,

$$f_y = (x + y, x^2 - 3y)_y = (1, -3)$$

Therefore,

$$Df(x, y) : \begin{pmatrix} 1 & 1 \\ 2x & -3 \end{pmatrix}$$

Example 9. Let's compute the derivative of $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ given by $f(x, y) = (x^2, \sin(y), xy)$.

$$Df(x, y) : \begin{pmatrix} f_x & f_y \end{pmatrix} = \begin{pmatrix} 2x & 0 \\ 0 & \cos(y) \\ y & x \end{pmatrix}$$

where

$$f_x = (x^2, \sin(y), xy)_x = (2x, 0, y)$$

and

$$f_y = (0, \cos(y), x).$$

Example 10. Let $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ be given by $f(x, y) = x^2 + xy + y^2$. We have:

$$Df(x, y) : \begin{pmatrix} 2x + y & x + 2y \end{pmatrix}$$

Now, let's compute the second derivative of f . That is, let's compute the derivative of this function $Df : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by $Df(x, y) = (2x + y, x + 2y)$. That is, *the entries of the matrix* itself for the first derivative describes a function that we are now taking the derivative of. We will notate this derivative as:

$$D^2f(x, y) : \begin{pmatrix} Df_x & Df_y \end{pmatrix}$$

We compute

$$Df_x = (2x + y, x + 2y)_x = (2, 1)$$

and

$$Df_y = (2x + y, x + 2y)_y = (1, 2)$$

Therefore, the second derivative is:

$$D^2f(x, y) : \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

Example 11. Let $f : \mathbb{R}^3 \rightarrow \mathbb{R}$ be given by $f(x, y, z) = xy + yz + xz^3$. Let's compute $D^2f(x, y, z)$. First,

$$Df(x, y, z) : \begin{pmatrix} y + z^3 & x + z & 3xz^2 \end{pmatrix}$$

The first derivative *matrix* entries themselves describe a function $\mathbb{R}^3 \rightarrow \mathbb{R}^3$. Then the derivative of this first derivative should be represented by a 3×3 matrix:

$$D^2f(x, y, z) : \begin{pmatrix} Df_x & Df_y & Df_z \end{pmatrix} = \begin{pmatrix} 0 & 1 & 3z^2 \\ 1 & 0 & 1 \\ 3z^2 & 0 & 6xz \end{pmatrix}$$

The derivative of a function can be described as a matrix. This matrix itself, thought of as a function such that each entry is an output component, may have a different domain and codomain than the original function. Hence, the matrix dimensions of the second derivative may differ from the matrix dimensions of the first derivative.

Second Derivative

Take a function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ which has a derivative $n \times m$ matrix Df . Take the entries in that derivative matrix and rearrange them into a tuple of length nm . Rotate that tuple into a column. When we take all of the partial derivatives of the column entries with respect to x , we get the column Df_x . Similarly we can get Df_y , Df_z , etc. Then the second derivative matrix D^2f is given by

$$D^2f : \begin{pmatrix} Df_x & Df_y & \dots \end{pmatrix}.$$

Notice that in our two examples of taking the second derivative that $m = 1$.

In chapter 7, we will see how we can use the second derivative matrix to identify if a point gives a maximum or minimum output value of a function. For now, just think of the second derivative matrix describing how we can approximate how much *the first derivative matrix itself as a matrix changes as the input changes*.

3.2.3 Chain Rule

Taking a derivative is just pretending that how the function changes from a point is a linear transformation. What about if we had a composition like $f \circ g$ where $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ is given by $f(x, y) = x \cdot y$ and $g : \mathbb{R} \rightarrow \mathbb{R}^2$ is given by $g(t) = (2t, 3t^2)$? Does it not make sense that the composition of the two approximating linear transformations would be the approximating linear transformation for the composition itself? That is, just as the functions compose, so do the linear transformations. But remember what it means for two linear transformations to compose—it means to matrix multiply! So, we simply multiply the two derivative matrices together! So, in this case,

$$Df(x, y) : \begin{pmatrix} y & x \end{pmatrix} \quad Dg(t) : \begin{pmatrix} 2 \\ 6t \end{pmatrix}$$

So, now to get the derivative matrix for $D(f \circ g)(t)$ where $f \circ g$ is a function $\mathbb{R} \rightarrow \mathbb{R}$, we just matrix multiply:

$$D(f \circ g) : \begin{pmatrix} y & x \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 6t \end{pmatrix} = \begin{pmatrix} 2y + 6xt \end{pmatrix}$$

Notice that we get a 1×1 matrix. Yet also realize that we are plugging in the output $(2t, 3t^2)$ of g to the input (x, y) of f . This means that $(x, y) = (2t, 3t^2)$ so that $x = 2t$ and $y = 3t^2$. Therefore, the matrix for the

derivative $D(f \circ g)$ ends up being simply:

$$(2y + 6xt) = (2 \cdot (3t^2) + 6 \cdot (2t) \cdot t) = 18t^2.$$

This is just as we would expect if we were to rewrite $(f \circ g)(t) = f(g(t)) = f(2t, 3t^2) = 6t^3$ and realize that the derivative of $6t^3$ is indeed $18t^2$ just as we computed with matrix multiplication!

Chain Rule is Matrix Multiplication

If f and g are smooth functions, let Df and Dg represent their respective derivative matrices given in column interpretations. Then, $Df \cdot Dg$ represents the matrix for the derivative of $f \circ g$ given in a column interpretation.

Example 12. Suppose that $f(x, y) = (y, -x)$ and $g(x, y) = (x + y, y - x)$. Then the matrix Df is given by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and the matrix Dg is given by $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$. Therefore, $D(f \circ g)$ is given by:

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

Indeed, $f(g(x, y)) = f(x + y, y - x) = (y - x, -x - y)$. One can check that the derivative matrix of this function matches the matrix multiplication.

3.2.4 Machine Learning

The key to a lot of machine learning is to use the first derivative matrix of a function to adjust the parameters that define another function f . The function f itself is the “brain” although *it is nothing more than numeric operations applied to numeric inputs*. In fact, matrix multiplication itself can be used in the definition of the function f . The parameters that define the function (like matrix entries) are considered *variable during learning* while the input and the observed desired output are considered *constant during learning*.

What is now variable during learning is adjusted according to the derivative matrix of a function g . The function g has those variable parameters that define f as inputs and the output of g is the square of the “distance” between the desired output vector and the computed output vector from f .

In chapter 5 we will learn more about what this “distance” means—it is the length of the vector formed by subtracting the desired output vector and the computed output vector.

But just think of the output of g as being a measure of how close our function is to working correctly. The smaller the output of g the better the function f is working.

We simply *subtract* from the matrix of the inputs of g (remember that these are the parameters of f) a

portion of the derivative matrix of g . *The effect is for the output of g to go downhill—so that the output of g is minimized as desired.*

Instead of running through all of the details that could pop up, we ourselves will do some observing. Run and experiment with the code in the SageMath activity at the link below:



[Link to run the code.](#)

```

var('a','b','c','d')
A=matrix(2,2,[a,b,c,d])
#Define our algorithm by a matrix multiplication where the matrix
#entries are just variables. Really we did not have to use a matrix function
#Just one for which we can compute the derivative and have enough parameters
f(x,y)=vector([x,y])*A
C={a:1,b:2,c:3,d:4}

#This is the square of the length of a vector. We want to minimize it.
def squaresum(v):
    return sum([j^2 for j in v])

def Learn(input,actual,C):
    output=f(input[0],input[1])
    #This outputs the square of the length of the
    #difference between the calculated output
    #and the actual output for a given input
    g(a,b,c,d)=squaresum(actual-output)
    #Just modify the matrix parameters a little each time
    #By the a negative proportion of the derivative matrix of g with respect to
    #the parameters a,b,c,d where the input and the observed actual are held constant.
    gderivative=vector(derivative(g)(a=C[a],b=C[b],c=C[c],d=C[d]))
    CC=gderivative*(-.01)+vector([C[a],C[b],C[c],C[d]])
    #The matrix parameters of A are modified here:
    C={a:CC[0].n(),b:CC[1].n(),c:CC[2].n(),d:CC[3].n()}
    return C

#Input
v=vector([2,3])
#Observed output
w=vector([1,5])
#Input
v1=vector([4,5])
#Observed output
w1=vector([3,1])

```

```

#At first:
print("Beginning Matrix Function (rounds after multiplication):")
print(A(a=C[a],b=C[b],c=C[c],d=C[d]))
print("At first input (2,3) and get:")
result=f(2,3)(a=C[a],b=C[b],c=C[c],d=C[d])
print(vector([round(j) for j in result]))
print("At first input (4,5) and get:")
result=f(4,5)(a=C[a],b=C[b],c=C[c],d=C[d])
print(vector([round(j) for j in result]))


#Lets try some repetitive observations
print("Now learning through some observations...")

print("We observe what should happen:")
print("(2,3) should be sent to (1,5) and (4,5) should be sent to (3,1)")
print("At first let's just observe (2,3) to (1,5) only")
print("and see how the output changes if input=(2,3) over 12 repeated observations:")
for i in range(12):
    C=Learn(v,w,C)
    result=f(2,3)(a=C[a],b=C[b],c=C[c],d=C[d])
    print(vector([round(j) for j in result]))
print("Seems to have learned. But is the \"brain\" of our function \"smart\" ")
print("enough to learn two things?")
print("It is going to take a lot of observations: 1300.")
print("Obviously the \"brain\" of our 2x2 matrix function is small.")
for i in range(1300):
    C=Learn(v,w,C)
    C=Learn(v1,w1,C)

#Now f is given by the following matrix:
print("Learned Matrix Function (rounds after multiplication):")
print(A(a=C[a],b=C[b],c=C[c],d=C[d]))
print("Now input (2,3) and get:")
result=f(2,3)(a=C[a],b=C[b],c=C[c],d=C[d])
print(vector([round(j) for j in result]))
print("Now input (4,5) and get:")
result=f(4,5)(a=C[a],b=C[b],c=C[c],d=C[d])
print(vector([round(j) for j in result]))
#Notice that eventually the function with the changed parameters responds to the observation and
#changes itself so that it gives something close to the desired output.

```

Key Concepts from this Section

- **lines and planes are fibers:** (page 217) Lines and planes are fibers of linear transformations.
- **graph:** (page 217) The graph of the function $z = f(x, y)$ where $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ is the fiber $h^{-1}(0)$ in 3-space of the function $h : \mathbb{R}^3 \rightarrow \mathbb{R}$ given by $h(x, y, z) = f(x, y) - z$. Of course if we defined h differently like $h(x, y) = f(x, y) - z + 1$, then the graph would be the fiber $h^{-1}(1)$.
- **lines and planes are graphs of shifts:** (page 217) Lines and planes can be thought of as graphs (i.e. fibers) of functions. Those functions themselves are shifts of linear transformations.

- **derivative of a function $\mathbb{R}^2 \rightarrow \mathbb{R}$:** (page 219) Consider the figure above. Assume that the graph of $z = f(x, y)$ looks approximately flat like a plane at the point (x, y, z) on its graph. Suppose further that we would like to measure the change of f (notated as Δf) as the input moves from (x, y) to $(x + \Delta x, y + \Delta y)$. Computationally, we have:

$$\Delta f = f(x + \Delta x, y + \Delta y) - f(x, y).$$

Notice that this is a vertical distance between two points on the graph. Then, the derivative (notated $Df(x, y)$) of f at (x, y) is a linear transformation $\mathbb{R}^2 \rightarrow \mathbb{R}$ that tells us precisely what Δf would be if the function f were actually flat like a plane itself. That is, $Df(x, y)$ is described as:

$$(\Delta x, \Delta y) \mapsto \Delta f$$

- **f_x :** (page 220) Assume that the graph of $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ given by $(x, y) \mapsto z$ is approximated by a plane through a point (x, y, z) . All the points on the plane that have the same y value as this point form a line. We call the slope of this line f_x . This emphasizes that along this line, f is a function of x . The variable x is the only one changing.
- **f_y :** (page 220) Assume that the graph of $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ given by $(x, y) \mapsto z$ is approximated by a plane through a point (x, y, z) . All the points on the plane that have the same x value as this point form a line. We call the slope of this line f_y . This emphasizes that along this line, f is a function of y . The variable y is the only one changing.
- **smooth function:** (page 221) A function is smooth if it at every point in its domain, it is approximated by a shift of a linear transformation. Which transformation we consider changes as we move from point to point.
- **precise definition of smooth function—optional:** (page 221) To make this precise, we assume that we know how to take distances in the domain and codomain of the function. Then we say that a function f is smooth at an input vector v if and only if given $\epsilon > 0$, there exists δ such that if the distance from v to another vector w is less than δ , then there exists a linear transformation given by a matrix A such that the distance from $f(v) + A \cdot (w - v)$ to $f(w)$ is less than ϵ .
- **derivative:** (page 222) The derivative of a smooth function f at an input point is the linear transformation such that when shifted approximates that function f near that point. In the precise definition, it is the linear transformation given by the matrix A .
- **partial derivatives:** (page 222) We call the expression f_x the partial derivative of f with respect to x .
- **second derivative:** (page 225) Take a function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ which has a derivative $n \times m$ matrix Df . Take the entries in that derivative matrix and rearrange them into a tuple of length nm . Rotate that tuple into a column. When we take all of the partial derivatives of the column entries with respect to x , we get

the column Df_x . Similarly we can get Df_y , Df_z , etc. Then the second derivative matrix D^2f is given by

$$D^2f : \begin{pmatrix} Df_x & Df_y & \cdots \end{pmatrix}.$$

- **chain rule is matrix multiplication:** (page 226) If f and g are smooth functions, let Df and Dg represent their respective derivative matrices given in column interpretations. Then, $Df \cdot Dg$ represents the matrix for the derivative of $f \circ g$ given in a column interpretation.

3.2.5 Exercises

Planes and Lines as Fibers

1. Find a function $h : \mathbb{R}^2 \rightarrow \mathbb{R}$ and an element $c \in \mathbb{R}$ so that the line $x + 2y = 3$ is the fiber $h^{-1}(c)$.
2. Find a function $h : \mathbb{R}^2 \rightarrow \mathbb{R}$ and an element $c \in \mathbb{R}$ so that the line $y = 5x - 7$ is the fiber $h^{-1}(c)$.
3. Find a function $h : \mathbb{R}^3 \rightarrow \mathbb{R}$ and an element $c \in \mathbb{R}$ so that the plane $x + 2y - z = 4$ is the fiber $h^{-1}(c)$.
4. Find a function $h : \mathbb{R}^3 \rightarrow \mathbb{R}$ and an element $c \in \mathbb{R}$ so that the plane $z = -5x - y + 11$ is the fiber $h^{-1}(c)$.

Find the First Derivative

Find the matrix for the first derivative of the following functions.

5. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$

$$\begin{aligned} f(x, y) = \\ (-8y^4, 4x + 4y, 4x^3y + 4xy) \end{aligned}$$

6. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$

$$\begin{aligned} f(x, y) = \\ (4x^3y + 2xy, -6y^4 + 12xy, 2x + y) \end{aligned}$$

7. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$f(x, y) = (-5y^4 + 2xy, 2x^3y + 3xy)$$

8. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$f(x, y) = (2x - 2y, 2x^3y + 2xy)$$

9. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$

$$\begin{aligned} f(x, y) = \\ (4x, 3x^3y + 4xy, -7y^4 + 9xy) \end{aligned}$$

10. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$

$$f(x, y) = (-y^4, y, x^3y)$$

11. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$f(x, y) = (2x^3y, -y)$$

12. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$

$$f(x, y) = (3x - 4y, -3y^4, 3xy)$$

13. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$f(x, y) = (-2y^4 + xy, x^3y + xy)$$

14. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = (4x - y)$$

15. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$f(x, y) = (3x - 2y, -4y^4 + 3xy)$$

16. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$

$$f(x, y) = (4xy, 4x - 4y, -4y^4)$$

17. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = (-5y^4 + 12xy)$$

18. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$f(x, y) = (-3y^4, 3x - 2y)$$

19. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = (0)$$

20. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = (4x^3y + 3xy)$$

21. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

$$f(x, y, z) = (3x^3z, xyz, 0)$$

22. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = (y + 3z)$$

23. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

$$\begin{aligned} f(x, y, z) = \\ (x^3z + 4xy, xyz, -3y + 4z) \end{aligned}$$

24. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

$$f(x, y, z) = (xyz, 2x^3z + xy, z)$$

25. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$

$$f(x, y, z) = (xyz, 3y + z)$$

26. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

$$f(x, y, z) = (-2y, xyz, x^3z)$$

27. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

$$\begin{aligned} f(x, y, z) = \\ (2x^3z + 3xy, y + 3z, xyz) \end{aligned}$$

28. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = (x^3z + 2xy)$$

29. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$

$$f(x, y, z) = (xy, xyz)$$

30. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

$$f(x, y, z) = (-y + 4z, xyz, 4xy)$$

31. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = (4xy)$$

32. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = (3x^3z + xy)$$

33. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = (4z)$$

34. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

$$\begin{aligned} f(x, y, z) = \\ (xyz, 3x^3z + 4xy, 3y + 4z) \end{aligned}$$

35. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$

$$f(x, y, z) = (2x^3z + 3xy, 3z)$$

36. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = (2y + 4z)$$

Find the Second Derivative

Find the matrix for the second derivative of the following functions.

37. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = x^2 - 2y^2$$

38. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = -4y^4 + xy$$

39. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = 2x^3y + 4xy$$

40. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = x^3y + xy$$

41. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = x^3y + 4xy$$

42. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = -8y^4 + 8xy$$

43. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = x^2 - y^2$$

44. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = 4x^2 + 2y^2$$

45. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = -4y^4 + 3xy$$

46. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = 2x^2$$

47. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = -5y^4$$

48. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = xy$$

49. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = -2y^4$$

50. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = 2x^3y + xy$$

51. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = -4y^4$$

52. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = 2x^2 - y^2$$

53. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = 4x^3z$$

54. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = 4xy$$

55. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = xyz$$

56. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = 0$$

57. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = 3x^3z + 4xy$$

58. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = 3y$$

59. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = y + 3z$$

60. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = 4x^3z + 3xy$$

61. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = -3y + 2z$$

62. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = 3z$$

Approximating Change

Give a linear approximation for Δf (how much f changes) as the input changes from $(\Delta x, \Delta y)$ to $(x + \Delta x, y + \Delta y)$.

63. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = (-2 y^4)$$

$$\Delta x = 0.2 \quad \Delta y = -0.1$$

$$(x, y) = (1, 0)$$

64. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = (4 x^3 y + 4 x y)$$

$$\Delta x = 0.3 \quad \Delta y = -0.3$$

$$(x, y) = (4, 3)$$

65. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$f(x, y) = (x - 2 y, x^3 y + x y)$$

$$\Delta x = -0.2 \quad \Delta y = -0.1$$

$$(x, y) = (1, 1)$$

66. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$

$$f(x, y) = (-8 y^4 + 4 x y, 4 x + 3 y, 4 x^3 y + 4 x y)$$

$$\Delta x = -0.2 \quad \Delta y = 0.2$$

$$(x, y) = (2, 0)$$

67. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$

$$f(x, y) = (-y^4 + 4 x y, -3 y, x^3 y)$$

$$\Delta x = 0.4 \quad \Delta y = -0.4$$

$$(x, y) = (2, 0)$$

68. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$f(x, y) = (2 x^3 y + 4 x y, -6 y^4 + 4 x y)$$

$$\Delta x = 0.1 \quad \Delta y = -0.4$$

$$(x, y) = (1, 1)$$

69. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = (-4 y^4 + 6 x y)$$

$$\Delta x = -0.1 \quad \Delta y = 0.4$$

$$(x, y) = (3, 1)$$

70. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$f(x, y) = (x^3 y + x y, x)$$

$$\Delta x = -0.3 \quad \Delta y = 0.2$$

$$(x, y) = (2, 1)$$

71. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = (x - y)$$

$$\Delta x = 0.2 \quad \Delta y = -0.3$$

$$(x, y) = (4, 2)$$

72. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = (x^3 y + xy)$$

$$\Delta x = 0.4 \quad \Delta y = -0.5$$

$$(x, y) = (3, 1)$$

The Chain Rule

Use the chain rule to find the matrix $D(f \circ g)$ for the following:

73. $f(x, y) = (x + 5y, 3x - y)$

$$g(x) = (3x + 1, x^2)$$

75. $f(x, y) = (3x + 4y)$

$$g(x, y) = (3x + y, x^2 + 3y)$$

77. $f(x, y) = (3x - y, 3x + y, 3x + 5y)$

$$g(x) = (x + 1, 3x^2)$$

79. $f(x, y) = (12x - y, x + 2y, x + 5y)$

$$g(x, y) = (x + y, x^2 + y)$$

81. $f(x, y) = (5y, 0, 6x - y)$

$$g(x, y) = (y, x^2)$$

74. $f(x, y) = (9x - y, 2y)$

$$g(x) = (2x + 3, 0)$$

76. $f(x, y) = (x + 5y)$

$$g(x, y) = (x + y, x^2 + y)$$

78. $f(x, y) = (9x - y, x + 5y)$

$$g(x, y) = (x + y, x^2 + y)$$

80. $f(x, y) = (9x - y, 3x + 2y, 3x + 5y)$

$$g(x, y) = (3x + y, x^2 + 3y)$$

82. $f(x, y) = (2x + 5y)$

$$g(x) = (3, 2x^2)$$

For the following, make sure to actually plug the output of g into the derivative matrix for f before multiplying matrices!

$$\mathbf{83.} \quad f(x, y) = (3x - y, xy, 5xy)$$

$$g(x, y) = (y, x^2)$$

$$\mathbf{84.} \quad f(x, y) = \\ (9x - y, 2xy + 2x, 5xy + 2x)$$

$$g(x) = (2x + 3, 2x^2)$$

$$\mathbf{85.} \quad f(x, y) = (3x - y, 5xy + 4x)$$

$$\mathbf{86.} \quad f(x, y) = (5xy + 3x)$$

$$g(x) = (3x + 1, 4x^2)$$

$$g(x) = (3x + 1, 3x^2)$$

$$\mathbf{87.} \quad f(x, y) = (12x - y, 3xy + 2x)$$

$$\mathbf{88.} \quad f(x, y) = (5xy)$$

$$g(x) = (3x + 4, 2x^2)$$

$$g(x, y) = (y, x^2)$$

$$\mathbf{89.} \quad f(x, y) = (5xy + 4x)$$

$$\mathbf{90.} \quad f(x, y) = (6x - y)$$

$$g(x) = (4x + 4, 4x^2)$$

$$g(x) = (2x + 2, 3x^2)$$

3.2.6 Solutions

1. $h(x, y) = x + 2y - 3$ and $c = 0$ is one possible solution. Or we could define $h(x, y) = x + 2y$ and say that $c = 3$.

2. $h(x, y) = 5x - y - 7$ and $c = 0$ is one possible solution. Or we could define $h(x, y) = 5x - y$ and say that $c = 7$.

3. $h(x, y, z) = x + 2y - z - 4$ and $c = 0$ is one possible solution. Or we could define $h(x, y, z) = x + 2y - z$ and say that $c = 4$.

4. $h(x, y, z) = 5x + y + z - 11$ and $c = 0$ is one possible solution. Or we could define $h(x, y, z) = 5x + y + z$ and say that $c = 11$.

$$\text{5. } \begin{pmatrix} 0 & -32y^3 \\ 4 & 4 \\ 12x^2y + 4y & 4x^3 + 4x \end{pmatrix}$$

$$\text{6. } \begin{pmatrix} 12x^2y + 2y & 4x^3 + 2x \\ 12y & -24y^3 + 12x \\ 2 & 1 \end{pmatrix}$$

$$\text{7. } \begin{pmatrix} 2y & -20y^3 + 2x \\ 6x^2y + 3y & 2x^3 + 3x \end{pmatrix}$$

$$\text{8. } \begin{pmatrix} 2 & -2 \\ 6x^2y + 2y & 2x^3 + 2x \end{pmatrix}$$

$$\text{9. } \begin{pmatrix} 4 & 0 \\ 9x^2y + 4y & 3x^3 + 4x \\ 9y & -28y^3 + 9x \end{pmatrix}$$

$$\text{10. } \begin{pmatrix} 0 & -4y^3 \\ 0 & 1 \\ 3x^2y & x^3 \end{pmatrix}$$

$$\text{11. } \begin{pmatrix} 6x^2y & 2x^3 \\ 0 & -1 \end{pmatrix}$$

$$\text{12. } \begin{pmatrix} 3 & -4 \\ 0 & -12y^3 \\ 3y & 3x \end{pmatrix}$$

$$\text{13. } \begin{pmatrix} y & -8y^3 + x \\ 3x^2y + y & x^3 + x \end{pmatrix}$$

$$\text{14. } \begin{pmatrix} 4 & -1 \end{pmatrix}$$

15. $\begin{pmatrix} 3 & -2 \\ 3y & -16y^3 + 3x \end{pmatrix}$

16. $\begin{pmatrix} 4y & 4x \\ 4 & -4 \\ 0 & -16y^3 \end{pmatrix}$

17. $\begin{pmatrix} 12y & -20y^3 + 12x \end{pmatrix}$

18. $\begin{pmatrix} 0 & -12y^3 \\ 3 & -2 \end{pmatrix}$

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

20. $\begin{pmatrix} 12x^2y + 3y & 4x^3 + 3x \end{pmatrix}$

21. $\begin{pmatrix} 9x^2z & 0 & 3x^3 \\ yz & xz & xy \\ 0 & 0 & 0 \end{pmatrix}$

22. $\begin{pmatrix} 0 & 1 & 3 \end{pmatrix}$

23. $\begin{pmatrix} 3x^2z + 4y & 4x & x^3 \\ yz & xz & xy \\ 0 & -3 & 4 \end{pmatrix}$

24. $\begin{pmatrix} yz & xz & xy \\ 6x^2z + y & x & 2x^3 \\ 0 & 0 & 1 \end{pmatrix}$

25. $\begin{pmatrix} yz & xz & xy \\ 0 & 3 & 1 \end{pmatrix}$

26. $\begin{pmatrix} 0 & -2 & 0 \\ yz & xz & xy \\ 3x^2z & 0 & x^3 \end{pmatrix}$

27. $\begin{pmatrix} 6x^2z + 3y & 3x & 2x^3 \\ 0 & 1 & 3 \\ yz & xz & xy \end{pmatrix}$

28. $\begin{pmatrix} 3x^2z + 2y & 2x & x^3 \end{pmatrix}$

29. $\begin{pmatrix} y & x & 0 \\ yz & xz & xy \end{pmatrix}$

30. $\begin{pmatrix} 0 & -1 & 4 \\ yz & xz & xy \\ 4y & 4x & 0 \end{pmatrix}$

31. $\begin{pmatrix} 4y & 4x & 0 \end{pmatrix}$

32. $\begin{pmatrix} 9x^2z + y & x & 3x^3 \end{pmatrix}$

33. $\begin{pmatrix} 0 & 0 & 4 \end{pmatrix}$

34. $\begin{pmatrix} yz & xz & xy \\ 9x^2z + 4y & 4x & 3x^3 \\ 0 & 3 & 4 \end{pmatrix}$

35. $\begin{pmatrix} 6x^2z + 3y & 3x & 2x^3 \\ 0 & 0 & 3 \end{pmatrix}$

36. $\begin{pmatrix} 0 & 2 & 4 \end{pmatrix}$

37. $\begin{pmatrix} 2 & 0 \\ 0 & -4 \end{pmatrix}$

38. $\begin{pmatrix} 0 & 1 \\ 1 & -48y^2 \end{pmatrix}$

39. $\begin{pmatrix} 12xy & 6x^2 + 4 \\ 6x^2 + 4 & 0 \end{pmatrix}$

40. $\begin{pmatrix} 6xy & 3x^2 + 1 \\ 3x^2 + 1 & 0 \end{pmatrix}$

41. $\begin{pmatrix} 6xy & 3x^2 + 4 \\ 3x^2 + 4 & 0 \end{pmatrix}$

42. $\begin{pmatrix} 0 & 8 \\ 8 & -96y^2 \end{pmatrix}$

43. $\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$

44. $\begin{pmatrix} 8 & 0 \\ 0 & 4 \end{pmatrix}$

45. $\begin{pmatrix} 0 & 3 \\ 3 & -48y^2 \end{pmatrix}$

46. $\begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$

47. $\begin{pmatrix} 0 & 0 \\ 0 & -60y^2 \end{pmatrix}$

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

49. $\begin{pmatrix} 0 & 0 \\ 0 & -24y^2 \end{pmatrix}$

50. $\begin{pmatrix} 12xy & 6x^2 + 1 \\ 6x^2 + 1 & 0 \end{pmatrix}$

51. $\begin{pmatrix} 0 & 0 \\ 0 & -48y^2 \end{pmatrix}$

52. $\begin{pmatrix} 4 & 0 \\ 0 & -2 \end{pmatrix}$

53. $\begin{pmatrix} 24xz & 0 & 12x^2 \\ 0 & 0 & 0 \\ 12x^2 & 0 & 0 \end{pmatrix}$

54. $\begin{pmatrix} 0 & 4 & 0 \\ 4 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

55. $\begin{pmatrix} 0 & z & y \\ z & 0 & x \\ y & x & 0 \end{pmatrix}$

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

57. $\begin{pmatrix} 18xz & 4 & 9x^2 \\ 4 & 0 & 0 \\ 9x^2 & 0 & 0 \end{pmatrix}$

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

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

60. $\begin{pmatrix} 24xz & 3 & 12x^2 \\ 3 & 0 & 0 \\ 12x^2 & 0 & 0 \end{pmatrix}$

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

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

63. $\begin{pmatrix} 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0.2 \\ -0.1 \end{pmatrix} \approx \begin{pmatrix} 0.0 \end{pmatrix}$

64. $\begin{pmatrix} 588 & 272 \end{pmatrix} \cdot \begin{pmatrix} 0.3 \\ -0.3 \end{pmatrix} \approx \begin{pmatrix} 94.8 \end{pmatrix}$

65. $\begin{pmatrix} 1 & -2 \\ 4 & 2 \end{pmatrix} \cdot \begin{pmatrix} -0.2 \\ -0.1 \end{pmatrix} \approx \begin{pmatrix} 0.0 \\ -1.0 \end{pmatrix}$

66. $\begin{pmatrix} 0 & 8 \\ 4 & 3 \\ 0 & 40 \end{pmatrix} \cdot \begin{pmatrix} -0.2 \\ 0.2 \end{pmatrix} \approx \begin{pmatrix} 1.6 \\ -0.2 \\ 8.0 \end{pmatrix}$

67. $\begin{pmatrix} 0 & 8 \\ 0 & -3 \\ 0 & 8 \end{pmatrix} \cdot \begin{pmatrix} 0.4 \\ -0.4 \end{pmatrix} \approx \begin{pmatrix} -3.2 \\ 1.2 \\ -3.2 \end{pmatrix}$

68. $\begin{pmatrix} 10 & 6 \\ 4 & -20 \end{pmatrix} \cdot \begin{pmatrix} 0.1 \\ -0.4 \end{pmatrix} \approx \begin{pmatrix} -1.4 \\ 8.4 \end{pmatrix}$

69. $\begin{pmatrix} 6 & 2 \end{pmatrix} \cdot \begin{pmatrix} -0.1 \\ 0.4 \end{pmatrix} \approx \begin{pmatrix} 0.2 \end{pmatrix}$

70. $\begin{pmatrix} 13 & 10 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -0.3 \\ 0.2 \end{pmatrix} \approx \begin{pmatrix} -1.9 \\ -0.3 \end{pmatrix}$

71. $\begin{pmatrix} 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0.2 \\ -0.3 \end{pmatrix} \approx \begin{pmatrix} 0.5 \end{pmatrix}$

72. $\begin{pmatrix} 28 & 30 \end{pmatrix} \cdot \begin{pmatrix} 0.4 \\ -0.5 \end{pmatrix} \approx \begin{pmatrix} -3.8 \end{pmatrix}$

73. $\begin{pmatrix} 10x + 3 \\ -2x + 9 \end{pmatrix}$

74. $\begin{pmatrix} 18 \\ 0 \end{pmatrix}$

75. $\begin{pmatrix} 8x + 9 & 15 \end{pmatrix}$

76. $\begin{pmatrix} 10x + 1 & 6 \end{pmatrix}$

77. $\begin{pmatrix} -6x + 3 \\ 6x + 3 \\ 30x + 3 \end{pmatrix}$

78. $\begin{pmatrix} -2x + 9 & 8 \\ 10x + 1 & 6 \end{pmatrix}$

79. $\begin{pmatrix} -2x + 12 & 11 \\ 4x + 1 & 3 \\ 10x + 1 & 6 \end{pmatrix}$

80. $\begin{pmatrix} -2x + 27 & 6 \\ 4x + 9 & 9 \\ 10x + 9 & 18 \end{pmatrix}$

81. $\begin{pmatrix} 10x & 0 \\ 0 & 0 \\ -2x & 6 \end{pmatrix}$

82. $\begin{pmatrix} 20x \end{pmatrix}$

83. $\begin{pmatrix} -2x & 3 \\ 2xy & x^2 \\ 10xy & 5x^2 \end{pmatrix}$

84. $\begin{pmatrix} -4x + 18 \\ 8(2x + 3)x + 8x^2 + 4 \\ 20(2x + 3)x + 20x^2 + 4 \end{pmatrix}$

85. $\begin{pmatrix} -8x + 9 \\ 40(3x + 1)x + 60x^2 + 12 \end{pmatrix}$

86. $\begin{pmatrix} 30(3x + 1)x + 45x^2 + 9 \end{pmatrix}$

87. $\begin{pmatrix} -4x + 36 \\ 12(3x + 4)x + 18x^2 + 6 \end{pmatrix}$

88. $\begin{pmatrix} 10xy & 5x^2 \end{pmatrix}$

89. $\begin{pmatrix} 160(x + 1)x + 80x^2 + 16 \end{pmatrix}$

90. $\begin{pmatrix} -6x + 12 \end{pmatrix}$

Recursive Sequences

3.3

3.3.1 Exercises	247
3.3.2 Solutions	249

Questions to Guide Your Study:

- How do you write a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ that describes a recursion

$$a_{n+2} = c \cdot a_{n+1} + d \cdot a_n?$$

- How can you use matrix powers to come up with a nonrecursive formula for a_n ?

We can use matrices to describe how certain types of sequences are defined. For instance, suppose that we have a sequence a_0, a_1, a_2, \dots defined so $a_0 = 1$ and $a_1 = 3$ and $a_{n+2} = 2 \cdot a_n + a_{n+1}$ which is called a **recursive formula** for the sequence. We can compute a_2 by setting $n = 0$ in the recursive formula to obtain: $a_2 = 2 \cdot a_0 + a_1 = 2 \cdot 1 + 3 = 5$. Likewise, we can find a_3 by setting $n = 1$ to obtain: $a_3 = 2 \cdot a_1 + a_2 = 2 \cdot 3 + 5 = 11$. Generally, in order to compute a_n , we need to know what the two previous terms in the list are. But matrix magic can turn this idea into *repeated matrix multiplication*. Let's see how!

First, we think of this “recursive process” given by the formula $a_{n+2} = 2 \cdot a_n + a_{n+1}$ as a function. We have the two positions in the sequence (a_n, a_{n+1}) as an input and a_{n+2} as an output. But repeated matrix multiplication (i.e. matrix function composition) would really only work *if the domain were the same as the codomain*. That is, we think: $(a_n, a_{n+1}) \mapsto (a_{n+1}, a_{n+2})$. This process is a linear transformation $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ since $f(a_n, a_{n+1}) = (a_{n+1}, a_{n+2}) = (a_{n+1}, 2 \cdot a_n + a_{n+1})$ describes the output variables as *linear combinations of the input variables*.

Let's use a column interpretation to come up with the matrix for this function f . We think: $f(e_1) = f(1, 0) = (0, 2 \cdot 1 + 0) = (0, 2)$ and $f(e_2) = f(0, 1) = (1, 2 \cdot 0 + 1) = (1, 1)$. Therefore, we find that f is given by the matrix:

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

If we let

$$f^{(n)} = \underbrace{f \circ f \circ f \circ \cdots \circ f}_{n \text{ times}},$$

then the linear transformation $f^{(n)}$ is given by

$$A^n = \underbrace{A \cdot A \cdot A \cdots A}_{n \text{ times}}.$$

This means that $A^n \cdot \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$ has shifted the pair (a_0, a_1) forward n times to (a_n, a_{n+1}) . Therefore,

$$\begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

In particular, we only want the top component a_n . So using a row interpretation, we know we can pick out the top (row—which is a single element in this case) of a matrix $\begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix}$ by multiplying by $\begin{pmatrix} 1 & 0 \end{pmatrix}$ on the left:

$$\begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

Using $a_0 = 1$, $a_1 = 3$, and multiplying on the left side of the equation, we obtain:

$$a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

We have just turned the recursive formula for the sequence into a (matrix multiplication) formula which depends only on n .



Example 1. Suppose that $a_0 = -2$, $a_1 = 1$ and $a_{n+2} = 3a_n - 5a_{n+1}$. Let's find a matrix multiplication formula for a_n using a column interpretation for the matrix we raise to the n th power. Letting $x = a_0$ and $y = a_1$, we think: $f(x, y) = (y, 2x - 5y)$ and compute $f(e_1) = f(1, 0) = (0, 2)$. Also, $f(e_2) = f(0, 1) = (1, -5)$. Therefore, our matrix is $\begin{pmatrix} 0 & 1 \\ 2 & -5 \end{pmatrix}$ and we have as in the reading above:

$$a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 2 & -5 \end{pmatrix}^n \cdot \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

Recursion to Matrix Powers via Columns

Suppose that $a_{n+2} = c \cdot a_n + d \cdot a_{n+1}$. Then, the recursion is given by the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by $f(x, y) = (y, cx + dy)$. Let A be the matrix which describes f according to a *column* interpretation. Then:

$$a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot A^n \cdot \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

Example 2. Suppose that $a_0 = 4$, $a_1 = -1$ and $a_{n+2} = -2a_n + 3a_{n+1}$. Let's find a matrix multiplication formula for a_n using a *row* interpretation for the matrix we raise to the n th power. Letting $x = a_0$ and $y = a_1$, we think: $f(x, y) = (y, 2x - 5y)$ and compute $f(e_1) = f(1, 0) = (0, 2)$. Also, $f(e_2) = f(0, 1) = (1, -5)$. Therefore, our matrix is $\begin{pmatrix} 0 & 2 \\ 1 & -5 \end{pmatrix}$ in a row interpretation. Then we have

$$\begin{pmatrix} a_n & a_{n+1} \end{pmatrix} = \begin{pmatrix} a_0 & a_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 1 & -5 \end{pmatrix}^n$$

Using $a_0 = 4$, $a_1 = -1$, and multiplying both sides of the equation on the right by $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ to pick out the left column (which is just the entry a_n), we have:

$$\begin{pmatrix} a_n & a_{n+1} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 1 & -5 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$a_n = \begin{pmatrix} 4 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 1 & -5 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Recursion to Matrix Powers via Rows

Suppose that $a_{n+2} = c \cdot a_n + d \cdot a_{n+1}$. Then, the recursion is given by the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by $f(x, y) = (y, cx + dy)$. Let A be the matrix which describes f according to a *row* interpretation. Then:

$$a_n = \begin{pmatrix} a_0 & a_1 \end{pmatrix} \cdot A^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Key Concepts from this Section

- **recursive formula:** (page 243) Let a_n represent a sequence. A recursive formula for a_n is a formula that depends on previous entries in the sequence. For instance, $a_n = a_{n-2} + 5 \cdot a_{n-4}$ would be a recursive formula. Such a formula is not complete until we have declared enough beginning entries in the sequence such as $a_0 = 5$, $a_1 = 2$ and so forth.
- **recursion to matrix powers via columns:** (page 244) Suppose that $a_{n+2} = c \cdot a_n + d \cdot a_{n+1}$. Then, the recursion is given by the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by $f(x, y) = (y, cx + dy)$. Let A be the matrix which describes f according to a *column* interpretation. Then:

$$a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot A^n \cdot \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

- **recursion to matrix powers via rows:** (page 245) Suppose that $a_{n+2} = c \cdot a_n + d \cdot a_{n+1}$. Then, the recursion is given by the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by $f(x, y) = (y, cx + dy)$. Let A be the matrix which describes f according to a *row* interpretation. Then:

$$a_n = \begin{pmatrix} a_0 & a_1 \end{pmatrix} \cdot A^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

3.3.1 Exercises

Recursion by a Column Interpretation

Write a formula for a_n using a matrix power where the matrix gives the recursion by a column interpretation.

1. $a_{n+2} = 2 \cdot a_n + 1 \cdot a_{n+1}$

$$a_0 = 4, \quad a_1 = 3$$

2. $a_{n+2} = 1 \cdot a_n + 1 \cdot a_{n+1}$

$$a_0 = 4, \quad a_1 = 2$$

3. $a_{n+2} = 2 \cdot a_n + 2 \cdot a_{n+1}$

$$a_0 = 3, \quad a_1 = 1$$

4. $a_{n+2} = 4 \cdot a_n + 3 \cdot a_{n+1}$

$$a_0 = 4, \quad a_1 = 2$$

5. $a_{n+2} = 1 \cdot a_n + 1 \cdot a_{n+1}$

$$a_0 = 3, \quad a_1 = 1$$

6. $a_{n+2} = 3 \cdot a_n + 1 \cdot a_{n+1}$

$$a_0 = 2, \quad a_1 = 0$$

7. $a_{n+2} = 2 \cdot a_n + 4 \cdot a_{n+1}$

$$a_0 = 1, \quad a_1 = 3$$

8. $a_{n+2} = 1 \cdot a_n + 2 \cdot a_{n+1}$

$$a_0 = 1, \quad a_1 = 4$$

9. $a_{n+2} = 3 \cdot a_n + 1 \cdot a_{n+1}$

$$a_0 = 4, \quad a_1 = 3$$

10. $a_{n+2} = 3 \cdot a_n + 3 \cdot a_{n+1}$

$$a_0 = 3, \quad a_1 = 4$$

11. $a_{n+2} = 4 \cdot a_n + 4 \cdot a_{n+1}$

$$a_0 = 0, \quad a_1 = 4$$

12. $a_{n+2} = 1 \cdot a_n + 2 \cdot a_{n+1}$

$$a_0 = 3, \quad a_1 = 4$$

Recursion by a Row Interpretation

Write a formula for a_n using a matrix power where the matrix gives the recursion by a row interpretation.

13. $a_{n+2} = 2 \cdot a_n + 1 \cdot a_{n+1}$

$$a_0 = 2, \quad a_1 = 1$$

14. $a_{n+2} = 4 \cdot a_n + 1 \cdot a_{n+1}$

$$a_0 = 2, \quad a_1 = 2$$

15. $a_{n+2} = 3 \cdot a_n + 3 \cdot a_{n+1}$

$$a_0 = 1, \quad a_1 = 4$$

16. $a_{n+2} = 1 \cdot a_n + 1 \cdot a_{n+1}$

$$a_0 = 0, \quad a_1 = 2$$

17. $a_{n+2} = 3 \cdot a_n + 4 \cdot a_{n+1}$

$$a_0 = 0, \quad a_1 = 1$$

18. $a_{n+2} = 2 \cdot a_n + 3 \cdot a_{n+1}$

$$a_0 = 2, \quad a_1 = 1$$

19. $a_{n+2} = 4 \cdot a_n + 1 \cdot a_{n+1}$

$$a_0 = 2, \quad a_1 = 1$$

20. $a_{n+2} = 3 \cdot a_n + 2 \cdot a_{n+1}$

$$a_0 = 0, \quad a_1 = 0$$

21. $a_{n+2} = 4 \cdot a_n + 1 \cdot a_{n+1}$

$$a_0 = 0, \quad a_1 = 3$$

22. $a_{n+2} = 2 \cdot a_n + 4 \cdot a_{n+1}$

$$a_0 = 1, \quad a_1 = 0$$

3.3.2 Solutions

$$\text{1. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

$$\text{2. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 4 \\ 2 \end{pmatrix}$$

$$\text{3. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}^n \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

$$\text{4. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 4 & 3 \end{pmatrix}^n \cdot \begin{pmatrix} 4 \\ 2 \end{pmatrix}$$

$$\text{5. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

$$\text{6. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 3 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

$$\text{7. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 4 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

$$\text{8. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 4 \end{pmatrix}$$

$$\text{9. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 3 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

$$\text{10. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 3 & 3 \end{pmatrix}^n \cdot \begin{pmatrix} 3 \\ 4 \end{pmatrix}$$

$$\text{11. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 4 & 4 \end{pmatrix}^n \cdot \begin{pmatrix} 0 \\ 4 \end{pmatrix}$$

$$\text{12. } a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^n \cdot \begin{pmatrix} 3 \\ 4 \end{pmatrix}$$

$$\text{13. } a_n = \begin{pmatrix} 2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\text{14. } a_n = \begin{pmatrix} 2 & 2 \end{pmatrix} \begin{pmatrix} 0 & 4 \\ 1 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\text{15. } a_n = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 0 & 3 \\ 1 & 3 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\text{16. } a_n = \begin{pmatrix} 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\text{17. } a_n = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 3 \\ 1 & 4 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\text{18. } a_n = \begin{pmatrix} 2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\mathbf{19.} \quad a_n = \begin{pmatrix} 2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 4 \\ 1 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\mathbf{20.} \quad a_n = \begin{pmatrix} 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\mathbf{21.} \quad a_n = \begin{pmatrix} 0 & 3 \end{pmatrix} \begin{pmatrix} 0 & 4 \\ 1 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\mathbf{22.} \quad a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 4 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Matrices for Digraphs

3.4

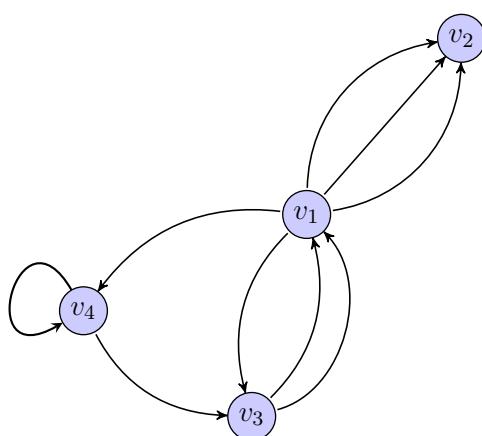
3.4.1 Adjacency Matrices	251
3.4.2 Incidence Matrices	256
3.4.3 Stochastic Matrices	259
3.4.4 Exercises	263
3.4.5 Solutions	267

Questions to Guide Your Study:

- *What is a digraph and what is an adjacency matrix?*
- *How do you build the adjacency matrix for a digraph?*
- *What do the powers of the adjacency matrix tell you?*
- *What is an incidence matrix and what does it tell you?*
- *How do you build the incidence matrix?*

3.4.1 Adjacency Matrices

Consider the following network of vertices and *directed edges* (arrows):



We call such a network a *directed graph* otherwise known as a *digraph*.

Directed Graph

A directed graph (also called a *digraph*) is a collection of vertices and edges. Each edge is an arrow with one vertex at its tail and one vertex at its tip.

Path Counting Question

How many distinct paths of length n (i.e. consisting of n arrows (directed edges)) start from some point in a specified collection of vertices and land at each vertex?

We will think of vertices as being *linearly independent vectors*. A collection of vertices then can be thought of as a sum. For instance, $\{v_1, v_3\}$ can be described as $v_1 + v_3$. Let $v_1 + v_3$ be a *starting collection* that we take our paths from.

Let's consider how many paths there are of length 2 that start somewhere in this collection and land at vertex 1. Considering the directed graph drawn above, we can tabulate what we see as follows:

Length 2 Paths				
	Paths ending at v_1	Paths ending at v_2	Paths ending at v_3	Paths ending at v_4
Paths out of v_1	2	0	1	1
Paths out of v_3	0	6	2	2

Notice that the number of paths that start at v_3 and end at v_2 is found by seeing that for each of the two distinct arrows from v_3 to v_1 , there are three distinct arrows from v_1 to v_3 . Hence there are $2 \cdot 3 = 6$ distinct paths from v_3 to v_2 . Also notice that there is one path of length 2 from v_1 to v_4 made up of traversing the edge from v_1 to v_4 and then going around the loop from v_4 to v_4 . Now to answer our question, we simply add the rows of the table:

Length 2 Paths				
	Paths ending at v_1	Paths ending at v_2	Paths ending at v_3	Paths ending at v_4
Paths out of $\{v_1, v_3\}$	2	6	3	3

In fact, this *adding* of results matches *adding* or rather *gathering more* vertices to the starting collection. Hence, answering the path counting question is an *additive function* from collections to results. Even if we do not know if our question is scalable—or if scaling vertices does not make sense at first, using a matrix map between vector spaces *still is additive and still answers our original question when we input vertex collections*. We can still use a matrix to answer an additive question!

We let

$$V = \mathbb{R} \cdot v_1 + \mathbb{R} \cdot v_2 + \mathbb{R} \cdot v_3 + \mathbb{R} \cdot v_4 = \langle v_1, v_2, v_3, v_4 \rangle$$

represent the \mathbb{R} -span of the vertices thought of as linearly independent vectors. That is, V is the vector space spanned by the vertices which make up a basis for it. In fact, notationally, we can think of these vertices as being represented as standard basis coordinate tuples:

Vertices as Standard Basis Vectors

Vertex	Vector Representation
v_1	$(1, 0, 0, 0)$
v_2	$(0, 1, 0, 0)$
v_3	$(0, 0, 1, 0)$
v_4	$(0, 0, 0, 1)$

Now, we can pose the function that answers our path counting question as a matrix function $V \rightarrow V$ where we think: $V = \mathbb{R}^4$. We use a **row** interpretation:

$$\begin{array}{c} v_1 \xrightarrow{\quad} \left(\begin{array}{cccc} 2 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 6 & 2 & 2 \\ 2 & 0 & 1 & 1 \end{array} \right) \\ v_2 \xrightarrow{\quad} \\ v_3 \xrightarrow{\quad} \\ v_4 \xrightarrow{\quad} \end{array}$$

Each row answers the question if the starting collection is just a single vertex. For instance, the first row $\begin{pmatrix} 2 & 0 & 1 & 1 \end{pmatrix}$ tells us how many paths of length 2 go from v_1 and end at each of the other vertices. So, there are 2 paths of length 2 from v_1 to v_1 , no paths of length 2 from v_1 to v_2 , 1 path of length 2 from v_1 to v_3 and 1 path of length 2 from v_1 to v_4 .

Using this matrix, we can answer our question that we posed earlier via a matrix multiplication. That is, let's look at all the paths of length 2 that come from $\{v_1, v_3\}$ which can be thought of as

$$v_1 + v_3 = (1, 0, 0, 0) + (0, 0, 1, 0) = (1, 0, 1, 0) :$$

$$\begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 6 & 2 & 2 \\ 2 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 6 & 3 & 3 \end{pmatrix}$$

which is precisely what we saw before.

Additive Questions via Matrices

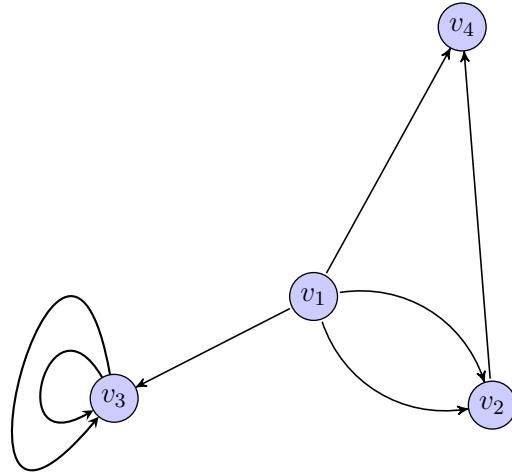
Questions are sometimes like functions. They may have an input parameter (like a collection of vertices on a directed graph) and then they have an output: *the solution*. If such a function is *additive only*, it may be answered via a *matrix function* since these answer questions which are *either* additive or scalable or *both*. Extending the domain and codomain of our question to a vector space may yield questions and answers that had no interpretation in our *original context*. But still, *additive questions are solved via matrices and matrix multiplication!*

Adjacency Matrix

An adjacency matrix for a directed graph is the matrix under a row interpretation that describes how to answer the path counting question when path length $n = 1$. That is, we are just counting single-arrow-length paths.



Example 1. Let's find the adjacency matrix for the following digraph:



Here it is:

$$\begin{pmatrix} 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

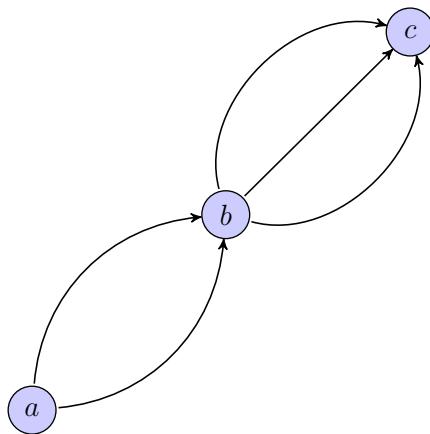
The first row tells us where all of the arrows point that come out of v_1 . The second row tells us where all of the arrows point that come out of v_2 and so forth.

The fact that the adjacency matrix represents a *scalable* function is actually useful if we compose the function with itself! If 2 paths arrive at a vertex b from a vertex a , we want to multiply 2 to the number of paths that come out of vertex b and arrive at vertex c to find how many length 2 routes there are from a to c through b . That is, *if we rescale the input, it rescales the output!*

So in the following diagram, there are

$$\underbrace{2}_{\text{input paths}} \cdot \underbrace{3}_{\text{output paths}} = 6$$

routes of length 2 from a to b :



This idea can be generalized to saying that the function which answers the path counting question for paths of length n is simply given by

$$f^{(n)} = \underbrace{f \circ f \circ f \circ \cdots \circ f}_{n \text{ times}}$$

if f solves the path counting question for paths of length 1. In fact, the function $f^{(n)}$ is given by

$$A^n = \underbrace{A \cdot A \cdot A \cdots A}_{n \text{ times}}$$

where A is the adjacency matrix of the digraph.

Adjacency Matrix Powers

The matrix that answers the path counting question for paths of length n is given by A^n where A is the adjacency matrix of the digraph.

Example 2. Suppose that A is the adjacency matrix in the last example. We compute A^2 :

$$A^2 = \begin{pmatrix} 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

This tells us that there is exactly 2 paths of length 2 that go from v_3 to v_3 , exactly 2 paths of length 2 that go from v_1 to v_3 and exactly 2 paths of length 2 that go from v_1 to v_4 . There are no other paths of length 2.

Example 3. Again, if A is the adjacency matrix from the last two examples,

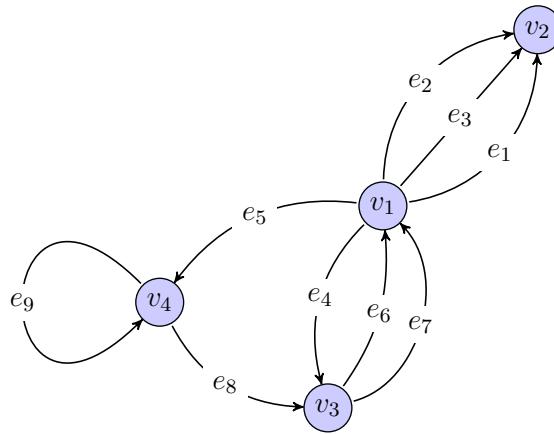
$$A^3 = \begin{pmatrix} 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

so that there are exactly 8 paths of length 3 from v_1 to v_3 and 16 from v_3 to v_3 . There are no other paths of length 3.

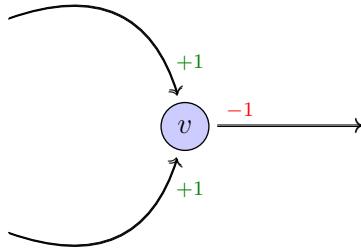
3.4.2 Incidence Matrices



Now we consider another digraph question that a linear transformation answers. Consider the following digraph where we have labeled the edges:



Think of each vertex in the digraph as a container. Each arrow signifies flow in or out of the container. We assume that the rate of flow is the same for each arrow. Suppose that around a vertex v we have two arrows in and one out:



We say that the total net flow or the *net edge incidence* at v is $+1 + 1 - 1 = +1$

Incidence

The incidence at a vertex in a digraph is the number of arrow tips subtract the number of arrow tails that touch it.

Vertex Touching Question

Given a collection of directed edges, what is the incidence on all the vertices due to *just these edges*?

This time, we think of *edges as being linearly independent vectors*. The \mathbb{R} -span of the edges makes up a vector space E . In our case, there are 9 edges. Thinking of the edge e_i as the standard basis vector e_i , we can think of E as being \mathbb{R}^9 . We can think of a collection of vertices like $\{e_1, e_2, e_5\}$ as a sum $e_1 + e_2 + e_5 \in E$.

There are 4 vertices which we can again think of as linearly independent vectors. We let V be the vector space formed as the \mathbb{R} -span of the vertices (as vectors). We think $V = \mathbb{R}^4$ just as we did in the previous section.

Our vertex touching question then has an input from $E = \mathbb{R}^9$ and the answer output is a tuple of incidence values—one for each vertex. These outputs then can be thought of as living in $V = \mathbb{R}^4$. This question is an *additive* question: gathering more edges just adds incidences together. Hence, we can use a linear transformation $f : E \rightarrow V$ to describe how to answer the vertex touching question.

We build the matrix for this function according to a column interpretation. We put the image of e_1 as the first column, the image of e_2 as the second column, etc. Each edge has a tip and a tail. The vertex at the tip gets a $+1$ and the vertex at a tail gets -1 . The single vertex on the loop e_9 gets a $+1$ and -1 at the vertex v_4 . This is a total net incidence of 0 at v_4 . There are *at most* two vertices that actually get an incidence value output for each input edge. Here is the (oriented) incidence matrix in this case:

$$\begin{matrix} & \begin{matrix} -1 & -1 & -1 & -1 & -1 & 1 & 1 & 0 & 0 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} & \left(\begin{array}{ccccccccc} -1 & -1 & -1 & -1 & -1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \end{array} \right) \end{matrix}$$

$\uparrow e_1 \quad \uparrow e_2 \quad \uparrow e_3 \quad \uparrow e_4 \quad \uparrow e_5 \quad \uparrow e_6 \quad \uparrow e_7 \quad \uparrow e_8 \quad \uparrow e_9$

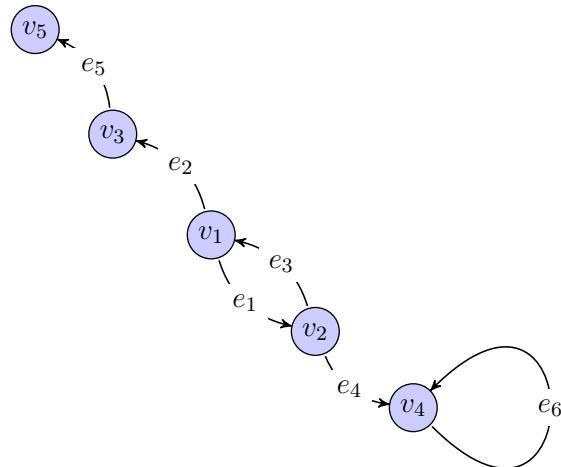
Oriented Incidence Matrix

Given a digraph with n vertices and m edges, the (oriented) incidence matrix is the $n \times m$ matrix whose columns are indexed by the edges in the following way. Each column has n entries each of which is indexed by the vertices. The column indexed by the edge that starts at vertex v_i and ends at vertex v_j has -1 in position i and a 1 in position j . All other entries of this column are 0 . If $V = \mathbb{R}^n$ and $E = \mathbb{R}^m$, then the incidence matrix describes a linear transformation $f : E \rightarrow V$ given by:

$$\begin{pmatrix} f(e_1) & f(e_2) & \cdots & f(e_m) \end{pmatrix}$$

where $f(e_i)$ describes the incidence values at each vertex from the edge e_i .

Example 4. Consider the following digraph:



The (oriented) incidence matrix is:

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

After we discuss Smith normal form of a matrix, we will see how the *quotient* vector space $V/f(E)$ actually gives us valuable information about the digraph itself.

3.4.3 Stochastic Matrices

What if we were to attach weights to an adjacency matrix—even in a probabilistic way? Perhaps we have:

$$A = \begin{pmatrix} .2 & .8 \\ .7 & .3 \end{pmatrix}$$

Reading the top row as destinations from v_1 , we could say that there is a 20% chance that flow out from v_1 will go back to v_1 and a 80% chance that it will go to v_2 . Reading the bottom row we could say that there is a 70% chance that flow out from v_2 will go to v_1 and a 30% chance that it will go back to v_2 . This type of matrix has a special name.

Right Stochastic Matrix

A right stochastic matrix is one in which each row has positive probabilities that all add to 1.

Likewise we could have a *left stochastic matrix*.

Left Stochastic Matrix

A left stochastic matrix is one in which each column has positive probabilities that all add to 1.

Example 5. Notice that

$$\begin{pmatrix} .2 & .8 \\ .7 & .3 \end{pmatrix}$$

is right stochastic but not left stochastic.

Theorem 3.4.1

Let A and B be two right stochastic matrices. Then AB is also a right stochastic matrix.

Proof. This is left as an exercise. Think of the case

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

Think about the row interpretation of matrix multiplication. The top row will be $a(e \ f) + b(g \ h)$ so that

adding all of the entries of the top row of the product is the same as adding

$$a(e + f) + b(g + h)$$

Can you see why this sum will be 1? □

Example 6. Notice that

$$A^2 = \begin{pmatrix} .2 & .8 \\ .7 & .3 \end{pmatrix}^2 = \begin{pmatrix} 0.6 & 0.4 \\ 0.35 & 0.65 \end{pmatrix}$$

so that the product of our right stochastic matrix with itself is again right stochastic.

Interpretation of Stochastic Multiplication

The first row of our example

$$A^2 = \begin{pmatrix} .2 & .8 \\ .7 & .3 \end{pmatrix}^2 = \begin{pmatrix} 0.6 & 0.4 \\ 0.35 & 0.65 \end{pmatrix}$$

tells us the probability that outflow from v_1 will come back to v_1 after 2 edges of travel is 60% and the probability that it will land at v_2 after two edges of travel is 40%. The second row tells us that the probability of outflow from v_2 will go to v_2 after 2 edges of travel is 35% and the probability that it will come back to v_2 after two edges of travel is 65%.

Notice that the sum of the first column is less than the sum of the second column. You can test this for higher A^n to see that this pattern persists. Hence v_2 is more likely to be linked to than v_1 . Therefore, v_2 should have preference if we were trying to rank vertices based upon “link flow.”

Understanding what happens to A^n as $n \rightarrow \infty$ is important idea used for ranking webpages on the internet for a search engine. In chapter 7 we will discuss techniques for quickly determining high powers of matrices.

Key Concepts from this Section

- **digraph:** (page 252) Another name for a directed graph. See directed graph.
- **directed graph:** (page 252) A directed graph (also called a *digraph*) is a collection of vertices and edges. Each edge is an arrow with one vertex at its tail and one vertex at its tip.

- **path counting question:** (page 252) How many distinct paths of length n (i.e. consisting of n arrows (directed edges)) start from some point in a specified collection of vertices and land at each vertex?
- **additive questions via matrices:** (page 253) Questions are sometimes like functions. They may have an input parameter (like a collection of vertices on a directed graph) and then they have an output: *the solution*. If such a function is *additive only*, it may be answered via a *matrix function* since these answer questions which are *either* additive or scalable or *both*. Extending the domain and codomain of our question to a vector space may yield questions and answers that had no interpretation in our *original context*. But still, *additive questions are solved via matrices and matrix multiplication!*
- **adjacency matrix:** (page 254) An adjacency matrix for a directed graph is the matrix under a row interpretation that describes how to answer the path counting question when path length $n = 1$. That is, we are just counting single-arrow-length paths.
- **adjacency matrix powers:** (page 255) The matrix that answers the path counting question for paths of length n is given by A^n where A is the adjacency matrix of the digraph.
- **incidence:** (page 257) The incidence at a vertex in a digraph is the number of arrow tips subtract the number of arrow tails that touch it.
- **vertex touching question:** (page 257) Given a collection of directed edges, what is the incidence on all the vertices due to *just these edges*?

- **oriented incidence matrix:** (page 258) Given a digraph with n vertices and m edges, the (oriented) incidence matrix is the $n \times m$ matrix whose columns are indexed by the edges in the following way. Each column has n entries each of which is indexed by the vertices. The column indexed by the edge that starts at vertex v_i and ends at vertex v_j has -1 in position i and a 1 in position j . All other entries of this column are 0 . If $V = \mathbb{R}^n$ and $E = \mathbb{R}^m$, then the incidence matrix describes a linear transformation $f : E \rightarrow V$ given by:

$$\begin{pmatrix} f(e_1) & f(e_2) & \cdots & f(e_m) \end{pmatrix}$$

where $f(e_i)$ describes the incidence values at each vertex from the edge e_i .

- **right stochastic matrix:** (page 259) A right stochastic matrix is one in which each row has positive probabilities that all add to 1 .
- **left stochastic matrix:** (page 259) A left stochastic matrix is one in which each column has positive probabilities that all add to 1 .
- **theorem 3.4.1 :** (page 259) Let A and B be two right stochastic matrices. Then AB is also a right stochastic matrix.

- **interpretation of stochastic multiplication:** (page 260) The first row of our example

$$A^2 = \begin{pmatrix} .2 & .8 \\ .7 & .3 \end{pmatrix}^2 = \begin{pmatrix} 0.6 & 0.4 \\ 0.35 & 0.65 \end{pmatrix}$$

tells us the probability that outflow from v_1 will come back to v_1 after 2 edges of travel is 60% and the probability that it will land at v_2 after two edges of travel is 40%. The second row tells us that the probability of outflow from v_2 will go to v_2 after 2 edges of travel is 35% and the probability that it will come back to v_2 after two edges of travel is 65%.

3.4.4 Exercises

Practice with Digraphs

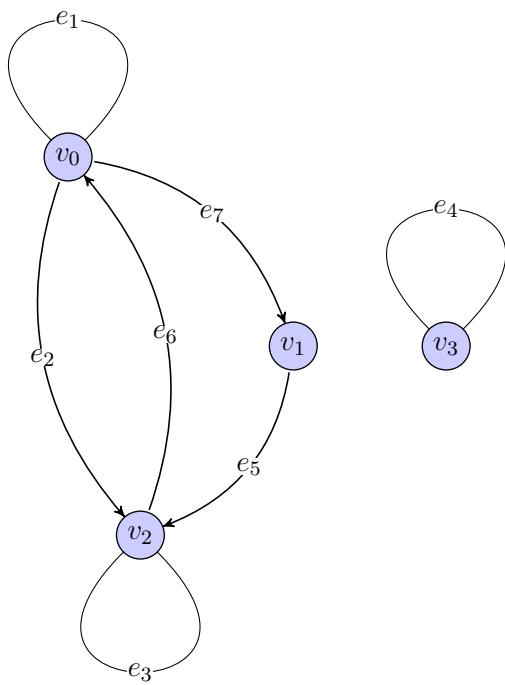
For each of the following:

(a) Find the adjacency matrix.

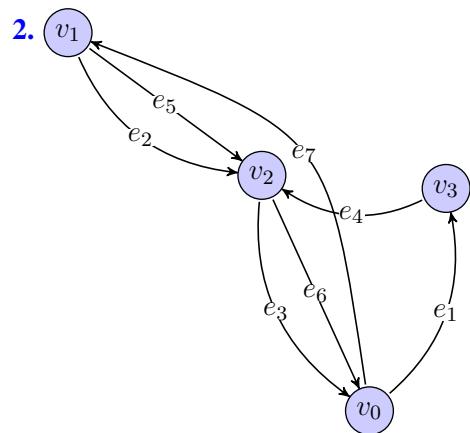
(b) Find the incidence matrix.

(c) Find how many paths of length 2 there are from v_1 to v_2 by using a power of the adjacency matrix.

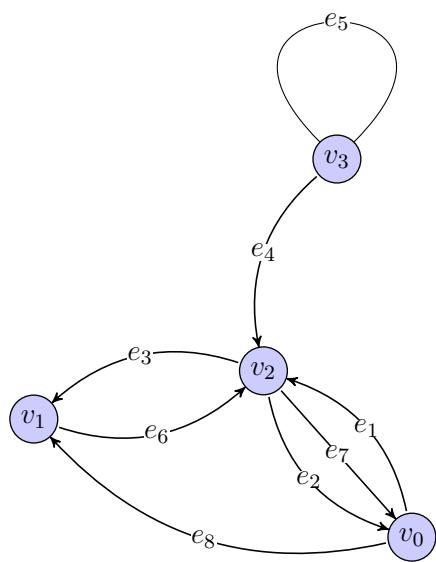
1.



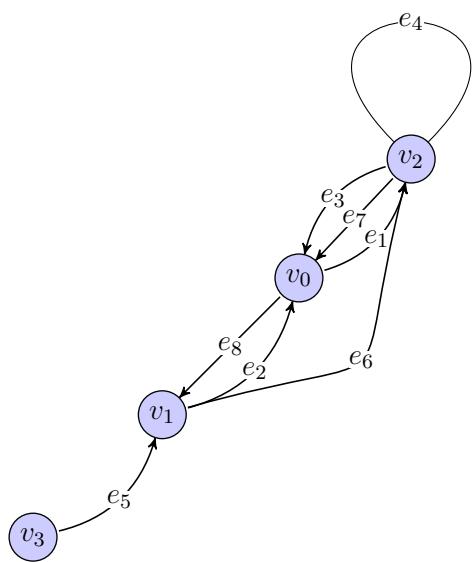
2.



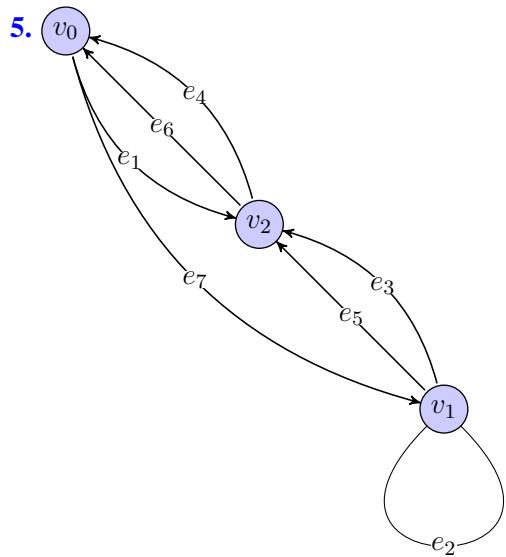
3.



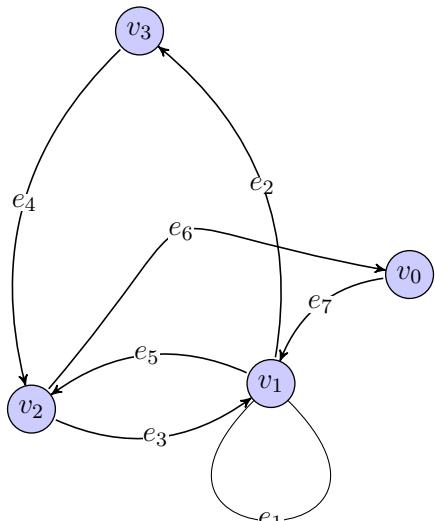
4.



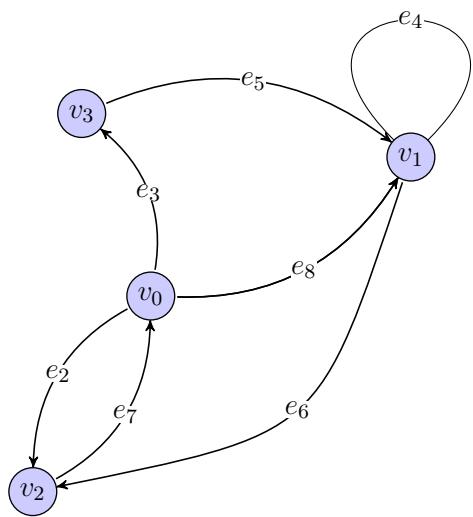
5.



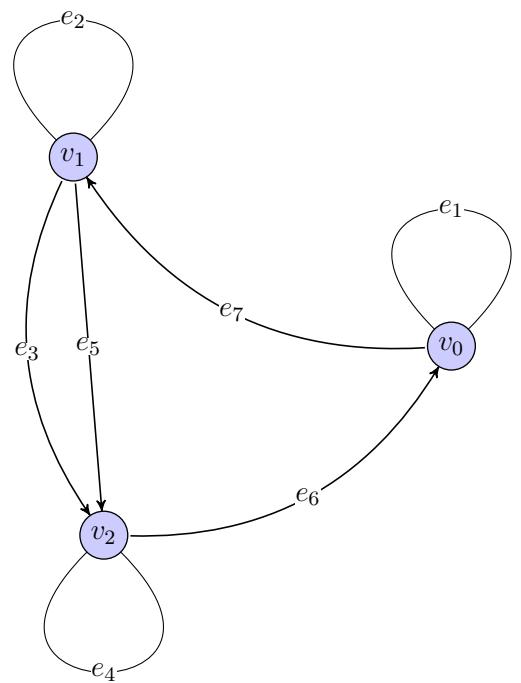
6.



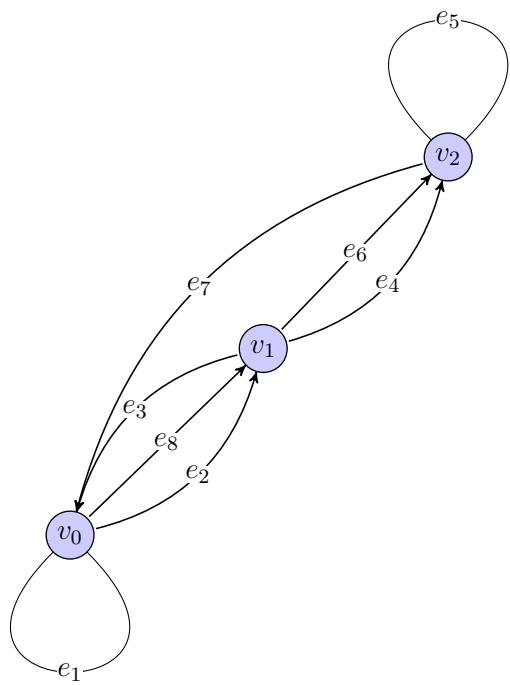
7.



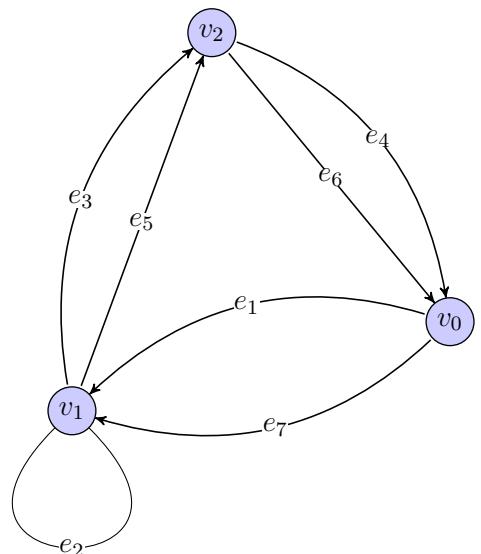
8.



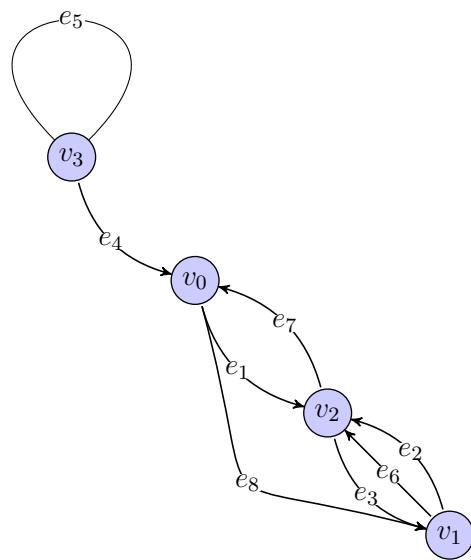
9.



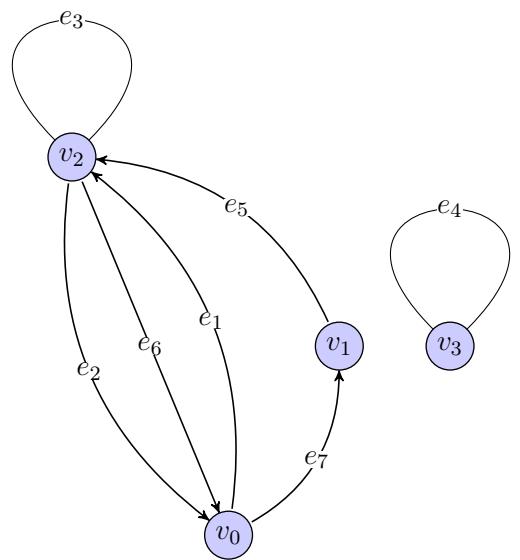
10.



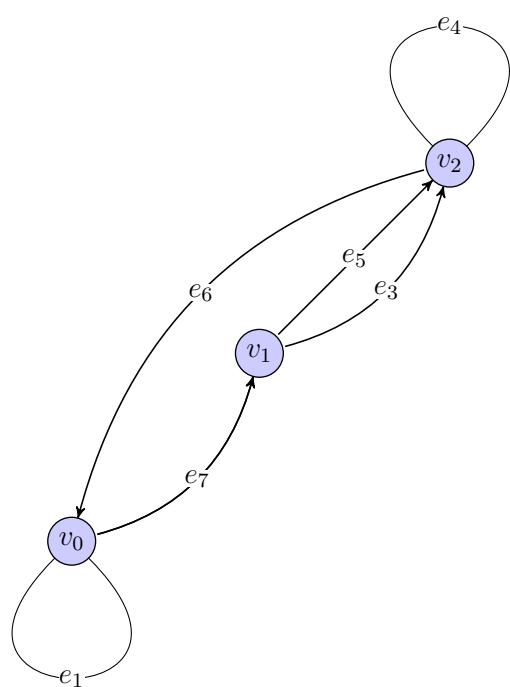
11.



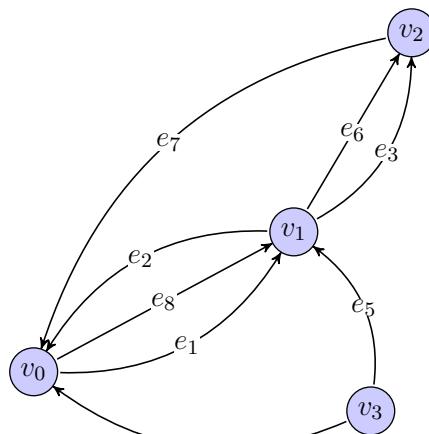
12.



13.



14.



Proof Practice

15. Let A and B be two 2×2 right stochastic matrices. Then prove that AB is also a stochastic matrix. Follow the hint given for this theorem in the reading.

3.4.5 Solutions

1.

(a)
$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(c) 1 path

2.

(a)
$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} -1 & 0 & 1 & 0 & 0 & 1 & -1 \\ 0 & -1 & 0 & 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 1 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix}$$

(c) 0 paths

3.

(a)
$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & 1 \\ 1 & -1 & -1 & 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(c) 0 paths

4.

(a)
$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} -1 & 1 & 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & -1 & 0 & 0 & 1 & -1 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix}$$

(c) 2 paths

5.

(a)
$$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 2 \\ 2 & 0 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} -1 & 0 & 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & -1 & 0 & -1 & 0 & 1 \\ 1 & 0 & 1 & -1 & 1 & -1 & 0 \end{pmatrix}$$

(c) 2 paths

6.

(a)
$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & -1 & 1 & 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 & 1 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 \end{pmatrix}$$

(c) 2 paths

7.

(a)
$$\begin{pmatrix} 0 & 2 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} -1 & -1 & -1 & 0 & 0 & 1 & -1 \\ 1 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 \end{pmatrix}$$

(c) 1 path

8.

(a)
$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & -1 & 0 \end{pmatrix}$$

(c) 4 paths

9.

(a)
$$\begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ 1 & 0 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & 1 & -1 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & -1 & 0 \end{pmatrix}$$

(c) 2 paths

10.

(a)
$$\begin{pmatrix} 0 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} -1 & 0 & 0 & 1 & 0 & 1 & -1 \\ 1 & 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & -1 & 1 & -1 & 0 \end{pmatrix}$$

(c) 2 paths

11.

(a)
$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} -1 & 0 & 0 & 1 & 0 & 0 & 1 & -1 \\ 0 & -1 & 1 & 0 & 0 & -1 & 0 & 1 \\ 1 & 1 & -1 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(c) 0 paths

12.

(a)
$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 1 & -1 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(c) 1 path

13.

$$(a) \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 1 \end{pmatrix}$$

(b)

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

(c) 2 paths

14.

$$(a) \begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

(b)

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

(c) 0 paths

15. Suppose that we have a product:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

where we know that $a + b = c + d = e + f = g + h = 1$ because the two matrices are right stochastic. Think about the row interpretation of matrix multiplication. The top row will be $a(e \ f) + b(g \ h)$ so that adding all of the entries of the top row of the product is the same as adding

$$a\underbrace{(e + f)}_{=1} + b\underbrace{(g + h)}_{=1} = a + b = 1$$

Thus the sum of the top row is one. The argument is the same with c replacing a and d replacing b for the bottom row. Hence the product is right stochastic.

Chapter 3 Selected Review Questions

Section 3.1

Can you find a matrix which describes a series of stretches, reflections, and rotations to the plane?

1. Column interpretation:

- Reflect across x axis.
- x values : Compress by a factor of 2.

2. Row interpretation:

- x and y values: Compress by a factor of 3.
- Reflect across y axis.
- Rotate by 135° .

Can you find the equation of a rotated graph?

3. Rotate by -60° :

$$x^2 + 4y^2 - 4 = 0$$

4. Rotate by $+45^\circ$:

$$x^2 + 4y^2 - 4 = 0$$

Section 3.2

Can you find the first derivative of a matrix function?

5. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

$$\begin{aligned}f(x, y, z) = \\(xyz, 4x^3z + 4xy, 2y + 4z)\end{aligned}$$

6. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$

$$f(x, y, z) = (2y, xyz)$$

Can you find the second derivative of a matrix function?

7. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^1$

$$f(x, y) = -4y^4 + 3xy$$

8. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^1$

$$f(x, y, z) = xyz$$

Section 3.3

Can you find a nonrecursive formula for a recursive sequence that involves a matrix power in a *column* interpretation?

9. $a_{n+2} = 2 \cdot a_n + 4 \cdot a_{n+1}$

$$a_0 = 3, \quad a_1 = 4$$

10. $a_{n+2} = 3 \cdot a_n + 4 \cdot a_{n+1}$

$$a_0 = 2, \quad a_1 = 3$$

Can you find a nonrecursive formula for a recursive sequence that involves a matrix power in a *row* interpretation?

11. $a_{n+2} = 4 \cdot a_n + 2 \cdot a_{n+1}$

$$a_0 = 1, \quad a_1 = 0$$

12. $a_{n+2} = 1 \cdot a_n + 4 \cdot a_{n+1}$

$$a_0 = 0, \quad a_1 = 4$$

Section 3.4

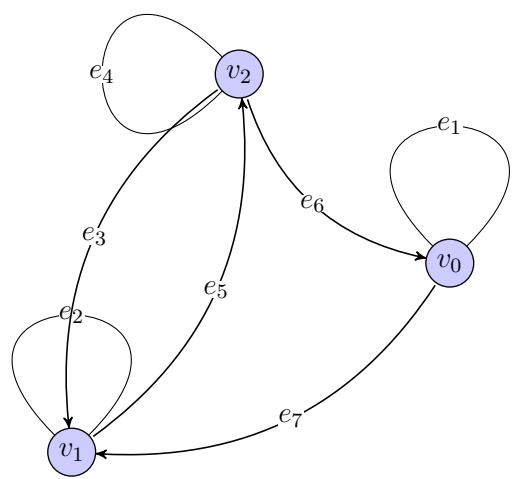
Can you find adjacency and incidence matrices and interpret what they mean?

(a) Find the adjacency matrix for a digraph.

(b) Find the (oriented) incidence matrix for a digraph.

(c) Understand what data comes from the powers of the adjacency matrix. In particular, can you find how many paths of length 3 come from vertex v_1 to v_2 by using a matrix power?

13.



Solutions/Hints

1. $\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & -1 \end{pmatrix}$

2. $\begin{pmatrix} \frac{1}{6}\sqrt{2} & -\frac{1}{6}\sqrt{2} \\ -\frac{1}{6}\sqrt{2} & -\frac{1}{6}\sqrt{2} \end{pmatrix}$

3. $(\sqrt{3}x + y)^2 + \frac{1}{4}(\sqrt{3}y - x)^2 - 4 = 0$

4. $\frac{1}{4}(\sqrt{2}x + \sqrt{2}y)^2 + (\sqrt{2}x - \sqrt{2}y)^2 - 4 = 0$

5. $\begin{pmatrix} yz & xz & xy \\ 12x^2z + 4y & 4x & 4x^3 \\ 0 & 2 & 4 \end{pmatrix}$

6. $\begin{pmatrix} 0 & 2 & 0 \\ yz & xz & xy \end{pmatrix}$

7. $\begin{pmatrix} 0 & 3 \\ 3 & -48y^2 \end{pmatrix}$

8. $\begin{pmatrix} 0 & z & y \\ z & 0 & x \\ y & x & 0 \end{pmatrix}$

9. $a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 4 \end{pmatrix}^n \cdot \begin{pmatrix} 3 \\ 4 \end{pmatrix}$

10. $a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 3 & 4 \end{pmatrix}^n \cdot \begin{pmatrix} 2 \\ 3 \end{pmatrix}$

11. $a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 4 \\ 1 & 2 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

12. $a_n = \begin{pmatrix} 0 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 4 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

13.

(a) $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

(b) $\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 & 1 & -1 & 0 \end{pmatrix}$

(c) 4 paths

Smith Normal

Form

4

Isomorphic Views of Matrices

4.1

4.1.1 Isomorphisms and What They Do	276
4.1.2 Some Simple Isomorphisms	280
4.1.3 Smith Normal Form	285
4.1.4 Finding Matrices for the Row and Column Isomorphisms	292
4.1.5 Using Smith Normal Form to Check Linear Independence	297
4.1.6 Exercises	303
4.1.7 Solutions	313

Questions to Guide Your Study:

- *What are isomorphisms between vector spaces and what do they do?*
- *What are some basic kinds of isomorphisms?*
- *How are row operations like post-compositions?*
- *How are column operations like pre-compositions?*
- *What is the Smith Normal form of a matrix with entries in \mathbb{R} ?*
- *How can the Smith Normal form tell us the dimensions of the range and kernel (null space) of a matrix (thought of as a linear transformation)?*

4.1.1 Isomorphisms and What They Do

Recall that the inverse to a function $f : D \rightarrow C$ is a function $g : C \rightarrow D$ that is simultaneously both a right and a left inverse to g . This means that f and g completely and perfectly undo each other whether we run f first or g first. When a function that preserves some kind of structure has an inverse *which also preserves the same type of structure*, it has a special name. In our case, we are preserving vector space structure. Functions that preserve vector space structure are called *linear transformations* and linear transformations that have linear transformation inverses are called *isomorphisms*.

Isomorphism of Vector Spaces

A linear transformation $f : D \rightarrow C$ between vector spaces D and C is called an isomorphism if and only if it has an inverse $g : C \rightarrow D$ which is also a linear transformation. Since f and g are inverses to each other, they would both therefore be isomorphisms. Since f and g both have left and right inverses (just each other), then they are both injective and surjective—they are bijective.

Essentially, an isomorphism is nothing more than *relabeling a basis*. Suppose that v_1, v_2 , and v_3 make up a basis for a vector space V and that $f : V \rightarrow W$ is an isomorphism of vector spaces. Here is a question: *do the images $f(v_1)$, $f(v_2)$, and $f(v_3)$ make up a basis for W ?* The answer is yes—the basis perfectly transforms into another one:

Theorem 4.1.1 Isomorphisms Relabel Bases

Given an isomorphism $f : V \rightarrow W$ of vector spaces, and a basis $\{v_1, v_2, v_3, \dots, v_n\}$ of V , then $\{f(v_1), f(v_2), f(v_3), \dots, f(v_n)\}$ is a basis for W .

Proof. We definition match for what it means to be a basis. We use the definition that a basis is a linearly independent collection that spans the space. So, to show that this collection $\{f(v_1), f(v_2), f(v_3), \dots, f(v_n)\}$ is a basis for W , we first show that it is linearly independent. Suppose that $a_1f(v_1) + a_2f(v_2) + \dots + a_nf(v_n) = 0_W$ for scalars a_1, \dots, a_n . We would like to show that these scalars are all 0. We use the fact that f is a linear transformation:

$$0_W = a_1f(v_1) + a_2f(v_2) + \dots + a_nf(v_n) = f(a_1v_1 + a_2v_2 + \dots + a_nv_n).$$

Yet, because f is injective, $f^{-1}(0_W) = \{0_V\}$ so that we must have:

$$a_1v_1 + a_2v_2 + \dots + a_nv_n = 0_V$$

Yet, since $\{v_1, v_2, v_3, \dots, v_n\}$ is a linearly independent collection of vectors in V , all of the scalars a_1, \dots, a_n must be 0. Therefore, $\{f(v_1), f(v_2), f(v_3), \dots, f(v_n)\}$ is a linearly independent collection of vectors in W .

Next, we need to show that $\{f(v_1), f(v_2), f(v_3), \dots, f(v_n)\}$ spans the space. Since $\{v_1, v_2, v_3, \dots, v_n\}$ spans the domain, then $\{f(v_1), f(v_2), f(v_3), \dots, f(v_n)\}$ spans the range of f . Yet, since f is surjective, the range is all of W so that we accomplish our goal.

Hence, $\{f(v_1), f(v_2), f(v_3), \dots, f(v_n)\}$ is a basis for W . □

Corollary 4.1.2 Isomorphisms Preserve Dimension

Suppose that $f : V \rightarrow W$ is an isomorphism of vector spaces. Then $\dim(V) = \dim(W)$.

We will be discussing how isomorphisms effect certain key attributes of a matrix function. Specifically, the range and the kernel (otherwise known as the *null space*) of a matrix function:

Kernel of a Linear Transformation

The kernel of a linear transformation $f : V \rightarrow W$ is the fiber over 0. That is, $f^{-1}(0_W)$. Sometimes we denote the kernel as $\ker(f)$ —but often we also write $f^{-1}(0_W)$.

Range of a Linear Transformation

The range of a linear transformation $f : V \rightarrow W$ is the collection of images of f . We write this as $f(V)$ or as $\text{range}(f)$.

- Under the column interpretation this would be the column space (i.e. span of the columns) of the matrix for f which is denoted as $\text{col}(f)$.
- Under the row interpretation this would be the row space (i.e. span of the rows) of the matrix for f which is noted as $\text{row}(f)$.

Theorem 4.1.3 Range and Kernel are Vector Spaces

Given a linear transformation $f : V \rightarrow W$, then the range $f(V)$ and the kernel $\ker(f)$ are vector spaces.

Proof. The range $f(V)$ is simply a span of a collection of vectors in W so therefore it is a subspace of W . The kernel $\ker(f)$ is a subset of V . To show that it is a subspace of V , it suffices to show that it is closed under addition and scalar multiplication. Suppose that $v, w \in \ker(f)$. Then, $f(v+w) = f(v) + f(w) = 0_W + 0_W = 0_W$ so that $v+w \in \ker(f)$. Therefore $\ker(f)$ is closed under addition. Next, given a scalar c , and $v \in \ker(f)$, then $f(c \cdot v) = c \cdot f(v) = c \cdot 0_W = 0_W$. Therefore, $c \cdot v \in \ker(f)$. Hence, $\ker(f)$ is a subspace of V . \square

Since the range and kernel are themselves vector spaces, they carry with them a dimension. Changing a function by running an isomorphism before or after it does not change the dimension of that function's range or kernel.

Theorem 4.1.4 Isomorphisms preserve the dimensions of the kernel and the range

Suppose that in the diagram below that all the functions are linear transformation and that i and j are isomorphisms:

$$A \xrightarrow{i} B \xrightarrow{f} C \xrightarrow{j} D$$

Then, we have the following equalities:

- (a) $\dim(\text{range}(f)) = \dim(\text{range}(f \circ i)) = \dim(\text{range}(j \circ f)) = \dim(\text{range}(j \circ f \circ i))$
- (b) $\dim(\ker(f)) = \dim(\ker(f \circ i)) = \dim(\ker(j \circ f)) = \dim(\ker(j \circ f \circ i))$

In simpler words, the isomorphisms i and j do not change the dimensions of the kernel and the range for the function f .

Proof. We prove each part one at a time:

- (a) Since i is an isomorphism, $i(A) = B$ so that $\text{range}(f \circ i) = f(i(A)) = f(B) = \text{range}(f)$. The first equality $\dim(\text{range}(f)) = \dim(\text{range}(f \circ i))$ is therefore trivially true.

To show the other equalities of part (a), we consider a restriction of j . That is, a domain restriction. Let's restrict the domain of j to $f(B) \subset C$ and call the restriction r . Then, $r : f(B) \rightarrow j(f(B))$ is a bijective linear transformation since it inherits injectivity and we reduced the codomain so that it would be surjective. The inverse function of r is just a restriction of j^{-1} so it is again a linear transformation. Hence, r itself is an isomorphism.

The function r then transfers the dimension of $f(B)$ to $j(f(B))$ so that we obtain $\dim(\text{range}(f)) = \dim(\text{range}(j \circ f))$. This is enough to prove part (a)

- (b) First we show that $\ker(j \circ f) = \ker(f)$ so that $\dim(\ker(f)) = \dim(\ker(j \circ f))$ would be a simple consequence. Since j is injective, we know that $\ker(j) = 0_C$ which means that $(j \circ f)(x) = j(f(x)) = 0_D$ implies that $f(x) = 0_C$ which implies that $x \in \ker(f)$. Now if $x \in \ker(f)$, then clearly, $j(f(x)) = j(0_C) = 0_D$ since j is additive and additive functions between additive groups always send the additive identity to the additive identity. Therefore, $x \in \ker(j \circ f)$.

Notice that if we restrict the domain of i to $i^{-1}(\ker(f))$, then for similar reasons for the restriction r we considered in the proof of (a), the restriction is an isomorphism between $i^{-1}(\ker(f))$ and $\ker(f)$. If we knew that $\ker(f \circ i) = i^{-1}(\ker(f))$, then $\dim(\ker(f)) = \dim(\ker(f \circ i))$.

So, all we have left is to show that $\ker(f \circ i) = i^{-1}(\ker(f))$: Suppose that $x \in \ker(f \circ i)$. Then, $f(i(x)) = 0_C$ so that $i(x) \in \ker(f)$ which means that $x \in i^{-1}(\ker(f))$. Now if $x \in i^{-1}(\ker(f))$, then $i(x) \in \ker(f)$ so that $f(i(x)) = 0_C$ which means that $x \in \ker(f \circ i)$. This is enough to prove part (b).

□

4.1.2 Some Simple Isomorphisms

There are many applications of knowing the dimension of the kernel and range of a matrix function. But, often it is very hard to see what these dimensions are right away. Yet, if we can run isomorphisms before and after our matrix function, we can simplify our picture until we can finally see what these dimensions should be.

We have three basic types isomorphisms which we will be running before and after matrix functions. They are *airdropping*, *rescaling*, and *rearranging*:

Examples of Three Basic Isomorphisms

Suppose that we have a vector $(a, b, c, d) \in \mathbb{R}^4$. The following operations on this vector define isomorphisms $\mathbb{R}^4 \rightarrow \mathbb{R}^4$ for a scalar $k \in \mathbb{R}$:

1. **Airdropping** between vector entries:

$$(a, b, c, d) \xrightarrow{+k \cdot a} (a, b, c+k \cdot a, d)$$

with inverse:

$$(a, b, c, d) \xrightarrow{-k \cdot a} (a, b, c-k \cdot a, d)$$

2. **Rescaling** an entry (if $k \neq 0$):

$$(a, b, c, d) \xrightarrow{k \cdot b} (a, k \cdot b, c, d)$$

with inverse:

$$(a, b, c, d) \xrightarrow{\frac{1}{k} \cdot b} (a, \frac{1}{k} \cdot b, c, d)$$

3. **Rearranging** entries:

$$(a, b, c, d) \xrightarrow{c \leftrightarrow b} (c, b, a, d)$$

which in this case is its own inverse since we just swapped two entries.

Suppose that we have a matrix function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ under the *column interpretation* given by

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

Let $j : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ be an airdrop given by

$$\begin{array}{c} \text{---} 2 \cdot a \\ \downarrow \\ (a, b, c) \end{array}$$

Then, let's try to see what the matrix for $j \circ f$ would look like. We know that the columns of $j \circ f$ will simply be the images $(j \circ f)(e_1)$, $(j \circ f)(e_2)$, and $(j \circ f)(e_3)$. So, we compute as follows remembering that $f(e_1)$, $f(e_2)$, and $f(e_3)$ are simply the columns of the matrix for f :

$$\begin{array}{c} \text{---} 2 \cdot 1 \\ \downarrow \\ \bullet e_1 \mapsto f(e_1) = (1, 2, 0) \mapsto (1, 0, 1) = (j \circ f)(e_1) \end{array}$$

$$\begin{array}{c} \text{---} 2 \cdot 2 \\ \downarrow \\ \bullet e_2 \mapsto f(e_2) = (2, -1, 1) \mapsto (2, -5, 1) = (j \circ f)(e_2) \end{array}$$

$$\begin{array}{c} \text{---} 2 \cdot 1 \\ \downarrow \\ \bullet e_3 \mapsto f(e_3) = (1, 1, 1) \mapsto (1, -1, 1) = (j \circ f)(e_1) \end{array}$$

Therefore, the matrix for $(j \circ f)$ is:

$$\left(\begin{array}{ccc} 1 & 2 & 1 \\ 2 & -1 & 1 \\ 0 & 1 & 1 \end{array} \right)_{(j \circ f)(e_1) \quad (j \circ f)(e_2) \quad (j \circ f)(e_3)}$$

We could have applied the airdrop j to $f(e_1)$, $f(e_2)$, and $f(e_3)$ all at the same time just looking at them in the matrix as follows:

$$\left(\begin{array}{ccc} \text{---} 2 \cdot 1 & \text{---} 2 \cdot 2 & \text{---} 2 \cdot 1 \\ 1 & 2 & 1 \\ 2 & -1 & 1 \\ 0 & 1 & 1 \end{array} \right) \mapsto \left(\begin{array}{ccc} 1 & 2 & 1 \\ 0 & -5 & -1 \\ 0 & 1 & 1 \end{array} \right)$$

Notice that it looks like we have lifted row 1 into the air, multiplied it by -2 and then dropped it on row 2. It was a *row operation* of our matrix.

Elementary Row Operation

Simultaneously applying one of our basic isomorphisms to all of the columns of a matrix looks like we are working with whole rows of entries at a time. Hence, this is called an *elementary row operation*. Assume a column interpretation for our matrix function. Then, It is like “post-composing” our matrix function with an isomorphism. That is, we run an isomorphism after we run the matrix function. The resulting matrix is the matrix for the composition.

Now, if we instead were following a row interpretation for our matrix, everything would be flipped:

$$\left(\begin{array}{ccc} 1 & -2 & 1 \\ 2 & -1 & 1 \\ 0 & 1 & 1 \end{array} \right) \xrightarrow{\quad \begin{array}{c} -2 \cdot 1 \\ +2 \cdot 2 \\ +2 \cdot 0 \end{array}} \left(\begin{array}{ccc} 1 & 0 & 1 \\ 2 & -5 & 1 \\ 0 & 1 & 1 \end{array} \right)$$

This would look like a “column operation” isomorphism happening afterwards in the row interpretation.

Suppose that this isomorphism is represented by a matrix C in the row interpretation. Then, if our original matrix is A , the resulting matrix after the column operation would be the same as the multiplication $A \cdot C$ with C appearing on the *right*. But an isomorphism is an *isomorphism in both row and column interpretations!* We explain this in a minute!

So, when we switch back to column interpretation, multiplication by C on the right is now an isomorphism which happens before the matrix function given by A (under the column interpretation). *But what is still the same is the fact that the matrix for $A \cdot C$ was obtained by a column operation!*

Yet, this should make sense: when we rearrange, rescale or airdrop on the columns, we doing so on the images $f(e_1)$, $f(e_2)$, and $f(e_3)$. We can push these ideas to the input e_1 , e_2 , and e_3 because f is a linear transformation.

In a column interpretation of a matrix, column operations just change up the input before we run it into the function f .

Elementary Column Operation

Simultaneously applying one of our basic isomorphisms to all of the rows of a matrix looks like we are working with whole columns of entries at a time. Hence, this is called an *elementary column operation*. Assume a column interpretation for our matrix function. Then, It is like “pre-composing” our matrix function with an isomorphism. That is, we run an isomorphism before we run the matrix function. The resulting matrix is the matrix for the composition.



Example 1. *Row airdrop is a post-isomorphism.* The following row operation is simply the function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ given by $f(x, y, z) = (x, y, z - 2x)$ applied to each column vector at the same time:

$$\left(\begin{array}{cccc} 1 & 2 & 1 & 3 \\ 1 & -2 \cdot 1 & -2 \cdot 2 & -2 \cdot 1 \\ 2 & 1 & 0 & 1 \\ 1 & 1 & -1 & 0 \end{array} \right) \rightarrow \left(\begin{array}{cccc} 1 & 2 & 1 & 3 \\ 1 & 1 & 0 & 1 \\ 0 & -3 & -3 & -6 \end{array} \right)$$

We are applying the function f to the *output* of the function f given according to a column interpretation. Then, if the original matrix is described by the function g , then the one after the row operation is described by $f \circ g$. Notice that f happens *after* the function g . It is a *post-isomorphism*. To emphasize that f is an isomorphism, notice that the inverse function $f^{-1} : \mathbb{R}^3 \rightarrow \mathbb{R}^3$, given by $f(x, y, z) = (x, y, z + 2x)$, is the row operation which undoes this one:

$$\left(\begin{array}{cccc} 1 & 2 & 1 & 3 \\ 1 & +2 \cdot 1 & +2 \cdot 2 & +2 \cdot 1 \\ 0 & -3 & -3 & -6 \end{array} \right) \rightarrow \left(\begin{array}{cccc} 1 & 2 & 1 & 3 \\ 1 & 1 & 0 & 1 \\ 2 & 1 & -1 & 0 \end{array} \right)$$



Example 2. *Column airdrop is a pre-isomorphism.* The following column operation is simply the function $f : \mathbb{R}^4 \rightarrow \mathbb{R}^4$ given by $f(x, y, z, w) = (x, y, z - 2x, w)$ applied to the row vectors (which themselves live in \mathbb{R}^4).

$$\left(\begin{array}{cccc} 1 & 1 & 2 & 1 \\ 1 & -2 \cdot 1 & 1 & 1 \\ 0 & -2 \cdot 0 & 1 & 4 \\ 2 & -2 \cdot 2 & -1 & 1 \end{array} \right) \rightarrow \left(\begin{array}{cccc} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 4 \\ 2 & -1 & -1 & 1 \end{array} \right)$$

We are applying the function f to the *output* of the function f given according to a *row interpretation*. Then, if the original matrix is described by the function g , then the matrix after the row operation is described by $f \circ g$. Suppose that A is the matrix describing g given above and B is the matrix describing g both according to a *row interpretation*. Then $\underbrace{A}_g \cdot \underbrace{B}_f$ describes $f \circ g$.

But what if we want to think about A and B according to a column interpretation? Since the matrix B describes an isomorphism according to a row interpretation, it also describes an isomorphism according to a column interpretation! But in a column interpretation, the function describing B happens first in the product $A \cdot B$. Let f^* be the function that gives the column interpretation function for the matrix B , and g^* be the column interpretation function for the matrix A . Then the column interpretation function for $\underbrace{A}_{g^*} \cdot \underbrace{B}_{f^*}$ is given by $g^* \circ \underbrace{f^*}_{\text{happens first}}$.

That is, write the matrix for f according to a row interpretation. Then, write the function f^* which describes this same matrix according to a column interpretation. The function f^* is an isomorphism that happens before our original matrix thought of as a function according to a column interpretation itself. *Column operations are pre-isomorphisms.* Here is the reverse column operation:

$$\left(\begin{array}{cccc} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 4 \\ 2 & -1 & -1 & 1 \end{array} \right) \longrightarrow \left(\begin{array}{cccc} 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 4 \\ 2 & -1 & 3 & 1 \end{array} \right)$$

This gives a reverse pre-isomorphism according to a column interpretation.

Theorem 4.1.5 Isomorphisms in Row and Column Interpretation

Suppose that a matrix represents an isomorphism in one of the interpretations, then it also represents an isomorphism in the other.

Proof. Suppose that the matrix A represents an isomorphism $D \rightarrow C$ in a column interpretation. Then there is a matrix B which represents its inverse $C \rightarrow D$. Then, $A \cdot B$ represents the composition that runs the matrix function B and then the matrix function A and yields the identity function id_C . Similarly, $B \cdot A$ represents the identity function id_D . But the identity function has the same representation in both interpretations, which means that the matrices A and B represent functions that are inverses to each other in both interpretations. Therefore, A must also represent an isomorphism in the row interpretation. The argument is the same if we were to first assume that the matrix A was an isomorphism in a row interpretation. \square

The *simplest* isomorphism is the identity map itself which *preserves everything* and has the *identity matrix* associated to it:

Identity Matrix

The identity $n \times n$ matrix is the matrix that describes the identity function $\text{id} : \mathbb{R}^n \rightarrow \mathbb{R}^n$. In particular:

$$e_1 \mapsto e_1 \quad e_2 \mapsto e_2 \quad e_3 \mapsto e_3 \quad \dots \quad e_1 \mapsto e_1$$

Under *both* the row and the column interpretations, the matrix looks like:

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

Often, this matrix is notated as I or id .

4.1.3 Smith Normal Form

A matrix function which does not represent an isomorphism could take its whole domain such as \mathbb{R}^3 and squash it to a flat plain if its range has dimension 2. This same matrix function would then squash a whole line of dimension 1 down to the origin.

Or a matrix function could squash 3-space to a one-dimensional line (its range) and send a whole two-dimensional plane (its kernel) to the origin.

We would like to be able to detect such general behavior of a function quickly. But we need the proper lens through which to view the matrix. We use an *isomorphism lens*. We illustrate with an example.

Suppose that we have a matrix function f given by

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

and we would like to determine what the dimensions are of $\text{range}(f)$ and $\text{ker}(f)$. Applying elementary row and column operations to the matrix will not change these dimensions. It would be nice to be able to perform operations until it is very obvious what the dimensions are. In our observations we will remember that the dimension is often computed as the size of any linearly independent spanning set (any such set is a minimally sized spanning set).

- Finding a linearly independent spanning collection allows us to compute dimension.
- Once found, remembering that it is also a minimal spanning collection helps us remember that the dimension is unique.

We apply some elementary row and column operations. These will not change the dimensions of the range and kernel of the matrix.

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & -1 \\ 0 & -2 \cdot 1 & -2 \cdot 1 \\ 2 & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & -1 \\ 0 & -1 & 2 \\ 2 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & +1 \cdot 1 & -1 \\ 0 & -1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 \cdot 0 & -1 \cdot 1 \\ 0 & -1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & +2 \cdot 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{pmatrix}$$

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

Let's consider what the kernel, i.e. the fiber over $0_{\mathbb{R}^3}$, is of this composition of f with row and column isomorphisms determined by the matrix S . This composition given by S acts on a linear combination $x \cdot e_1 + y \cdot e_2 + z \cdot e_3$ as follows:

$$x \cdot e_1 + y \cdot e_2 + z \cdot e_3 \mapsto x \cdot e_1 + y \cdot e_2 + z \cdot 0_{\mathbb{R}^3} = x \cdot e_1 + y \cdot e_2.$$

Because e_1 and e_2 are linearly independent, the only way for this combination to be 0 is for the coefficients x and y to both be 0. Yet z can be anything. Hence: $\ker(f) = \{ (0, 0, z) : z \in \mathbb{R} \} = \langle e_3 \rangle$ which has dimension 1. Notice that $\dim(\ker(f))$ is precisely the number of 0 columns in this matrix.

Also observe that the range of the composition is the span of the columns of this matrix which is $\langle e_1, e_2 \rangle$. Therefore, $\dim(\text{range}(f))$ is precisely the number of 1's that appear in this matrix. We are using the idea that That is, we can directly just read off the dimensions of the kernel and the range of the function f directly from this simplified matrix! We have just viewed the matrix function f through *an isomorphism lens!*

Smith Normal Form (over a field)

Let A be a $m \times n$ matrix with entries in a field. By applying elementary row and column operations, when we arrive at a matrix that looks like:

$$S = \begin{pmatrix} I & 0's \\ 0's & 0's \end{pmatrix}$$

where I is the identity matrix in the upper left corner and 0's fill the rest of the matrix, then we say that S is the Smith Normal Form of a matrix.

- Under the column interpretation, the number of zero *columns* is the dimension of the kernel and the number of 1's is the dimension of the range.
- Under the row interpretation, the number of zero *rows* is the dimension of the kernel and the number of 1's is the dimension of the range.



No matter if we use a row or a column interpretation, the dimension of the range of a matrix is exactly the same! This is because the Smith normal form is the same in both interpretations and both has the same

number of 1's—and remember that the number of 1's is how we can tell the dimension of the range. Because of this sameness, the dimension of the range deserves a special name:

Rank of a Matrix

The rank of a matrix is called the dimension of the range of the matrix function. It is the same in both interpretations.

We still have a special name for the dimension of the kernel—*but we must remember that it depends on which interpretation we choose*:

Nullity of a Matrix

The nullity of a matrix is called the dimension of the kernel of the matrix function.

- In a column interpretation, this is the number of columns of zeros in the Smith normal form.
- In a row interpretation, this is the number of rows of zeros in the Smith normal form.

Smith Normal form is *always obtainable* as long as the entries of our matrix are in a field. Also, as long as we assume that dimension is a unique property of a vector space, the Smith Normal form is unique. This is clearly true since one of the equivalent notions of dimension that we have comes from being a minimal number.

Theorem 4.1.6 Uniqueness and Existence of Smith Normal Form

Given any matrix with entries in a field, there exists a unique Smith normal form.

The following is an illustration of how we can always arrive at Smith normal form:

First, get a 1 in the upper left corner. Then, airdrop from that 1 to clear the entries to the right and down.

Repeat the process starting one column to the right and one row down.

$$\text{airdrop} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & * & * \\ 0 & * & * & * \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & * & * \end{pmatrix}$$



Example 3. *Computing Smith normal form.* We compute the Smith normal form of a 3×3 matrix:

$$\begin{pmatrix} 1 & 2 & 1 \\ 0 & (-2 \cdot 1) & (-2 \cdot 2) \\ 2 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} (-2 \cdot 1) & 2 & 1 \\ 1 & (-2 \cdot 0) & 1 \\ 0 & (-2 \cdot 1) & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} (-1 \cdot 1) & & \\ 1 & 0 & 1 \\ 0 & (-1 \cdot 0) & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & (-1 \cdot 0) & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} (-1 \cdot 0) & & \\ 1 & 0 & 0 \\ 0 & (-1 \cdot 1) & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Since there are two 1's in the Smith normal form, the rank of this matrix (the dimension of the range in both interpretations) is 2. Since there is one nonzero column, in the column interpretation the nullity or dimension of the kernel is 1. Since there is one nonzero row, in the row interpretation the nullity or dimension of the kernel is also 1.



Example 4. *Computing Smith normal form.* We compute the Smith normal form of a 3×4 matrix:

$$\begin{pmatrix} 2 & -1 & 0 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 1 & 2 \\ -1 \cdot 1 & -1 \cdot 0 & -1 \cdot 1 & -1 \cdot 2 \\ 0 & 1 & 1 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 1 & 2 \\ -1 \cdot 1 & -1 \cdot 0 & -1 \cdot 1 & -1 \cdot 2 \\ 0 & 1 & 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ -2 \cdot 1 & -2 \cdot 0 & -2 \cdot 1 & -2 \cdot 2 \\ 0 & 1 & 1 & -1 \\ 2 & -1 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 1 & 2 \\ -1 \cdot 1 & -1 \cdot 0 & -1 \cdot 0 & -3 \\ 0 & 1 & 1 & -2 \\ 0 & -1 & -2 & -3 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 1 & 2 \\ -1 \cdot 1 & -1 \cdot 0 & -1 \cdot 0 & -3 \\ 0 & 1 & 1 & -2 \\ 0 & -1 & -2 & -3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 2 \\ -2 \cdot 1 & -2 \cdot 0 & -2 \cdot 0 & -1 \\ 0 & 1 & 1 & -1 \\ 0 & -1 & -2 & -3 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & -1 & -2 & -3 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & +1 \cdot 0 & +1 \cdot 1 & +1 \cdot (-1) \\ 0 & -1 & -2 & -3 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & +1 \cdot 0 & +1 \cdot 1 & +1 \cdot (-1) \\ 0 & -1 & -2 & -3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 \cdot 0 & -1 \cdot 1 & -1 \cdot 0 & -1 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & -1 & -4 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ +1 \cdot 0 & +1 \cdot 1 & +1 \cdot 0 & -4 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & -1 & -4 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ +1 \cdot 0 & +1 \cdot 1 & +1 \cdot 0 & -4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -1 \cdot 0 & -1 \cdot 0 & -1 \cdot -1 & -1 \cdot -4 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 4 \end{pmatrix}$$

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

The dimension of the range—i.e. the rank—of the matrix is 3 and the dimension of the kernel with a column interpretation is 1. With respect to a row interpretation the dimension of the kernel is 0.

So, according to a row interpretation, all nonzero fibers, which are shifts of the 0 fiber having *only the zero vector in it* have exactly one element themselves. So, the matrix in this interpretation would be injective. This matrix is not injective, however, in the column interpretation since the kernel has many elements.

In a column interpretation since both the codomain and the range is \mathbb{R}^3 , this matrix represents a surjective function. In a row interpretation, however, the range has dimension 3 in comparison with the codomain which has dimension 4. Hence, this matrix is not surjective in a row interpretation.

Determining Injectivity and Surjectivity from Smith Normal form

If the kernel has dimension 0 in an interpretation, then the matrix function in that interpretation is injective. Otherwise, it is not.

If the dimension of the range is equal to the dimension of the codomain in an interpretation, then the matrix function in that interpretation is surjective. Otherwise, it is not.

Sorting through these thoughts yields:

Theorem 4.1.7 Duality of Injectivity and Surjectivity

A matrix function is injective in one interpretation if and only if it is surjective in the other interpretation.

That is, the only way that the range dimension can equal the codomain in a *column interpretation* is for there to be no zero rows. This is the same thing as saying that the dimension of the kernel (the nullity) is 0 in a *row interpretation!*

Example 5. Consider the Smith normal form:

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

Notice that the nullity in a row interpretation is 0. The rank of the matrix (i.e. the range in both interpretations) has dimension 2. The codomain in a column interpretation has dimension 2. Hence the range is equal to the codomain in a column interpretation. Thus, the matrix function would be surjective in column interpretation. Because the kernel in a row interpretation only has one element in it—the zero vector, the matrix function would be injective in a row interpretation. *This is a great example of the duality between injectivity and surjectivity across matrix function interpretations!*

Example 6. Consider the Smith normal form:

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

Since the dimension of the kernel in a column interpretation is 0, then this matrix function is injective in a column interpretation. *This means that in a row interpretation it is surjective!*

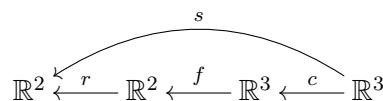
4.1.4 Finding Matrices for the Row and Column Isomorphisms



Let's consider a function $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ given under the *column interpretation* by the matrix:

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

Consider the path to Smith normal form. The row operations together make up an isomorphism r *after* our matrix function and the column operations together make up an isomorphism c *before*:



Since r and c themselves are linear transformations, they must have matrices associated with them. Here is a little though simple observation which will help us discover what those matrices are:

$$r = r \circ \text{id}_{\mathbb{R}^2}$$

The result of applying the row operations on the identity matrix is the matrix for the row operations! Indeed, $r \circ f = r \circ \text{id}_{\mathbb{R}^2} \circ f = (r \circ \text{id}_{\mathbb{R}^2}) \circ f$. But this should make sense since row operations are simply isomorphisms applied to output vectors of the matrix function—in the matrix we are running isomorphic processes on each column and each column is the image of a standard basis vector. If we run those same processes on standard basis vectors themselves, we can see where each standard basis vector travels—but is that not the information that a matrix holds itself to describe the function?

Let's consider what a row operations matrix could be for our example. Let's just run enough row operations until column operations can finish us off. *This may seem different from what we did above—but it works!*

$$\left(\begin{array}{ccc} & 1 & \\ \overset{1}{(-1 \cdot 0)} & & \\ & 1 & \\ \overset{1}{(-1 \cdot 1)} & & \\ & 1 & \\ 0 & & \\ \overset{2}{(-1 \cdot 1)} & & \\ & 1 & \end{array} \right) \longrightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Let's apply the same row operations to the identity matrix $\text{id}_{\mathbb{R}^2}$:

$$\begin{pmatrix} & 1 \\ \textcircled{-1 \cdot 0} & \textcircled{-1 \cdot 1} \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

This tells us a matrix that we could use for r :

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

In a similar way, under a *row* interpretation of multiplication,

$$c = \text{id}_{\mathbb{R}^3} \circ c.$$

Applying column operations to the identity matrix is like running isomorphic processes to the *rows* of the column matrix. The column operations, thought of as a matrix multiplication on the right are like isomorphisms that send row vectors to new row vectors. Indeed, that is just what column operations are. So to see what the column operation matrix is, just run the column operations to the identity matrix. Then, after we have the column operations matrix, *change your interpretation of multiplication back to a column interpretation* to see a function c that happens *before* f .

Continuing our example, let's find the matrix for c . So we need to know what operations we need to apply to finish off getting us to the Smith normal form for f :

$$\begin{pmatrix} & \textcircled{-1 \cdot 1} \\ 1 & 0 \\ \textcircled{-1 \cdot 0} & 1 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & \textcircled{-1 \cdot 0} \\ 0 & 0 \\ \textcircled{-1 \cdot 1} & 1 \\ 1 & 1 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Let's apply these same isomorphisms to $\text{id}_{\mathbb{R}^3}$:

$$\begin{pmatrix} & \textcircled{-1 \cdot 1} \\ 1 & 0 \\ \textcircled{-1 \cdot 0} & 1 \\ 0 & 1 \\ \textcircled{-1 \cdot 0} & 0 \\ 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & \textcircled{-1 \cdot 0} \\ 0 & -1 \\ \textcircled{-1 \cdot 1} & 0 \\ 1 & 0 \\ \textcircled{-1 \cdot 0} & 1 \\ 0 & 1 \end{pmatrix}$$

This takes us to the matrix for c :

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

We can check via matrix multiplication for $r \circ f \circ c$ if we really get the Smith normal form:

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & S \end{pmatrix}$$

In the upcoming sections, we will see that the matrices R and C can help us determine left and right inverses to functions and even help us solve systems of equations.

Row Operations Matrix

Assume a column interpretation. All of the *row* operations done on a $n \times m$ matrix A to determine its Smith normal form represent post-isomorphisms. Composing these post-isomorphisms together in the order applied yields a function. The matrix of this function is the row operations matrix R . We can find R by applying the same row operations that we do to the matrix A *in the same order* in finding its Smith normal form to a $n \times n$ identity matrix.

Column Operations Matrix

Assume a column interpretation. All of the *column* operations done on a matrix A to determine its Smith normal form represent pre-isomorphisms. Composing these pre-isomorphisms together in the opposite order applied yields a function. The matrix of this function is the column operations matrix C . We can find C by applying the same column operations that we do to the matrix A *in the same order* in finding its Smith normal form to a $m \times m$ identity matrix.

Notice that we always apply the *same operations in the same order* to an identity matrix in finding *both* the row and columns operations matrix. This actually takes care of any nuances in composing and switching interpretations.

Example 7. Finding the Row Operations Matrix We compute the row operations matrix for our work when

we found the Smith normal form in [example 4](#) for the matrix:

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

We omit all column operations that we had and *we just do the same row operations*—except we start on an identity matrix. This identity matrix is a function on the codomain (in the column interpretation) whose dimension is the number of rows of the matrix. So, we apply the row operations to a 3×3 identity matrix as follows:

$$\begin{array}{ccc} \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 0 & 0 & 1 \\ 0 & -1 \cdot 0 & -1 \cdot 0 \\ 1 & 0 & 0 \end{array} \right) \\ \left(\begin{array}{ccc} 0 & 0 & 1 \\ 0 & -2 \cdot 0 & -2 \cdot 0 \\ 1 & 0 & 0 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 0 & 0 & 1 \\ 0 & +1 \cdot 0 & +1 \cdot 1 \\ 1 & 0 & -2 \end{array} \right) \\ \left(\begin{array}{ccc} 0 & 0 & 1 \\ 0 & 1 & -1 \\ -1 \cdot 1 & -1 \cdot 1 & -1 \cdot -3 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 0 & 0 & 1 \\ 0 & 1 & -1 \\ -1 & -1 & 3 \end{array} \right) \end{array}$$

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

Example 8. *Finding the Column Operations Matrix.* Now let's find the column operations matrix for the same matrix as in the last example using the row operations from [example 4](#). Since our beginning matrix is a 3×4 matrix, maps (i.e. functions) that happen before the matrix function under a column interpretation must have codomain \mathbb{R}^4 since our matrix has domain \mathbb{R}^4 . Since, the column operations map is an isomorphism, it

must be a square matrix. Consequently, our column operations matrix will be a 4×4 matrix. We compute it by performing the same column operations that we did to get our Smith normal form on the identity 4×4 matrix as follows:

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

with annotations:
 Row 1: $(-1 \cdot 1)$
 Row 2: $(-1 \cdot 0)$
 Row 3: $(-1 \cdot 0)$
 Row 4: $(-1 \cdot 0)$

 \rightarrow

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

with annotations:
 Row 1: $(-2 \cdot 1)$
 Row 2: $(-2 \cdot 0)$
 Row 3: $(-2 \cdot 0)$
 Row 4: $(-2 \cdot 0)$

 \rightarrow

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

with annotations:
 Row 1: $(-1 \cdot 0)$
 Row 2: $(-1 \cdot 1)$
 Row 3: $(-1 \cdot 0)$
 Row 4: $(-1 \cdot 0)$

 \rightarrow

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

with annotations:
 Row 1: $(+1 \cdot 0)$
 Row 2: $(+1 \cdot 1)$
 Row 3: $(+1 \cdot 0)$
 Row 4: $(+1 \cdot 0)$

 \rightarrow

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

with annotations:
 Row 1: $(-4 \cdot (-1))$
 Row 2: $(-4 \cdot (-1))$
 Row 3: $(-4 \cdot 1)$
 Row 4: $(-4 \cdot 0)$

 \rightarrow

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

 \rightarrow

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

Example 9. Let's check to see if our row and our column operation matrices R and C that we computed actually give us the Smith normal form as desired:

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

R A C S

4.1.5 Using Smith Normal Form to Check Linear Independence

How can we tell if one vector is in the span of some vectors? That is, how can we tell if a vector lies in a plane? Or how can we tell if a collection of vectors is linearly independent—or if a collection of vectors forms a basis? All of these questions can be answered in the same way with Smith normal form *since they all deal with checking linear independence*. All we need to do is to build a matrix whose columns are these vectors. If the nullity (dimension of the kernel) in the column interpretation is 0, then the matrix represents an injective function which is enough to guarantee linear independence of the columns.

Theorem 4.1.8

To decide if a set of vectors is linearly independent, simply line up the vectors as columns in a matrix. If the nullity of this matrix (i.e. dimension of the kernel) in a column interpretation is 0, then the vectors are linearly independent. Otherwise, they are not.

Checking if a Vector is in Subspace

Suppose that V is a vector space and W is a subspace of V . Also suppose that $\{w_1, \dots, w_n\}$ is a basis for W . Then to see if v is in W , make a matrix A with columns given as:

$$A = (v \quad w_1 \quad \cdots \quad w_n)$$

If the dimension of the kernel in the column interpretation is 0, then v is not in the subspace. Otherwise, v is in the subspace.

Example 10. Consider the vector $v = (1, 2, 0, 1)$. Is it in the subspace $W = \langle (2, 1, 3, 1), (8, 7, 9, 5) \rangle$ of \mathbb{R}^4 . First, we need to be sure that the vectors $(2, 1, 3, 1)$ and $(8, 7, 9, 5)$ form a basis for W . That is, we need

to check to see if they are linearly independent. We do so by finding the following Smith normal form:

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

Very good—now let's check to see if the vector v is in the subspace by seeing if v together with the basis for W is a linearly *dependent* collection of vectors. We do this by calculating the following Smith normal form:

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

Since this matrix does not represent an injective function in a column interpretation, the columns are not linearly independent. *They are linearly dependent.* This means that v must be in the span of the other two vectors which themselves form a linearly independent collection.

Example 11. Extending the last example, suppose that we took the vector $v = (1, 0, 0, 0)$ instead:

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

Notice that now v along with the two basis vector of W form a linearly independent collection. Therefore, the vector v is not in W .

Key Concepts from this Section

- **isomorphism of vector spaces:** (page 276) A linear transformation $f : D \rightarrow C$ between vector spaces D and C is called an isomorphism if and only if it has an inverse $g : C \rightarrow D$ which is also a linear transformation. Since f and g are inverses to each other, they would both therefore be isomorphisms. Since f and g both have left and right inverses (just each other), then they are both injective and surjective—they are bijective.
- **theorem 4.1.1 isomorphisms relabel bases:** (page 277) Given an isomorphism $f : V \rightarrow W$ of vector spaces, and a basis $\{v_1, v_2, v_3, \dots, v_n\}$ of V , then $\{f(v_1), f(v_2), f(v_3), \dots, f(v_n)\}$ is a basis for W .

- **corollary 4.1.2 isomorphisms preserve dimension:** (page 277) Suppose that $f : V \rightarrow W$ is an isomorphism of vector spaces. Then $\dim(V) = \dim(W)$.
- **null space:** (page 278) Another name for the kernel of a matrix function.
- **kernel of a linear transformation:** (page 278) The kernel of a linear transformation $f : V \rightarrow W$ is the fiber over 0. That is, $f^{-1}(0_W)$. Sometimes we denote the kernel as $\ker(f)$ —but often we also write $f^{-1}(0_W)$.
- **range of a linear transformation:** (page 278) The range of a linear transformation $f : V \rightarrow W$ is the collection of images of f . We write this as $f(V)$ or as $\text{range}(f)$.
 - Under the column interpretation this would be the column space (i.e. span of the columns) of the matrix for f which is denoted as $\text{col}(f)$.
 - Under the row interpretation this would be the row space (i.e. span of the rows) of the matrix for f which is noted as $\text{row}(f)$.
- **theorem 4.1.3 range and kernel are vector spaces:** (page 278) Given a linear transformation $f : V \rightarrow W$, then the range $f(V)$ and the kernel $\ker(f)$ are vector spaces.
- **theorem 4.1.4 isomorphisms preserve the dimensions of the kernel and the range:** (page 278) Suppose that in the diagram below that all the functions are linear transformation and that i and j are isomorphisms:

$$A \xrightarrow{i} B \xrightarrow{f} C \xrightarrow{j} D$$

Then, we have the following equalities:

- $\dim(\text{range}(f)) = \dim(\text{range}(f \circ i)) = \dim(\text{range}(j \circ f)) = \dim(\text{range}(j \circ f \circ i))$
- $\dim(\ker(f)) = \dim(\ker(f \circ i)) = \dim(\ker(j \circ f)) = \dim(\ker(j \circ f \circ i))$

In simpler words, the isomorphisms i and j do not change the dimensions of the kernel and the range for the function f .

- **airdropping:** (page 280) Airdropping is the process of adding a multiple of one row to another or a multiple of one column to another in a matrix.
- **rescaling:** (page 280) Rescaling a row or a column of a matrix is an elementary row or column operation
- **rearranging:** (page 280) Rearranging the rows or columns of a matrix is a type of elementary row or column operation.
- **examples of three basic isomorphisms:** (page 280) Suppose that we have a vector $(a, b, c, d) \in \mathbb{R}^4$. The following operations on this vector define isomorphisms $\mathbb{R}^4 \rightarrow \mathbb{R}^4$ for a scalar $k \in \mathbb{R}$:

1. **Airdropping** between vector entries:

$$(a, b, c, d) \xrightarrow{+k \cdot a} (a, b, c+k \cdot a, d)$$

with inverse:

$$(a, b, c, d) \xrightarrow{-k \cdot a} (a, b, c-k \cdot a, d)$$

2. **Rescaling** an entry (if $k \neq 0$):

$$(a, b, c, d) \xrightarrow{k \cdot b} (a, (k \cdot b), c, d)$$

with inverse:

$$(a, b, c, d) \xrightarrow{\frac{1}{k} \cdot b} (a, \left(\frac{1}{k} \cdot b\right), c, d)$$

3. **Rearranging** entries:

$$(a, b, c, d) \xrightarrow{c \leftrightarrow b} (c, b, a, d)$$

which in this case is its own inverse since we just swapped two entries.

- **elementary row operation:** (page 281) Simultaneously applying one of our basic isomorphisms to all of the columns of a matrix looks like we are working with whole rows of entries at a time. Hence, this is called an *elementary row operation*. Assume a column interpretation for our matrix function. Then, It is like “post-composing” our matrix function with an isomorphism. That is, we run an isomorphism after we run the matrix function. The resulting matrix is the matrix for the composition.
- **elementary column operation:** (page 282) Simultaneously applying one of our basic isomorphisms to all of the rows of a matrix looks like we are working with whole columns of entries at a time. Hence, this is called an *elementary column operation*. Assume a column interpretation for our matrix

function. Then, It is like “pre-composing” our matrix function with an isomorphism. That is, we run an isomorphism before we run the matrix function. The resulting matrix is the matrix for the composition.

- **theorem 4.1.5 isomorphisms in row and column interpretation:** (page 284) Suppose that a matrix represents an isomorphism in one of the interpretations, then it also represents an isomorphism in the other.
- **identity matrix:** (page 284) The identity $n \times n$ matrix is the matrix that describes the identity function $\text{id} : \mathbb{R}^n \rightarrow \mathbb{R}^n$. In particular:

$$e_1 \mapsto e_1 \quad e_2 \mapsto e_2 \quad e_3 \mapsto e_3 \quad \dots \quad e_1 \mapsto e_1$$

Under *both* the row and the column interpretations, the matrix looks like:

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Often, this matrix is notated as I or id .

- **smith normal form (over a field):** (page 287) Let A be a $m \times n$ matrix with entries in a field. By applying elementary row and column operations, when we arrive at a matrix that looks like:

$$S = \begin{pmatrix} I & 0\text{'s} \\ 0\text{'s} & 0\text{'s} \end{pmatrix}$$

where I is the identity matrix in the upper left corner and 0's fill the rest of the matrix, then we say that S is the Smith Normal Form of a matrix.

- Under the column interpretation, the number of zero *columns* is the dimension of the kernel and the number of 1's is the dimension of the range.
- Under the row interpretation, the number of zero *rows* is the dimension of the kernel and the number of 1's is the dimension of the range.
- **rank of a matrix:** (page 288) The rank of a matrix is called the dimension of the range of the matrix function. It is the same in both interpretations.
- **nullity of a matrix:** (page 288) The nullity of a matrix is called the dimension of the kernel of the matrix function.
 - In a column interpretation, this is the number of columns of zeros in the Smith normal form.

- In a row interpretation, this is the number of rows of zeros in the Smith normal form.
- **theorem 4.1.6 uniqueness and existence of smith normal form:** (page 288) Given any matrix with entries in a field, there exists a unique Smith normal form.
- **determining injectivity and surjectivity from smith normal form:** (page 291) If the kernel has dimension 0 in an interpretation, then the matrix function in that interpretation is injective. Otherwise, it is not.

If the dimension of the range is equal to the dimension of the codomain in an interpretation, then the matrix function in that interpretation is surjective. Otherwise, it is not.

- **theorem 4.1.7 duality of injectivity and surjectivity:** (page 291) A matrix function is injective in one interpretation if and only if it is surjective in the other interpretation.
- **row operations matrix:** (page 294) Assume a column interpretation. All of the *row* operations done on a $n \times m$ matrix A to determine its Smith normal form represent post-isomorphisms. Composing these post-isomorphisms together in the order applied yields a function. The matrix of this function is the row operations matrix R . We can find R by applying the same row operations that we do to the matrix A *in the same order* in finding its Smith normal form to a $n \times n$ identity matrix.
- **column operations matrix:** (page 294) Assume a column interpretation. All of the *column* operations done on a matrix A to determine its Smith normal form represent pre-isomorphisms. Composing these pre-isomorphisms together in the opposite order applied yields a function. The matrix of this function is the column operations matrix C . We can find C by applying the same column operations that we do to the matrix A *in the same order* in finding its Smith normal form to a $m \times m$ identity matrix.
- **theorem 4.1.8 :** (page 297) To decide if a set of vectors is linearly independent, simply line up the vectors as columns in a matrix. If the nullity of this matrix (i.e. dimension of the kernel) in a column interpretation is 0, then the vectors are linearly independent. Otherwise, they are not.
- **checking if a vector is in subspace:** (page 297) Suppose that V is a vector space and W is a subspace of V . Also suppose that $\{w_1, \dots, w_n\}$ is a basis for W . Then to see if v is in W , make a matrix A with columns given as:

$$A = \begin{pmatrix} v & w_1 & \cdots & w_n \end{pmatrix}$$

If the dimension of the kernel in the column interpretation is 0, then v is not in the subspace. Otherwise, v is in the subspace.

4.1.6 Exercises

Find Smith Normal Form

Find the Smith normal form of each of the following:

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

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

$$3. \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

$$4. \begin{pmatrix} -2 & -1 & -1 & -2 \\ 2 & 1 & 1 & 2 \end{pmatrix}$$

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

$$6. \begin{pmatrix} 2 \\ 2 \\ -1 \\ 1 \end{pmatrix}$$

$$7. \begin{pmatrix} 1 & -2 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & -2 \\ -2 & -1 & -2 & 1 & 1 \\ 2 & -4 & 0 & 2 & -4 \\ 0 & 0 & -2 & 0 & 4 \end{pmatrix}$$

$$8. \begin{pmatrix} -2 & 0 & -1 & 0 \\ 2 & -2 & 1 & 1 \\ 0 & -2 & 0 & 1 \end{pmatrix}$$

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

$$10. \begin{pmatrix} 1 & -2 & -1 & -2 \end{pmatrix}$$

11. $\begin{pmatrix} 1 \\ 1 \\ 2 \\ 2 \\ 1 \end{pmatrix}$

12. $\begin{pmatrix} -2 \\ 4 \end{pmatrix}$

13. $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$

14. $\begin{pmatrix} -2 & 1 \\ 1 & 0 \\ -1 & 1 \end{pmatrix}$

15. $\begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix}$

16. $\begin{pmatrix} 1 & 2 \\ 1 & -2 \\ -1 & 0 \\ 4 & 0 \end{pmatrix}$

17. $\begin{pmatrix} 0 \\ -1 \\ 2 \\ -1 \end{pmatrix}$

18. $\begin{pmatrix} 2 & 1 & 2 & 0 & 2 \\ 2 & 1 & 2 & 0 & 2 \\ -2 & -1 & 0 & -2 & -2 \\ -4 & -2 & -4 & 0 & -4 \\ -4 & -4 & -4 & 2 & -2 \end{pmatrix}$

19. $\begin{pmatrix} -2 & 2 & -2 & 2 \\ -2 & 2 & -2 & 2 \\ -2 & -2 & 2 & 2 \\ -2 & -2 & 2 & 2 \end{pmatrix}$

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

Find Row and Column Operation Matrices

Find the row and column operations matrices *assuming* that you have taken the steps given to arrive at the Smith normal form. *The steps given are computer randomly generated and accomplish the intended purpose even if they may be redundant or inefficient.*

Nonetheless, write the column and row operation matrices assuming these steps!

(a) **Find the row operations matrix.**

(b) **Find the column operations matrix.**

21. add $-1 \cdot (\text{row } 1)$ to row 2

add $1 \cdot (\text{column } 1)$ to column 4

add $-2 \cdot (\text{row } 1)$ to row 2

add $1 \cdot (\text{column } 3)$ to column 4

swap columns 3 and 2

add $2 \cdot (\text{column } 4)$ to column 2

$$A = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 3 & 0 & 1 & -4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

22. add $1 \cdot (\text{row } 3)$ to row 1

swap columns 1 and 4

swap columns 2 and 1

swap columns 3 and 2

add $1 \cdot (\text{column } 4)$ to column 2

add $-1 \cdot (\text{column } 2)$ to column 4

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

23. add $-2 \cdot (\text{row } 3)$ to row 2

swap columns 2 and 1

swap rows 3 and 2

add $1 \cdot (\text{row } 4)$ to row 3

add $2 \cdot (\text{row } 2)$ to row 4

$$A = \begin{pmatrix} 0 & 1 \\ 4 & 0 \\ 1 & 0 \\ -2 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

24. add $-2 \cdot (\text{row } 3)$ to row 1

swap columns 1 and 2

add $1 \cdot (\text{column } 1)$ to column 2

add $1 \cdot (\text{row } 1)$ to row 3

add $2 \cdot (\text{row } 2)$ to row 1

$$A = \begin{pmatrix} 3 & -1 \\ 1 & 0 \\ 3 & -1 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

25. swap rows 3 and 1

swap rows 2 and 1

add $1 \cdot (\text{row } 1)$ to row 2

add $-1 \cdot (\text{column } 1)$ to column 3

swap rows 1 and 3

add $1 \cdot (\text{column } 3)$ to column 1

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

- 26.** swap columns 2 and 1
 add $-1 \cdot (\text{row } 2)$ to row 1
 swap rows 4 and 2
 add $2 \cdot (\text{row } 4)$ to row 1
 add $-1 \cdot (\text{row } 2)$ to row 3
 add $-2 \cdot (\text{column } 1)$ to column 2

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

- 27.** swap columns 1 and 2
 swap columns 2 and 4
 swap rows 1 and 2
 add $-2 \cdot (\text{column } 4)$ to column 3
 add $2 \cdot (\text{column } 2)$ to column 1
 add $-2 \cdot (\text{row } 2)$ to row 1

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

- 28.** swap columns 2 and 1
 add $-1 \cdot (\text{row } 2)$ to row 1
 swap columns 2 and 3
 swap rows 1 and 2
 add $2 \cdot (\text{column } 2)$ to column 3

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

- 29.** add $1 \cdot (\text{row } 2)$ to row 3
 add $-1 \cdot (\text{row } 3)$ to row 2
 add $-2 \cdot (\text{column } 2)$ to column 1
 swap rows 2 and 1
 swap rows 1 and 2

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

- 30.** add $-2 \cdot (\text{column } 2)$ to column 3
 swap rows 1 and 4
 add $1 \cdot (\text{column } 3)$ to column 2
 add $2 \cdot (\text{row } 2)$ to row 3
 add $-1 \cdot (\text{column } 1)$ to column 3
 add $1 \cdot (\text{row } 2)$ to row 4

$$A = \begin{pmatrix} 0 & -1 & -2 \\ 0 & 1 & 2 \\ 0 & -2 & -4 \\ 1 & -1 & -1 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

- 31.** swap columns 5 and 1
 add $-1 \cdot (\text{column 3})$ to column 1
 add $1 \cdot (\text{column 3})$ to column 5
 swap rows 1 and 3
 add $2 \cdot (\text{row 1})$ to row 2
 add $-2 \cdot (\text{column 2})$ to column 1

$$A = \begin{pmatrix} -1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

- 32.** add $-1 \cdot (\text{row 1})$ to row 2
 swap columns 2 and 1
 add $2 \cdot (\text{row 2})$ to row 1
 add $2 \cdot (\text{column 1})$ to column 2
 add $2 \cdot (\text{column 1})$ to column 2

$$A = \begin{pmatrix} -6 & 1 \\ -5 & 1 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- 33.** add $2 \cdot (\text{column 4})$ to column 1
 swap columns 3 and 2
 swap columns 4 and 3
 add $2 \cdot (\text{row 5})$ to row 4
 swap rows 1 and 4
 swap columns 2 and 4

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

- 34.** swap columns 3 and 1
 add $-1 \cdot (\text{column 1})$ to column 3
 add $-1 \cdot (\text{row 1})$ to row 2
 add $1 \cdot (\text{column 3})$ to column 2
 swap columns 3 and 2
 add $-1 \cdot (\text{row 2})$ to row 1

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

- 35.** add $-2 \cdot (\text{column 2})$ to column 4
 swap rows 1 and 3
 swap rows 2 and 3
 add $-2 \cdot (\text{column 4})$ to column 2
 swap rows 2 and 1

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

36. swap rows 5 and 1

swap columns 2 and 3

swap rows 5 and 3

swap rows 4 and 2

add $-1 \cdot (\text{column 4})$ to column 3

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

37. add $-2 \cdot (\text{row 2})$ to row 1

swap rows 2 and 1

add $-1 \cdot (\text{row 3})$ to row 1

swap rows 3 and 1

add $1 \cdot (\text{row 3})$ to row 2

$$A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

38. swap rows 1 and 4

add $-1 \cdot (\text{row 3})$ to row 4

add $1 \cdot (\text{column 2})$ to column 1

swap columns 2 and 1

add $2 \cdot (\text{column 2})$ to column 1

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

39. swap rows 4 and 3

swap columns 1 and 2

swap rows 1 and 4

add $1 \cdot (\text{column 2})$ to column 3

swap rows 5 and 4

swap rows 5 and 2

$$A = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

40. swap columns 3 and 1

add $-1 \cdot (\text{row 1})$ to row 2

swap rows 5 and 2

swap rows 2 and 4

add $1 \cdot (\text{row 1})$ to row 3

swap rows 3 and 4

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Interpreting Smith Normal Form

Suppose that you have found the Smith normal form S of your matrix A . Now is your chance to interpret what this means for your matrix A .

- (a) Find the rank of the matrix.
- (b) Find the nullity (i.e. kernel dimension) in a column interpretation.
- (c) Find the nullity (i.e. kernel dimension) in a row interpretation.
- (d) Determine whether the matrix function in a column interpretation is injective and/or surjective.
- (e) Determine whether the matrix function in a row interpretation is injective and/or surjective.

$$41. A = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & -1 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$42. A = \begin{pmatrix} 2 & 1 & 0 \\ -3 & -2 & 0 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$43. A = \begin{pmatrix} 0 & -1 \\ 0 & 1 \\ 1 & 2 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$44. A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$45. A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$46. A = \begin{pmatrix} 2 & 0 & 0 & 1 & 0 \\ 8 & 1 & 2 & 3 & 0 \\ 8 & 0 & 1 & 4 & 0 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$47. A = \begin{pmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & 2 & -1 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\mathbf{48.} A = \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\mathbf{49.} A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ -4 & 1 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\mathbf{50.} A = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$$

$$\mathbf{51.} A = \begin{pmatrix} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\mathbf{52.} A = \begin{pmatrix} 1 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\mathbf{53.} A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\mathbf{54.} A = \begin{pmatrix} 0 & 3 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 2 & 0 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathbf{55.} A = \begin{pmatrix} 1 & 0 & 1 & -1 \\ 1 & 0 & 0 & -2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathbf{56.} A = \begin{pmatrix} 1 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 \end{pmatrix}$$

$$\mathbf{57.} A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\mathbf{58.} A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$59. A = \begin{pmatrix} 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$60. A = \begin{pmatrix} -1 & 1 \\ 5 & -4 \end{pmatrix} \longrightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Checking Linear Independence: Subspace Containment

For each of the following, decide if the vector v is in the subspace W by using a Smith normal form to check for linear independence or dependence.

$$61. v = (-1, 1, 0, 0)$$

$$W = \langle (0, 2, 2, 2), (-2, 0, -2, -2) \rangle$$

$$62. v = (0, -2, 0, 1)$$

$$W = \langle (-2, -1, 0, 1), (4, 4, 0, -3) \rangle$$

$$63. v = (1, 1, -2, 2)$$

$$W = \langle (-1, -1, -2, 2), (0, 0, -1, 2) \rangle$$

$$64. v = (1, -2, -1, 0)$$

$$W = \langle (-2, -1, -1, -2), (1, 2, 0, 2) \rangle$$

$$65. v = (0, 1, 1, -1)$$

$$W = \langle (-2, -2, 1, 1), (4, 6, 0, -4) \rangle$$

$$66. v = (0, 2, -1, -2)$$

$$W = \langle (2, -2, -2, 2), (-2, 8, -1, -8) \rangle$$

$$67. v = (-1, 0, 2, 1)$$

$$W = \langle (0, -2, 2, 0), (0, 0, 0, -2) \rangle$$

$$68. v = (-1, 0, 2, -1)$$

$$W = \langle (-1, -2, 1, 2), (-2, -2, -2, 0) \rangle$$

$$69. v = (-2, -1, -1, -1)$$

$$W = \langle (-2, 1, 2, -2), (-2, 5, 8, -4) \rangle$$

$$70. v = (0, -1, -2, 2)$$

$$W = \langle (0, 0, -1, -1), (0, 1, 1, 2) \rangle$$

$$71. v = (1, -2, -1, 2)$$

$$W = \langle (0, -1, -2, 1), (-2, 1, 2, -1) \rangle$$

$$72. v = (-1, -2, -1, 2)$$

$$W = \langle (-1, 0, 1, 0), (-5, -6, -1, 6) \rangle$$

73. $v = (1, 2, 1, 0)$

$$W = \langle (2, 0, -2, -1), (5, -2, -7, -3) \rangle$$

74. $v = (-1, 0, 1, 1)$

$$W = \langle (0, 1, 1, 1), (-3, 3, 6, 6) \rangle$$

4.1.7 Solutions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21. Solutions by part:

(a) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 \\ 0 & 2 & 0 & 1 \end{pmatrix}$

22. Solutions by part:

(a) $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

(b) $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

23. Solutions by part:

$$(a) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & -2 & 1 \\ 0 & 0 & 2 & 1 \end{pmatrix}$$

$$(b) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

24. Solutions by part:

$$(a) \begin{pmatrix} 1 & 2 & -2 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{pmatrix}$$

$$(b) \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

25. Solutions by part:

$$(a) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$(b) \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

26. Solutions by part:

$$(a) \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$(b) \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$$

27. Solutions by part:

$$(a) \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}$$

$$(b) \begin{pmatrix} 0 & 0 & -2 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 \end{pmatrix}$$

28. Solutions by part:

$$(a) \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$(b) \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

29. Solutions by part:

$$(a) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$(b) \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$$

30. Solutions by part:

$$(a) \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

$$(b) \begin{pmatrix} 1 & 0 & -1 \\ 0 & -1 & -2 \\ 0 & 1 & 1 \end{pmatrix}$$

31. Solutions by part:

$$(a) \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 0 & 0 \end{pmatrix}$$

$$(b) \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ -2 & 1 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

32. Solutions by part:

$$(a) \begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix}$$

$$(b) \begin{pmatrix} 0 & 1 \\ 1 & 4 \end{pmatrix}$$

33. Solutions by part:

$$(a) \begin{pmatrix} 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$(b) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 1 & 0 \end{pmatrix}$$

34. Solutions by part:

$$(a) \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$$

$$(b) \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{pmatrix}$$

35. Solutions by part:

$$(a) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$(b) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & -2 & 0 & 1 \end{pmatrix}$$

36. Solutions by part:

$$(a) \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$(b) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}$$

37. Solutions by part:

$$(a) \begin{pmatrix} 0 & 0 & 1 \\ 1 & -1 & -1 \\ 0 & 1 & -1 \end{pmatrix}$$

$$(b) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

38. Solutions by part:

$$(a) \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

$$(b) \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix}$$

39. Solutions by part:

$$(a) \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$(b) \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

40. Solutions by part:

$$(a) \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$(b) \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

41. Solutions by part:

(a) 3

(b) 1

- (c) 1
- (d) Column interpretation: not injective, not surjective
- (e) Row Interpretation: not injective, not surjective

42. Solutions by part:

- (a) 2
- (b) 1
- (c) 0
- (d) Column interpretation: not injective, surjective
- (e) Row Interpretation: injective, not surjective

43. Solutions by part:

- (a) 2
- (b) 0
- (c) 1
- (d) Column interpretation: injective, not surjective
- (e) Row Interpretation: not injective, surjective

44. Solutions by part:

- (a) 2
- (b) 0
- (c) 2
- (d) Column interpretation: injective, not surjective
- (e) Row Interpretation: not injective, surjective

45. Solutions by part:

- (a) 1
- (b) 2

- (c) 2
- (d) Column interpretation: not injective, not surjective
- (e) Row Interpretation: not injective, not surjective

46. Solutions by part:

- (a) 3
- (b) 2
- (c) 0
- (d) Column interpretation: not injective, surjective
- (e) Row Interpretation: injective, not surjective

47. Solutions by part:

- (a) 2
- (b) 2
- (c) 0
- (d) Column interpretation: not injective, surjective
- (e) Row Interpretation: injective, not surjective

48. Solutions by part:

- (a) 2
- (b) 1
- (c) 0
- (d) Column interpretation: not injective, surjective
- (e) Row Interpretation: injective, not surjective

49. Solutions by part:

- (a) 2
- (b) 0

- (c) 1
- (d) Column interpretation: injective, not surjective
- (e) Row Interpretation: not injective, surjective

50. Solutions by part:

- (a) 1
- (b) 2
- (c) 0
- (d) Column interpretation: not injective, surjective
- (e) Row Interpretation: injective, not surjective

51. Solutions by part:

- (a) 3
- (b) 2
- (c) 0
- (d) Column interpretation: not injective, surjective
- (e) Row Interpretation: injective, not surjective

52. Solutions by part:

- (a) 1
- (b) 1
- (c) 0
- (d) Column interpretation: not injective, surjective
- (e) Row Interpretation: injective, not surjective

53. Solutions by part:

- (a) 2
- (b) 1

- (c) 0
- (d) Column interpretation: not injective, surjective
- (e) Row Interpretation: injective, not surjective

54. Solutions by part:

- (a) 2
- (b) 2
- (c) 1
- (d) Column interpretation: not injective, not surjective
- (e) Row Interpretation: not injective, not surjective

55. Solutions by part:

- (a) 3
- (b) 1
- (c) 2
- (d) Column interpretation: not injective, not surjective
- (e) Row Interpretation: not injective, not surjective

56. Solutions by part:

- (a) 1
- (b) 0
- (c) 0
- (d) Column interpretation: injective, surjective
- (e) Row Interpretation: injective, surjective

57. Solutions by part:

- (a) 1
- (b) 1

- (c) 2
- (d) Column interpretation: not injective, not surjective
- (e) Row Interpretation: not injective, not surjective

58. Solutions by part:

- (a) 3
- (b) 1
- (c) 1
- (d) Column interpretation: not injective, not surjective
- (e) Row Interpretation: not injective, not surjective

59. Solutions by part:

- (a) 3
- (b) 1
- (c) 1
- (d) Column interpretation: not injective, not surjective
- (e) Row Interpretation: not injective, not surjective

60. Solutions by part:

- (a) 2
- (b) 0
- (c) 0
- (d) Column interpretation: injective, surjective
- (e) Row Interpretation: injective, surjective

61. yes, Smith Normal Form:

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

62. yes, Smith Normal Form:

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

63. no, Smith Normal Form:

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

64. no, Smith Normal Form:

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

65. yes, Smith Normal Form:

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

66. yes, Smith Normal Form:

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

67. no, Smith Normal Form:

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

68. no, Smith Normal Form:

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

69. yes, Smith Normal Form:

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

70. no, Smith Normal Form:

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

71. no, Smith Normal Form:

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

72. yes, Smith Normal Form:

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

73. yes, Smith Normal Form:

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

74. yes, Smith Normal Form:

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

Reduced Row Echelon Form

4.2

4.2.1 Reduced Row Echelon Form and Bases	325
4.2.2 Solving Systems of Equations	331
4.2.3 Shortcut to the Kernel by Columns	336
4.2.4 Independent and Inconsistent Systems	339
4.2.5 Solving Systems with the Row Operations Matrix	341
4.2.6 Exercises	346
4.2.7 Solutions	352

Questions to Guide Your Study:

- *What is reduced row echelon form and how do you compute it?*
- *How can you use the reduced row echelon form to help solve a system of equations?*
- *How can you use column operations to help you solve a dependent system of equations?*
- *What is a fast technique to find the basis of the kernel of a linear transformation?*

4.2.1 Reduced Row Echelon Form and Bases

Every time that we perform an elementary row operation, we take a column vector and send it to another one. Often we trace the destinations of all the column vectors simultaneously. When we do this, we are changing the same corresponding entries across all of the columns. The effect? It looks like we are doing operations on the rows. But the outcome is that we are changing all of the columns by the same isomorphism.

What if we were to only perform row operations on our way to Smith Normal form? We may not actually get there—but we would get pretty close. Some of our column vectors would actually make it to standard basis vectors and some would not. Here is an example of something we might see:

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

Let's analyze what we see. In this example, there are three *pivots*. We illustrate what these are and then define them:

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

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

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

Pivot

A pivot is an “1” entry in the matrix such that:

- it appears at the corner of a rectangle made with the lower left corner of the matrix. This rectangle is all filled with zeros except for this entry “1.”
- all other entries in the column of the “1” are zeros.

$$\begin{pmatrix} * & 0's & * \\ 0's & (1) & * \\ 0's & 0's & * \end{pmatrix}$$

We search for as many pivots as we can while only doing row operations. We try to get us as close as

possible to Smith normal form and arrive at something called *reduced row echelon form*.

Reduced Row Echelon Form

The *reduced row echelon form* of a matrix is the closest to Smith normal form that we can get by only doing row operations. To be in this form, *every row* either has to:

- be filled completely with zeros
- or contain precisely one pivot.

$$\left(\begin{array}{ccccccc} : & : & : & \dots & : & : & : \\ 0 & \textcircled{1} & * & \dots & * & * & \dots \\ : & : & : & \dots & : & : & : \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots \end{array} \right)$$

Relationships between the columns of the reduced row echelon form isomorphically transfer back to the columns of the original matrix. The columns of the original matrix span the range of the matrix function under the column interpretation. In fact, the reduced row echelon form can tell us precisely what a basis is for the range of our matrix function!

Theorem 4.2.1 Basis for the Range and Reduced Row Echelon Form

The columns that map to pivot columns through row operations form a basis for the range of a matrix function under the column interpretation.

Proof. The pivot columns in the reduced row echelon form minimally span the range of the reduced row echelon form (in the column interpretation). Running the row operations (which are isomorphisms) backwards, the same linear combinations are maintained. Therefore, the columns that map to pivot columns through row operations *also* minimally span the range of the original matrix (under the column interpretation). \square

Theorem 4.2.2 Reduced Row Echelon Form is Unique

The reduced Row Echelon form of a matrix is unique.

Proof. Suppose the columns of a $m \times n$ matrix ordered from left to right are labeled as: $c_1, c_2, c_3, \dots, c_n \in \mathbb{R}^m$. A reduced row echelon form is determined by an isomorphism $r : \mathbb{R}^m \rightarrow \mathbb{R}^m$ that is a composition of row operations. The columns of the the reduced echelon form determined by r are $r(c_1), r(c_2), r(c_3), \dots, r(c_n) \in \mathbb{R}^m$. In order to follow the rules of a reduced row echelon form, we must have the following:

1. Every column of a reduced row echelon form is a linear combination of the pivoted columns (which are standard basis vectors e_i) that come before it. The pivots happen in consecutive rows from the top (i.e. going from e_1, e_2, \dots, e_k without skipping). The rows of zeros are all at the bottom. Notationally, for any index $1 \leq i \leq n$, then $\langle r(c_1), r(c_2), \dots, r(c_i) \rangle = \langle e_1, \dots, e_k \rangle$ for some index k .

2. After the first pivot, each successive pivot “1” appears one row lower than the previous one. Another way of saying this is that as we examine the columns from left to right, the *first column vector* of the reduced row echelon form which is not in the span of the pivoted columns up to that point must be a pivoted column itself. Notationally, if $r(c_{i+1})$ is not in $\langle r(c_1), r(c_2), \dots, r(c_i) \rangle = \langle e_1, \dots, e_k \rangle$, then $r(c_{i+1}) = e_{k+1}$.

Because the pivoted columns up to a point are linearly independent, the linear combinations described in (1) are uniquely determined by which pivoted columns we have used. But which pivoted columns we use are uniquely determined by (2). Let’s discuss why. Since r is an isomorphism, the statement $r(c_{i+1})$ is not in $\langle r(c_1), r(c_2), \dots, r(c_i) \rangle$ is exactly the same as the statement c_{i+1} is not in $\langle c_1, c_2, \dots, c_i \rangle$. For a given set of ordered columns $c_1, c_2, c_3, \dots, c_n$, and an index $1 \leq i \leq n$ there is one and only one yes or no answer to each of these questions. This means that there is one and only way to choose which columns will be pivoted and in which row each pivot entry “1” will occur.

In the reduced row echelon form, the entries in each column describe the unique linear combination realized by that column in terms of the pivoted columns before it. The uniqueness of the pivoted columns and the linear combinations of them, no matter what r is, ensures that there is one and only one reduced row echelon form. \square

How to Find Reduced Echelon Form

1. To start, Use row operations to put a 1 as far to the left and as high as possible.
2. Airdrop up and down from this “1” to turn it into a pivot.
3. After a pivot has been found, try to find the next one. Use row operations ***only with rows lower than any previous pivot*** to make a 1 as far to the left and high as possible, ***yet to the right and lower than any previous pivot***.
4. Airdrop up and down from this “1” to turn it into a pivot.
5. Repeat steps (3) and (4) until the reduced row echelon form is obtained.



Example 1. *Finding Spanning Columns.*

Suppose that we have the matrix

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

We will find a collection of columns that span the range of this matrix under the column interpretation by finding the reduced row echelon form of this matrix. *We only use row operations!* As soon as we get a pivot in one column, we try to get a pivot in the next column. If one is not obtainable there, we go to the next column and try there.

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} \textcircled{1} & 0 & 1 \\ 0 & \textcircled{-1 \cdot 0} & 1 \\ 0 & 1 & \textcircled{-1 \cdot 1} \end{pmatrix} \rightarrow \begin{pmatrix} \textcircled{1} & 0 & 1 \\ 0 & \textcircled{-1 \cdot 0} & 1 \\ 0 & 1 & \textcircled{-1 \cdot 1} \end{pmatrix} \rightarrow \begin{pmatrix} \textcircled{1} & 0 & 1 \\ 0 & \textcircled{1} & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Now notice the positions of the two pivot columns:

$$\text{first column: } \begin{pmatrix} \textcircled{1} \\ 0 \\ 0 \end{pmatrix}, \quad \text{second column: } \begin{pmatrix} 0 \\ \textcircled{1} \\ 0 \end{pmatrix}$$

This means that the first and second columns of the matrix A form a basis for the range:

$$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$



Example 2. *Finding Spanning Columns.*

Let's find a basis for the range of the following matrix

under the column interpretation:

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

Again, we only use row operations trying to get pivots starting at the left and working right:

$$\left(\begin{array}{ccccc} 1 & 0 & 1 & 2 & 0 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & -3 & -1 & 3 & 1 \end{array} \right) \xrightarrow{\quad} \left(\begin{array}{ccccc} 1 & 0 & 1 & 2 & 0 \\ 1 & 0 & 2 & 3 & 0 \\ 2 & -3 & -1 & 3 & 1 \end{array} \right)$$

$$\left(\begin{array}{ccccc} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 2 & -3 & -1 & 3 & 1 \end{array} \right) \xrightarrow{\quad} \left(\begin{array}{ccccc} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & -3 & -1 & 3 & 1 \end{array} \right)$$

$$\left(\begin{array}{ccccc} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & -3 & -1 & 3 & 1 \end{array} \right) \xrightarrow{\quad} \left(\begin{array}{ccccc} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & -3 & -1 & 1 & 1 \end{array} \right)$$

$$\left(\begin{array}{ccccc} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & -3 & -1 & 1 & 1 \end{array} \right) \xrightarrow{\quad} \left(\begin{array}{ccccc} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 1 \end{array} \right)$$

$$\left(\begin{array}{ccccc} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 1 \end{array} \right) \xrightarrow{\quad} \left(\begin{array}{ccccc} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{array} \right)$$

$$\left(\begin{array}{ccccc}
 1 & 0 & 1 & 2 & 0 \\
 -2 \cdot 0 & -2 \cdot 0 & -2 \cdot 0 & -2 \cdot 1 & -2 \cdot \frac{1}{2} \\
 0 & 0 & 0 & 1 & \frac{1}{2}
 \end{array} \right) \rightarrow
 \left(\begin{array}{ccccc}
 1 & 0 & 1 & 2 & -1 \\
 0 & 1 & 0 & 0 & -\frac{1}{2} \\
 0 & 0 & 0 & 1 & \frac{1}{2}
 \end{array} \right)$$

The pivots are in the first, second and fourth columns. This tells us that the first, second and fourth columns of the matrix A make up a basis for the range of A under a column interpretation:

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

4.2.2 Solving Systems of Equations



Suppose that we are given a system of equations:

$$\begin{aligned}
 6x - 6y + 6z + 8w + 22u &= 0 \\
 3x - 3y + 3z &+ 9u = 6 \\
 -x + y - z + 2w &= -3 \\
 x - y + z + 2u &= 1
 \end{aligned}$$

Solving this system is the same thing as finding a linear combination with scalars x, y, z, w , and u that looks like:

$$x \cdot \begin{pmatrix} 6 \\ 3 \\ -1 \\ 1 \end{pmatrix} + y \cdot \begin{pmatrix} -6 \\ -3 \\ 1 \\ -1 \end{pmatrix} + z \cdot \begin{pmatrix} 6 \\ 3 \\ -1 \\ 1 \end{pmatrix} + w \cdot \begin{pmatrix} 8 \\ 0 \\ 2 \\ 0 \end{pmatrix} + u \cdot \begin{pmatrix} 22 \\ 9 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 6 \\ -3 \\ 1 \end{pmatrix}$$

Let's just try to find one set of scalars that make this linear combination work. Applying the same row operation isomorphisms to each of these column vectors *will preserve this linear combination*. Remember that

isomorphisms are *reversible*. So let's isomorphically view this linear combination in the simplest setting possible to see what a possible linear combination could be. We look at the reduced row echelon form when we have lined all of these column vectors up. Let's line up the column vectors in an **augmented matrix**:

$$\left(\begin{array}{ccccc|c} 6 & -6 & 6 & 8 & 22 & 0 \\ 3 & -3 & 3 & 0 & 9 & 6 \\ -1 & 1 & -1 & 2 & 0 & -3 \\ 1 & -1 & 1 & 0 & 2 & 1 \end{array} \right)$$

Notice that the vertical line signifies the equal signs “=.” The column vector on the right is the result of the linear combination of column vectors on the left. After we perform the necessary row operations, we find that the reduced row echelon form is:

$$\left(\begin{array}{ccccc|c} 1 & -1 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

We omitted the individual steps for finding this form so that we can focus on the overall process. Now looking at this setting, it is easier to come up with a working linear combination. In particular, just assign 0 to variables that don't correspond to pivots, and the rest will be uniquely determined:

$$x \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + y \cdot \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + z \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + w \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + u \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -2 \\ 1 \\ 0 \end{pmatrix}$$

Notice that y and z do not correspond to pivots. That is, they are just scalars assigned to extra vectors that we do not need to get the full span. Just assign 0 to these:

$$x \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + w \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + u \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -2 \\ 1 \\ 0 \end{pmatrix}$$

It is then clear that $x = -1$, $y = 0$, $z = 0$, $w = -2$ and $u = 1$ are a working set of scalars by inspection. This set of scalars will work back in the original system too since the reverse isomorphisms will preserve this linear combination!

But how do we get *all* solutions to this system of equations? We do this by thinking of solving the system as being the same as finding the fiber of an additive function (even a linear transformation). The nonempty fibers of an additive function have a very nice characterization. Consider the additive function $f : \mathbb{R}^5 \rightarrow \mathbb{R}^4$ given by the matrix (under the column interpretation):

$$\begin{pmatrix} 6 & -6 & 6 & 8 & 22 \\ 3 & -3 & 3 & 0 & 9 \\ -1 & 1 & -1 & 2 & 0 \\ 1 & -1 & 1 & 0 & 2 \end{pmatrix}$$

The system of equations can be expressed as $f(x, y, z, w, u) = (0, 6, -3, 1)$ which in terms of matrix multiplication looks like:

$$\begin{pmatrix} 6 & -6 & 6 & 8 & 22 \\ 3 & -3 & 3 & 0 & 9 \\ -1 & 1 & -1 & 2 & 0 \\ 1 & -1 & 1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \\ w \\ u \end{pmatrix} = \begin{pmatrix} 0 \\ 6 \\ -3 \\ 1 \end{pmatrix}$$

The solutions to this system of equation are just the elements of the fiber $f^{-1}(0, 6, -3, 1)$. We already know that

$$(-1, 0, 0, -2, 1) \in f^{-1}(0, 6, -3, 1).$$

This is what the reduced row echelon form viewpoint did for us. But now, how do we get all solutions?

We remember that all nonempty fibers of an additive function are just additive shifts of the fiber over $0_{\mathbb{R}^4} = (0, 0, 0, 0)$ (the additive identity of the codomain). That is:

$$f^{-1}(0, 6, -3, 1) = \underbrace{(-1, 0, 0, -2, 1)}_{\text{Any element of the fiber}} + \underbrace{f^{-1}(0, 0, 0, 0)}_{\ker(f)}$$

$f^{-1}(0, 6, -3, 1)$ can be
used to shift with

Therefore, we simply need to find out what is in $f^{-1}(0, 0, 0, 0)$, add it to $(-1, 0, 0, -2, 1)$, and then we will be done.

Let's consider what is happening when we compute Smith Normal form:

$$\mathbb{R}^4 \xleftarrow{r} \mathbb{R}^4 \xleftarrow{f} \mathbb{R}^5 \xleftarrow{c} \mathbb{R}^5$$

s

where s is the function corresponding to the smith normal form, r is the row operations isomorphism which we used to get *reduced row echelon form* and c is the isomorphism corresponding to the column operations

that remain. Let's trace $0_{\mathbb{R}^4}$ back through the maps to find preimages:

$$\begin{array}{ccccc} & & s & & \\ & \swarrow r & & \searrow c & \\ 0_{\mathbb{R}^4} & \xleftarrow{f} & 0_{\mathbb{R}^4} & \xleftarrow{s^{-1}} & 0_{\mathbb{R}^5} \\ & \searrow f^{-1}(0_{\mathbb{R}^4}) & & & \end{array}$$

Notice that the column operations isomorphism c maps the kernel $\ker(s)$ onto $\ker(f)$. This means that we can compute $\ker(f)$ as $c(\ker(s))$.

To do this, let's first determine $\ker(s)$ by looking at the Smith normal form of the function f :

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

By inspection, we can see that $\ker(s) = \langle e_4, e_5 \rangle$. That is, the standard basis vectors that correspond to the zero columns span the kernel of the Smith normal form. Now, we need to compute the images of e_4 and e_5 under the column map to find a set of vectors that spans $\ker(f)$. The images of e_4 and e_5 are precisely the fourth and fifth columns of the column operations matrix. We can compute the column operations matrix easily starting right from the reduced row echelon form (just concentrating on the columns that give the map f —we do not need the augmented matrix for this):

$$\begin{array}{c} \begin{pmatrix} 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

Applying the same steps to the identity matrix $\text{id}_{\mathbb{R}^5}$ we have:

$$\begin{array}{c}
 \left(\begin{array}{ccccc}
 1 & 0 & 0 & 0 & 0 \\
 1 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 1
 \end{array} \right) \xrightarrow{\quad} \left(\begin{array}{ccccc}
 -1 & 1 & 0 & 0 & 0 \\
 1 & -1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 1
 \end{array} \right) \xrightarrow{\quad} \\
 \left(\begin{array}{ccccc}
 1 & 1 & -1 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 1
 \end{array} \right) \xrightarrow{\quad} \left(\begin{array}{ccccc}
 1 & 0 & -1 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 1 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1
 \end{array} \right) \xrightarrow{\quad} \\
 \left(\begin{array}{ccccc|cc}
 1 & 0 & 0 & 1 & -1 \\
 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 1 \\
 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0
 \end{array} \right)
 \end{array}$$

$c(e_4) \quad c(e_5)$

Therefore, all the solutions to the system of equations are given by the set:

$$f^{-1}(0, 6, -3, 1) = (-1, 0, 0, -2, 1) + \langle (1, 1, 0, 0, 0), (-1, 0, 1, 0, 0) \rangle$$

Other ways of writing this include:

$$\{(-1, 0, 0, -2, 1) + a \cdot (1, 1, 0, 0, 0) + b \cdot (-1, 0, 1, 0, 0) : a, b \in \mathbb{R}\} = \{(-1 + a + b, a, b, -2, 1) : a, b \in \mathbb{R}\}$$

$$x = -1 + a - b \quad y = a \quad z = b \quad w = -2 \quad z = 1$$

$$(-1 + y - z, y, z, -2, 1)$$

Notice that the solution depends on the values of y and z . These are two *free variables*, since they can be anything they like. We call this type of system of equations a *dependent system*.

Dependent System

A dependent system is one in which the kernel of the corresponding matrix function has dimension greater than 0. That is, the function is not injective. *The fiber we are trying to find as we solve the system is also nonempty.*

Now, we could have arrived at this last form very quickly from the reduced row echelon form:

$$\left(\begin{array}{ccccc|c} 1 & -1 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right) \longrightarrow x \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + y \cdot \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + z \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + w \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + u \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -2 \\ 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} x - y - z \\ w \\ u \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -2 \\ 1 \\ 0 \end{pmatrix} \longrightarrow \begin{matrix} x - y + z & = -1 \\ w & = -2 \\ u & = 1 \end{matrix} \longrightarrow (-1 + y - z, y, z, -2, 1)$$

Yet, the advantage of using the column operations matrix is that we can see the *basis* for the kernel and we will find this useful in later sections. It is true though, that we can still see the basis of the kernel in the solution

$$(-1 + y - z, y, z, -2, 1).$$

Just look at the free variables y and z one at a time. First, delete anything from this tuple that is not a multiple of y so that we get: $(y, y, 0, 0, 0) = y \cdot (1, 1, 0, 0, 0)$. Next, do the same for z : $(-z, 0, z, 0, 0) = z \cdot (-1, 0, 1, 0, 0)$. Now, we have our basis for our kernel as $(1, 1, 0, 0, 0)$ and $(-1, 0, 1, 0, 0)$ just as before. Really, how we move from the reduced row echelon form to the solution is a matter of style. Different methods give different insights.

4.2.3 Shortcut to the Kernel by Columns

Let's discuss another way to see the basis vectors of the kernel which shortens the column operations method. Just remember that we are starting from the reduced row echelon form which is almost in the Smith normal form. Hence, there are not many column operations to consider. But we can actually see the result of the column operations on the identity matrix quickly right in the reduced row echelon form itself!



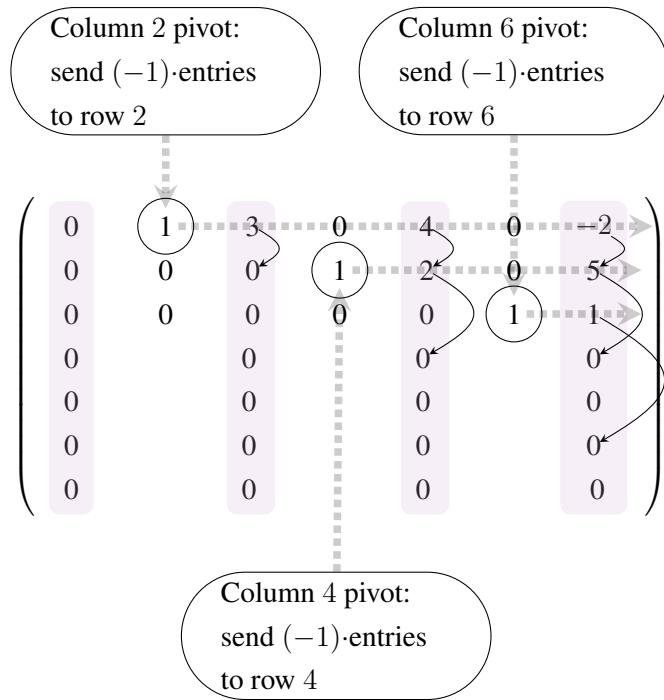
Example 3. Here is an example. Suppose that we have a reduced row echelon form of

$$\left(\begin{array}{ccccccc} 0 & 1 & 3 & 0 & 4 & 0 & -2 \\ 0 & 0 & 0 & 1 & 2 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array} \right)$$

Without switching the order of any columns, we can imagine what happens on a 7×7 identity matrix as airdropping occurs. Why 7×7 ? Because there are 7 columns. The process of imagining can be quite fast. Here are some illustrations to help:

$$\left(\begin{array}{ccccccc} 0 & \textcircled{1} & 3 & \textcircled{0} & 4 & 0 & -2 \\ 0 & 0 & 0 & \textcircled{1} & 2 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & \textcircled{1} & 1 \\ 0 & 0 & 0 & & 0 & & 0 \\ 0 & 0 & 0 & & 0 & & 0 \\ 0 & 0 & 0 & & 0 & & 0 \\ 0 & 0 & 0 & & 0 & & 0 \end{array} \right)$$

Step 2: Move the nonzero entries in these columns downward and change their sign according to the following rule: if an entry is in the same row as a pivot in column i , move $-1 \cdot$ (the entry) down to row i .



It may reduce confusion if one starts at the lower pivot and then moves to successively higher pivots.

$$\left(\begin{array}{ccccccc} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -3 & 1 & -4 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & & -2 & & -5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

Step 3: Add in the identity matrix. That is, add 1 to the entries in all diagonal positions (i, i) .

$$\left(\begin{array}{ccccccc} 0+1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0+1 & -3 & 1 & -4 & 0 & 2 \\ 0 & 0 & 0+1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & +1 & -2 & & -5 \\ 0 & 0 & 0 & 0+1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & +1 & -1 & \\ 0 & 0 & 0 & 0 & 0 & 0+1 & \end{array} \right)$$

Result: The highlighted columns have now turned into the basis for the kernel:

$$\left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & -3 & -4 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & -5 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

4.2.4 Independent and Inconsistent Systems

The easy case is when the kernel is just the zero vector. Then, we do not even need to find a basis for the kernel. The solution we come up with from the reduced row echelon form is enough. This kind of system is called *an independent system*.

Independent System

An independent system is one in which the corresponding matrix function is injective and *the fiber we are trying to find is nonempty*.

Example 4. Suppose that we have a system of equations

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

We form an augmented matrix and compute the reduced row echelon form of it:

$$\left(\begin{array}{cc|c} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 2 & 1 & 2 \end{array} \right) \rightarrow \left(\begin{array}{cc|c} \textcircled{1} & 0 & 1 \\ 0 & \textcircled{1} & 0 \\ 0 & 0 & 0 \end{array} \right)$$

Notice that there are no nonpivot columns to the left of the line. This means that the kernel is simply the zero vector. Hence, the matrix

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 2 & 1 \end{pmatrix}$$

represents an injective function f . The solution is $x = 1$ and $y = 0$. That is, $f^{-1}(1, 1, 2) = \{(1, 0)\}$. There is

only one element in this fiber. This is an *independent system*.

Now, when there ends up being no solution at all then the solution is called *inconsistent*.

Inconsistent System

An inconsistent system is one in which fiber we are trying to determine is empty.

We can determine if a system is inconsistent by seeing if there is a row in the reduced row echelon form of the augmented matrix such that to the left of the line there are zeros and to the right is something nonzero.

Example 5. Suppose that we have a system of equations

$$\begin{array}{rcl} x & = & 1 \\ x + y & = & 1 \\ y & = & 1 \end{array}$$

We form an augmented matrix and compute the reduced row echelon form of it:

$$\left(\begin{array}{cc|c} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{array} \right) \rightarrow \left(\begin{array}{cc|c} \textcircled{1} & 0 & 1 \\ 0 & \textcircled{1} & 0 \\ 0 & 0 & 1 \end{array} \right)$$

Again, the matrix

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

represents an injective function f . But there is no way to get a linear combination like:

$$a \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + b \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

Therefore, $f^{-1}(1, 1, 1) = \emptyset$. There is no solution to this system of equations. It is *inconsistent*.

4.2.5 Solving Systems with the Row Operations Matrix

Suppose that we would like to solve the two systems:

$$\begin{array}{rcl} x & +y & -z = 1 \\ x & +y & +z = 2 \\ 2x & +2y & = 3 \end{array}$$

$$\begin{array}{rcl} x & +y & -z = -3 \\ x & +y & +z = 5 \\ 2x & +2y & = 2 \end{array}$$

Notice that we are trying to find (x, y, z) so that

$$\underbrace{\begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & 1 \\ 2 & 2 & 0 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} x \\ y \\ z \end{pmatrix}}_v = b$$

where b is $(1, 2, 3)$ in the first system and $(-3, 5, 2)$ in the second system. Let R be the row operations matrix that puts A into reduced row echelon form (which then can be put into Smith normal form by column operations). Then, $Av = b$ can turn into $RAv = Rb$ where RA is the reduced row echelon form of A .

So if we find R and RA , we can reuse them again and again if we want to change b .

$$\left(\begin{array}{ccc} 1 & 1 & -1 \\ 1 & 1 & 1 \\ 2 & 2 & 0 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 1 & 1 & -1 \\ 0 & 0 & 2 \\ 2 & 2 & 0 \end{array} \right) \rightarrow$$

$$\left(\begin{array}{ccc} 1 & 1 & -1 \\ 0 & 0 & 2 \\ 0 & 0 & 2 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 1 & 1 & -1 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{array} \right) \rightarrow$$

$$\left(\begin{array}{ccc} 1 & 1 & -1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{array} \right)$$

Therefore,

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

Now, we find the row operations matrix R :

$$\begin{array}{ccc} \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 1 & 1 & -1 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) \\ \left(\begin{array}{ccc} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) \\ \left(\begin{array}{ccc} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) \\ \left(\begin{array}{ccc} 1 & 0 & 0 \\ -2 & 0 & 1 \\ 0 & 1 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 1 & 0 & 0 \\ -2 & 0 & 1 \\ 0 & 1 & 1 \end{array} \right) \\ \left(\begin{array}{ccc} 1 & 0 & 0 \\ -2 & 0 & 1 \\ 0 & 1 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 1 & 0 & 0 \\ -2 & 0 & 1 \\ 0 & 1 & 1 \end{array} \right) \\ \left(\begin{array}{ccc} 1 & 0 & 0 \\ -2 & 0 & 1 \\ 0 & 1 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 1 & 0 & 0 \\ -2 & 0 & 1 \\ 0 & 1 & 1 \end{array} \right) \end{array}$$

So,

$$R = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -1 & -1 & 1 \end{pmatrix}$$

Therefore, to solve our two systems, we compute Rb for each one:

$$\underbrace{\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -1 & -1 & 1 \end{pmatrix}}_R \cdot \underbrace{\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}}_b = \begin{pmatrix} \frac{3}{2} \\ \frac{1}{2} \\ 0 \end{pmatrix}$$

$$\underbrace{\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -1 & -1 & 1 \end{pmatrix}}_R \cdot \underbrace{\begin{pmatrix} -3 \\ 5 \\ 2 \end{pmatrix}}_b = \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix}$$

This is what we augment to the reduced row echelon form to solve the systems. For the first system:

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & \frac{3}{2} \\ 0 & 0 & 1 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \end{array} \right)$$

For the second system:

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

The kernel in both cases *is the same because it only depends on the matrix A not b which just tells us the shift!*
By the column trick, the kernel in both cases is $\langle (-1, 1, 0) \rangle$.

Then we only need the particular solution in both cases. The particular solution for the first system could be $(\frac{3}{2}, 0, \frac{1}{2})$ (i.e. just anything that works). The particular solution for the second system could be $(1, 0, 4)$. Hence,

$$\text{First System Solution: } \left(\frac{3}{2}, 0, \frac{1}{2} \right) + \langle (-1, 1, 0) \rangle \quad \text{Second System Solution: } (1, 0, 4) + \langle (-1, 1, 0) \rangle$$

Suppose that f is the function representing the column interpretation of matrix multiplication by A . Then we have just found a method for quickly computing any fiber of f .

Extra Note

Often “LU Decompositions” are taught in order to accomplish the same goal of solving multiple systems with only changing b . Yet LU decompositions are not always possible and do not save much time if any.

Example 6. Using f as the function representing the same matrix A above, let’s try to find the fiber $f^{-1}(1, 1, 1)$. We compute:

$$\underbrace{\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -1 & -1 & 1 \end{pmatrix}}_R \cdot \underbrace{\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}}_b = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$$

Therefore, we are solving:

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{array} \right)$$

The last row is interpreted as $0 = -1$ which is a false statement. Hence, this system has no solution. Therefore,

$$f^{-1}(1, 1, 1) = \emptyset$$

Key Concepts from this Section

- **pivot:** (page 326) A pivot is an “1” entry in the matrix such that:

- it appears at the corner of a rectangle made with the lower left corner of the matrix. This rectangle is all filled with zeros except for this entry “1.”
- all other entries in the column of the “1” are zeros.

$$\begin{pmatrix} * & 0's & * \\ 0's & \textcircled{1} & * \\ 0's & 0's & * \end{pmatrix}$$

- **reduced row echelon form:** (page 327) The *reduced row echelon form* of a matrix is the closest to Smith normal form that we can get by only doing row operations. To be in this form, *every row* either has to:

- be filled completely with zeros
- or contain precisely one pivot.

$$\begin{pmatrix} : & : & : & \dots & : & : & : \\ 0 & \textcircled{1} & * & \dots & * & * & \dots \\ : & : & : & \dots & : & : & : \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots \end{pmatrix}$$

- **theorem 4.2.1 basis for the range and reduced row echelon form:** (page 327) The columns that map to pivot columns through row operations form a basis for the range of a matrix function under the column interpretation.
- **theorem 4.2.2 reduced row echelon form is unique:** (page 327) The reduced Row Echelon form of a matrix is unique.
- **how to find reduced echelon form:** (page 328)

1. To start, Use row operations to put a 1 as far to the left and as high as possible.
2. Airdrop up and down from this “1” to turn it into a pivot.

3. After a pivot has been found, try to find the next one. Use row operations *only with rows lower than any previous pivot* to make a 1 as far to the left and high as possible, *yet to the right and lower than any previous pivot*.
4. Airdrop up and down from this “1” to turn it into a pivot.
5. Repeat steps (3) and (4) until the reduced row echelon form is obtained.

- **augmented matrix:** (page 332)
- **free variables:** (page 336) Variables in a solution to a system of equations that can be anything in that solution.
- **dependent system:** (page 336) A dependent system is one in which the kernel of the corresponding matrix function has dimension greater than 0. That is, the function is not injective. *The fiber we are trying to find as we solve the system is also nonempty.*
- **independent system:** (page 339) An independent system is one in which the corresponding matrix function is injective and *the fiber we are trying to find is nonempty*.
- **inconsistent system:** (page 340) An inconsistent system is one in which fiber we are trying to determine is empty.

4.2.6 Exercises

Finding a Basis for a Span

Use the reduced row echelon form to determine which columns of the following matrices serve as a basis for the range of the matrix. *Using the column interpretation of the matrix as a function.*

$$1. \begin{pmatrix} -5 & -5 & 12 \\ 2 & 2 & -4 \\ 16 & 16 & -37 \\ 3 & 3 & -6 \end{pmatrix}$$

$$2. \begin{pmatrix} 8 & 2 & 2 \\ 11 & 2 & 2 \\ -17 & -3 & -3 \end{pmatrix}$$

$$3. \begin{pmatrix} -12 & 6 & 12 \\ 2 & -1 & -2 \\ 2 & -1 & -3 \\ 0 & 0 & -1 \\ -6 & 3 & 6 \end{pmatrix}$$

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

$$5. \begin{pmatrix} 7 & 1 & -1 \\ 7 & 3 & -3 \\ -21 & -3 & 3 \\ 2 & 2 & -2 \end{pmatrix}$$

$$6. \begin{pmatrix} -3 & -1 \\ 23 & 11 \\ 3 & 1 \end{pmatrix}$$

$$7. \begin{pmatrix} 9 & 0 & 0 & 0 & 18 \\ -2 & 0 & 0 & 0 & -4 \\ -1 & 4 & 0 & 0 & 8 \\ 0 & -2 & 0 & 0 & -4 \\ 3 & 0 & 0 & 0 & 6 \end{pmatrix}$$

$$8. \begin{pmatrix} -1 & -1 & 0 \\ 4 & 4 & 0 \\ -2 & -2 & 0 \\ -2 & -2 & -1 \\ 3 & 3 & 0 \end{pmatrix}$$

$$9. \begin{pmatrix} -8 & 8 & -4 \\ 2 & -2 & 1 \\ -2 & 0 & 0 \\ 6 & -4 & 2 \end{pmatrix}$$

$$10. \begin{pmatrix} 7 & 3 \\ 12 & 6 \\ 1 & 1 \\ 4 & 3 \end{pmatrix}$$

11.
$$\begin{pmatrix} -18 & -18 & -36 \\ -9 & -9 & -18 \\ -2 & 0 & -4 \end{pmatrix}$$

12.
$$\begin{pmatrix} 1 & -2 & -1 \\ -3 & 6 & 3 \\ 2 & -6 & -2 \\ -2 & 4 & 2 \end{pmatrix}$$

13.
$$\begin{pmatrix} 2 & -2 \\ 0 & 1 \\ -6 & 7 \end{pmatrix}$$

14.
$$\begin{pmatrix} -1 & -5 \\ 0 & 3 \\ 2 & -3 \\ -1 & 1 \end{pmatrix}$$

15.
$$\begin{pmatrix} 2 & -6 \\ -1 & -1 \\ 1 & -1 \\ -1 & 3 \end{pmatrix}$$

16.
$$\begin{pmatrix} 0 & -4 & -2 \\ 2 & -10 & -5 \\ 7 & -38 & -19 \end{pmatrix}$$

17.
$$\begin{pmatrix} 0 & 6 & 0 & 3 & 6 \\ -8 & 4 & 0 & 2 & 8 \\ 16 & -2 & 0 & -1 & -18 \\ -12 & 2 & 0 & 1 & 14 \end{pmatrix}$$

18.
$$\begin{pmatrix} -1 & 0 \\ 2 & -2 \\ 1 & -2 \\ -1 & 0 \\ 1 & -2 \end{pmatrix}$$

19.
$$\begin{pmatrix} -1 & 0 & -2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 \\ 1 & 0 & 7 & 0 & 0 \\ 2 & 0 & 7 & 3 & 6 \\ -2 & 0 & -2 & 2 & 4 \end{pmatrix}$$

20.
$$\begin{pmatrix} 7 & 1 & -1 \\ 11 & 2 & -2 \end{pmatrix}$$

Dependent Systems of Equations

Solve the following systems of equations by using the reduced row echelon form *and* the column operations on the way to Smith normal form.

21.
$$\begin{array}{rcl} x & -2y & -2z & +2w = -4 \\ & & w & = -1 \\ 2x & -4y & -4z & = -4 \\ -x & +2y & +2z & = 2 \end{array}$$

22.
$$\begin{array}{rcl} x & -2y & +2z & -4w & -3t = 2 \\ & & z & -w & -t = 1 \\ & & u & -t & = -1 \end{array}$$

$$\begin{array}{rcl} \textbf{23.} & x - y + 3z = -1 \\ & y - z = 1 \\ & -x - 2z = 0 \end{array}$$

$$\begin{array}{rcl} \textbf{24.} & x - y + 2z = 0 \\ & y - 2z = 2 \\ & -x = -2 \end{array}$$

$$\begin{array}{rcl} \textbf{25.} & x - y - 4w - 3t = 2 \\ & z = 2 \\ & u = 0 \end{array}$$

$$\begin{array}{rcl} \textbf{26.} & x - 3y + 4z = -7 \\ & y - z = 2 \\ & -x - z = 1 \end{array}$$

$$\begin{array}{rcl} \textbf{27.} & x - 2y - z + 2w = -4 \\ & z - w = 2 \\ & -x + 2y - w = 2 \end{array}$$

$$\begin{array}{rcl} \textbf{28.} & x - y - 2z + 3w = 5 \\ & z - 2w = -2 \\ & -x + y + w = -1 \end{array}$$

$$\begin{array}{rcl} \textbf{29.} & x - 4z + w = 6 \\ & z = -1 \\ & -x - w = -2 \end{array}$$

$$\begin{array}{rcl} \textbf{30.} & x - y + 2z = 1 \\ & y + z = -1 \\ & -x - 3z = 0 \end{array}$$

$$\begin{array}{rcl} \textbf{31.} & x + 5z = 1 \\ & y + 2z = 0 \\ & -x - 5z = -1 \end{array}$$

$$\begin{array}{rcl} \textbf{32.} & x - 3y - 5w - t = 2 \\ & z + w + 2t = -2 \\ & u - t = -2 \end{array}$$

$$\begin{array}{rcl} \textbf{33.} & x + 2y - 5z - 6w = 10 \\ & z + w = -2 \\ & -x - 2y + w = 0 \end{array}$$

$$\begin{array}{rcl} \textbf{34.} & x - 7z - 3w - t = -14 \\ & z = 2 \\ & -x + 3w = 0 \end{array}$$

$$\begin{array}{rcl} \textbf{35.} & x + 2z - 2w - 2u = 1 \\ & y - 2z - 2w + u = -2 \\ & -2x - 4z + 4w + 4u = -2 \end{array}$$

$$\begin{array}{rcl} \textbf{36.} & x - 4z + w = 1 \\ & w = 0 \\ & 2x - 8z = 2 \\ & -x + 4z = -1 \end{array}$$

$$\begin{array}{rcl} \textbf{37.} & x - 2y + 3z + 7w = 2 \\ & y - 4w = 0 \\ & -2x - 6z + 2w = -4 \end{array}$$

$$\begin{array}{rcl} \textbf{38.} & x - y - 6z = -2 \\ & w = 2 \\ & 2x - 2y - 12z = -4 \\ & -x + y + 6z = 2 \end{array}$$

39.
$$\begin{array}{rcl} x + y - 6z - 16w & = & -1 \\ z + 2w & = & 0 \\ -x - y + 4w & = & 1 \end{array}$$

40.
$$\begin{array}{rcl} x + y + 7z & = & -2 \\ y + z & = & -2 \\ -x - 6z & = & 0 \end{array}$$

Finding Fibers

Find the indicated fiber of the function f given by the associated matrix according to the column interpretation and write your solution in set builder notation if the fiber has more than one element.

41. $f^{-1}(-1, 0, 0)$

$$\left(\begin{array}{ccccccc} 1 & 2 & 2 & 3 & 0 & 3 \\ 0 & 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{array} \right)$$

42. $f^{-1}(0, 1, 1)$

$$\left(\begin{array}{ccc} 1 & -1 & 0 \\ 0 & 1 & -2 \\ 1 & 0 & -2 \end{array} \right)$$

43. $f^{-1}(5, 2, 1)$

$$\left(\begin{array}{ccccccc} 1 & 1 & 2 & 8 & 0 & 1 \\ 0 & 0 & 1 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{array} \right)$$

44. $f^{-1}(1, -2, 1, -2)$

$$\left(\begin{array}{cccc} 1 & -1 & 2 & -1 \\ 0 & 0 & 0 & 1 \\ -1 & 1 & -2 & 0 \\ 2 & -2 & 4 & 0 \end{array} \right)$$

45. $f^{-1}(-1, 0, -1)$

$$\left(\begin{array}{ccc} 1 & -2 & 6 \\ 0 & 1 & -3 \\ 1 & 0 & 0 \end{array} \right)$$

46. $f^{-1}(0, 0, -1)$

$$\left(\begin{array}{ccccccc} 1 & 3 & 1 & 7 & 0 & 1 \\ 0 & 0 & 1 & 5 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{array} \right)$$

47. $f^{-1}(-4, -1, 2)$

$$\left(\begin{array}{ccccccc} 1 & 4 & 2 & 12 & 0 & -5 \\ 0 & 0 & 1 & 4 & 0 & -3 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{array} \right)$$

48. $f^{-1}(1, -1, 0)$

$$\left(\begin{array}{ccc} 1 & -1 & -1 \\ 0 & 1 & -1 \\ 1 & 0 & -2 \end{array} \right)$$

49. $f^{-1}(8, -2, -2, 4)$

$$\begin{pmatrix} 1 & -3 & 3 & -3 \\ 0 & 0 & 0 & 1 \\ -1 & 3 & -3 & 0 \\ 2 & -6 & 6 & 0 \end{pmatrix}$$

50. $f^{-1}(0, 1, 2)$

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

51. $f^{-1}(-1, -1)$

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

52. $f^{-1}(-2, 2, 2)$

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

53. $f^{-1}(4, -2, -1)$

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

54. $f^{-1}(1, -1, 0)$

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

55. $f^{-1}(-2, 0)$

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

56. $f^{-1}(-3, -2, 0)$

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

57. $f^{-1}(-1, -1, 2)$

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

58. $f^{-1}(-1, 2, -1)$

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 2 & 0 \end{pmatrix}$$

59. $f^{-1}(-2, 1, -1)$

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

60. $f^{-1}(0, 2, 2)$

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

61. $f^{-1}(-1, -2, -1)$

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

62. $f^{-1}(-1, 0, 1)$

$$\begin{pmatrix} 1 & 6 \\ 0 & 1 \\ 2 & 0 \end{pmatrix}$$

4.2.7 Solutions

1. r.r.e.f.

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

$$(-5, 2, 16, 3), (12, -4, -37, -6)$$

2. r.r.e.f.

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

$$(8, 11, -17), (2, 2, -3)$$

3. r.r.e.f.

$$\begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$(-12, 2, 2, 0, -6), (12, -2, -3, -1, 6)$$

4. r.r.e.f.

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

$$(3, 3, 1, 2), (-5, -6, 3, -3), (1, 0, 2, 1)$$

5. r.r.e.f.

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

$$(7, 7, -21, 2), (1, 3, -3, 2)$$

6. r.r.e.f.

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

$$(-3, 23, 3), (-1, 11, 1)$$

7. r.r.e.f.

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

$$(9, -2, -1, 0, 3), (0, 0, 4, -2, 0),$$

8. r.r.e.f.

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

$$(-1, 4, -2, -2, 3), (0, 0, 0, -1, 0)$$

$$(18, -4, 8, -4, 6)$$

9. r.r.e.f.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$(-8, 2, -2, 6), (8, -2, 0, -4)$$

10. r.r.e.f.

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

$$(7, 12, 1, 4), (3, 6, 1, 3)$$

11. r.r.e.f.

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$(-18, -9, -2), (-18, -9, 0)$$

12. r.r.e.f.

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

$$(1, -3, 2, -2), (-2, 6, -6, 4)$$

13. r.r.e.f.

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

$$(2, 0, -6), (-2, 1, 7)$$

14. r.r.e.f.

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

$$(-1, 0, 2, -1), (-5, 3, -3, 1)$$

15. r.r.e.f.

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

$$(2, -1, 1, -1), (-6, -1, -1, 3)$$

16. r.r.e.f.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \frac{1}{2} \\ 0 & 0 & 0 \end{pmatrix}$$

$$(0, 2, 7), (-4, -10, -38)$$

17. r.r.e.f.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$(0, -8, 16, -12), (6, 4, -2, 2), (6, 8, -18, 14)$$

18. r.r.e.f.

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

$$(-1, 2, 1, -1, 1), (0, -2, -2, 0, -2)$$

19. r.r.e.f.

$$\left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

$$(-1, 0, 1, 2, -2), \quad (-2, 1, 7, 7, -2), \quad (0, 1, 0, 3, 2)$$

20. r.r.e.f.

$$\left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & -1 \end{array} \right)$$

$$(7, 11), \quad (1, 2)$$

21. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & -2 & -2 & 0 & -2 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w) =$$

$$\{ (-2, 0, 0, -1) + a \cdot (2, 1, 0, 0) + b \cdot (2, 0, 1, 0) : a, b \in \mathbb{R} \}$$

22. r.r.e.f.

$$\left(\begin{array}{cccccc|c} 1 & -2 & 0 & -2 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 & -1 \end{array} \right)$$

All Solutions:

$$(x, y, z, w, u, t) =$$

$$\{ (0, 0, 1, 0, -1, 0) + a \cdot (2, 1, 0, 0, 0, 0) + b \cdot (2, 0, 1, 1, 0, 0) + c \cdot (1, 0, 1, 0, 1, 1) : a, b, c \in \mathbb{R} \}$$

23. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 2 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (0, 1, 0) + a \cdot (-2, 1, 1) : a \in \mathbb{R} \}$$

24. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & -2 & 2 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (2, 2, 0) + a \cdot (0, 2, 1) : a \in \mathbb{R} \}$$

25. r.r.e.f.

$$\left(\begin{array}{cccccc|c} 1 & -1 & 0 & -4 & 0 & -3 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w, u, t) =$$

$$\{ (2, 0, 2, 0, 0, 0) + a \cdot (1, 1, 0, 0, 0, 0) + b \cdot (4, 0, 0, 1, 0, 0) + c \cdot (3, 0, 0, 0, 0, 1) : a, b, c \in \mathbb{R} \}$$

26. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (-1, 2, 0) + a \cdot (-1, 1, 1) : a \in \mathbb{R} \}$$

27. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & -2 & 0 & 1 & -2 \\ 0 & 0 & 1 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w) =$$

$$\{ (-2, 0, 2, 0) + a \cdot (2, 1, 0, 0) + b \cdot (-1, 0, 1, 1) : a, b \in \mathbb{R} \}$$

28. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & -1 & 0 & -1 & 1 \\ 0 & 0 & 1 & -2 & -2 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w) =$$

$$\{ (1, 0, -2, 0) + a \cdot (1, 1, 0, 0) + b \cdot (1, 0, 2, 1) : a, b \in \mathbb{R} \}$$

29. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w) =$$

$$\{ (2, 0, -1, 0) + a \cdot (0, 1, 0, 0) + b \cdot (-1, 0, 0, 1) : a, b \in \mathbb{R} \}$$

30. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 3 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (0, -1, 0) + a \cdot (-3, -1, 1) : a \in \mathbb{R} \}$$

31. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 5 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (1, 0, 0) + a \cdot (-5, -2, 1) : a \in \mathbb{R} \}$$

32. r.r.e.f.

$$\left(\begin{array}{ccccccc|c} 1 & -3 & 0 & -5 & 0 & -1 & 2 \\ 0 & 0 & 1 & 1 & 0 & 2 & -2 \\ 0 & 0 & 0 & 0 & 1 & -1 & -2 \end{array} \right)$$

All Solutions:

$$(x, y, z, w, u, t) =$$

$$\{ (2, 0, -2, 0, -2, 0) + a \cdot (3, 1, 0, 0, 0, 0) + b \cdot (5, 0, -1, 1, 0, 0) + c \cdot (1, 0, -2, 0, 1, 1) : a, b, c \in \mathbb{R} \}$$

33. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & 2 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w) =$$

$$\{ (0, 0, -2, 0) + a \cdot (-2, 1, 0, 0) + b \cdot (1, 0, -1, 1) : a, b \in \mathbb{R} \}$$

34. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & -3 & 0 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w) =$$

$$\{ (0, 0, 2, 0) + a \cdot (0, 1, 0, 0) + b \cdot (3, 0, 0, 1) : a, b \in \mathbb{R} \}$$

35. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & 0 & 2 & -2 & -2 & 1 \\ 0 & 1 & -2 & -2 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w, u) =$$

$$\{ (1, -2, 0, 0, 0) + a \cdot (-2, 2, 1, 0, 0) + b \cdot (2, 2, 0, 1, 0) + c \cdot (2, -1, 0, 0, 1) : a, b, c \in \mathbb{R} \}$$

36. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & 0 & -4 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w) =$$

$$\{ (1, 0, 0, 0) + a \cdot (0, 1, 0, 0) + b \cdot (4, 0, 1, 0) : a, b \in \mathbb{R} \}$$

37. r.r.e.f.

$$\left(\begin{array}{ccccc|c} 1 & 0 & 3 & -1 & 0 & 2 \\ 0 & 1 & 0 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w, u) =$$

$$\{ (2, 0, 0, 0, 0) + a \cdot (-3, 0, 1, 0, 0) + b \cdot (1, 4, 0, 1, 0) + c \cdot (0, 0, 0, 0, 1) : a, b, c \in \mathbb{R} \}$$

38. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & -1 & -6 & 0 & -2 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w) =$$

$$\{ (-2, 0, 0, 2) + a \cdot (1, 1, 0, 0) + b \cdot (6, 0, 1, 0) : a, b \in \mathbb{R} \}$$

39. r.r.e.f.

$$\left(\begin{array}{ccccc|c} 1 & 1 & 0 & -4 & -1 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w) =$$

$$\{ (-1, 0, 0, 0) + a \cdot (-1, 1, 0, 0) + b \cdot (4, 0, -2, 1) : a, b \in \mathbb{R} \}$$

40. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 6 & 0 \\ 0 & 1 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (0, -2, 0) + a \cdot (-6, -1, 1) : a \in \mathbb{R} \}$$

41. r.r.e.f.

$$\left(\begin{array}{cccccc|c} 1 & 2 & 0 & -1 & 0 & -1 & -1 \\ 0 & 0 & 1 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 \end{array} \right)$$

$\{ (-1, 0, 0, 0, 0, 0) + a \cdot (-2, 1, 0, 0, 0, 0) + b \cdot (1, 0, -2, 1, 0, 0) + c \cdot (1, 0, -2, 0, -2, 1) : a, b, c \in \mathbb{R} \}$

42. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & -2 & 1 \\ 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

$$\{ (1, 1, 0) + a \cdot (2, 2, 1) : a \in \mathbb{R} \}$$

43. r.r.e.f.

$$\left(\begin{array}{cccccc|c} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 4 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{array} \right)$$

$$\{(1, 0, 2, 0, 1, 0) + a \cdot (-1, 1, 0, 0, 0, 0) + b \cdot (0, 0, -4, 1, 0, 0) + c \cdot (-1, 0, 0, 0, 0, 1) : a, b, c \in \mathbb{R}\}$$

44. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & -1 & 2 & 0 & -1 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

$$\{(-1, 0, 0, -2) + a \cdot (1, 1, 0, 0) + b \cdot (-2, 0, 1, 0) : a, b \in \mathbb{R}\}$$

45. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & -1 \\ 0 & 1 & -3 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

$$\{(-1, 0, 0) + a \cdot (0, 3, 1) : a \in \mathbb{R}\}$$

46. r.r.e.f.

$$\left(\begin{array}{cccccc|c} 1 & 3 & 0 & 2 & 0 & 3 & 0 \\ 0 & 0 & 1 & 5 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & -1 \end{array} \right)$$

$$\{(0, 0, 0, 0, -1, 0) + a \cdot (-3, 1, 0, 0, 0, 0) + b \cdot (-2, 0, -5, 1, 0, 0) + c \cdot (-3, 0, 2, 0, 1, 1) : a, b, c \in \mathbb{R}\}$$

47. r.r.e.f.

$$\left(\begin{array}{cccccc|c} 1 & 4 & 0 & 4 & 0 & 1 & -2 \\ 0 & 0 & 1 & 4 & 0 & -3 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 \end{array} \right)$$

$$\{(-2, 0, -1, 0, 2, 0) + a \cdot (-4, 1, 0, 0, 0, 0) + b \cdot (-4, 0, -4, 1, 0, 0) + c \cdot (-1, 0, 3, 0, -1, 1) : a, b, c \in \mathbb{R}\}$$

48. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & -2 & 0 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

$$\{(0, -1, 0) + a \cdot (2, 1, 1) : a \in \mathbb{R}\}$$

49. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & -3 & 3 & 0 & 2 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

$$\{(2, 0, 0, -2) + a \cdot (3, 1, 0, 0) + b \cdot (-3, 0, 1, 0) : a, b \in \mathbb{R}\}$$

50. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & 2 & 0 & 2 & -2 \\ 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

$$\{(-2, 0, 1, 0) + a \cdot (-2, 1, 0, 0) + b \cdot (-2, 0, 2, 1) : a, b \in \mathbb{R}\}$$

51. r.r.e.f.

$$\left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & -1 \end{array} \right)$$

$$(1, -1)$$

52. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{array} \right)$$

$$(2, 2, 2)$$

53. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & -1 \end{array} \right)$$

$$(2, -2, -1)$$

54. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{array} \right)$$

$$(2, -1, 0)$$

55. r.r.e.f.

$$\left(\begin{array}{cc|c} 1 & 0 & -2 \\ 0 & 1 & 0 \end{array} \right)$$

$$(-2, 0)$$

56. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{array} \right)$$

$$(1, -2, 0)$$

57. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(-1, -1, 2) = \emptyset$$

58. r.r.e.f.

$$\left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(-1, 2, -1) = \emptyset$$

59. r.r.e.f.

$$\left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(-2, 1, -1) = \emptyset$$

60. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(0, 2, 2) = \emptyset$$

61. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & -2 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(-1, -2, -1) = \emptyset$$

62. r.r.e.f.

$$\left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(-1, 0, 1) = \emptyset$$

Inverses

4.3

4.3.1 Right Inverses	359
4.3.2 Left Inverses	364
4.3.3 Inverses	367
4.3.4 Exercises	371
4.3.5 Solutions	373

Questions to Guide Your Study:

- *How and when can you compute a left inverse? a right inverse?*
- *What about just regular inverses?*

Remember that matrices represent functions. In this section we will be talking about how to represent a left, right, or just plain inverse of a function as a matrix. Finding inverse matrices is very valuable for changing which basis a matrix function is written with respect to. We address this topic in the next section. Here in this section, we focus primarily on *how we find inverses*.

4.3.1 Right Inverses



If the rank (range dimension) of a matrix is equal to the dimension of the codomain, then the matrix represents a linear transformation which is *surjective*. Remember that surjective means that the range is the same as the codomain. We can tell if a subspace is equal to the whole space *just by seeing if the dimension of the subspace is the same as the dimension of the overall space!*

Surjective Matrix Function

A matrix represents a surjective linear transformation under the column interpretation if the number of rows is equal to the dimension of the range (the rank).

Example 1. The matrix

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

represents a surjective linear transformation under the column interpretation. The rank is 2 and the number of rows is 2. Its Smith normal form is

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

which is of the form $(\text{id } 0\text{'s})$.

Now, all surjective linear transformations have something in common: they all have *right inverses*. Let's review what a right inverse is.

Right Inverse of a Linear Transformation

Given a linear transformation $f : D \rightarrow C$, then a right inverse $g : C \rightarrow D$ is a linear transformation such that if we compose it *on the right* $f \circ g$ then we get: $f \circ g = \text{id}_C$. It is a map that comes “before.” In the column interpretation, we think of a matrix multiplication on the right.

How do we compute the right inverse of a matrix that represents a surjection $f : D \rightarrow C$? We know that that the identity matrix of id_C is a submatrix of the Smith normal form of the matrix for f . In fact, since the number of rows equals the dimension of the range, the Smith normal form looks like:

$$(\text{id}_C \quad 0\text{'s})$$

where there are the *maximum* number of pivots in this “reduced column echelon form.” This maximality does something great:

Theorem 4.3.1

Suppose that a linear transformation is surjective and is given by the matrix A under the column interpretation. Then, it suffices to *only use column operations* to get the Smith normal form. So, if C is a matrix representing all of the column operations and S , the Smith normal form, $A \cdot C = S$.

This is almost enough to get a right inverse! If B is a matrix representing a right inverse, then $A \cdot B = \text{id}$. Now S is not id —but it almost is! Just take out the columns in the matrix C that make the zero columns in S . Then, C with some columns removed *will be a right inverse!*

Let $n = \dim(\text{range}(f))$ which is the *number of rows* of the matrix representing f . Then, we can find the right inverse from the column operations matrix as follows:

$$\begin{pmatrix} \text{id}_{n \times n} & \text{0's} \end{pmatrix} = (\text{matrix for } f) \cdot$$

 Column Operations Matrix
(
First n columns
Rest of the matrix
)

$$\begin{pmatrix} \text{id}_{n \times n} & \text{0's} \end{pmatrix} = (\text{matrix for } f) \cdot$$

 Column Operations Matrix
(
First n columns
Rest of the matrix
)

$$\text{id}_{n \times n} = (\text{matrix for } f) \cdot$$

 Right Inverse
(
First n columns
)

 **Example 2.** *Finding a right inverse.* Let's find a right inverse of the matrix

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

We start by finding the Smith normal form *by only using column operations*:

$$\begin{array}{ccc}
 \left(\begin{array}{ccc} (-1 \cdot 1) & & \\ 1 & 1 & 2 \\ (-1 \cdot 0) & & \\ 0 & 1 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} (-2 \cdot 1) & & \\ 1 & 0 & 2 \\ (-2 \cdot 0) & & \\ 0 & 1 & 1 \end{array} \right) \\
 \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \end{array} \right)
 \end{array}$$

Now, we find the column operations matrix by applying these *same* column operations to the 3×3 identity matrix (since there are 3 columns in A):

$$\begin{array}{c}
 \left(\begin{array}{ccc}
 1 & 0 & 0 \\
 0 & 1 & 0 \\
 0 & 0 & 1
 \end{array} \right) \rightarrow \left(\begin{array}{ccc}
 1 & -1 & 0 \\
 0 & 1 & 0 \\
 0 & 0 & 1
 \end{array} \right) \rightarrow \\
 \left(\begin{array}{ccc}
 1 & -1 & -2 \\
 0 & 1 & 0 \\
 0 & 0 & 1
 \end{array} \right) \rightarrow \left(\begin{array}{ccc}
 1 & -1 & -1 \\
 0 & 1 & -1 \\
 0 & 0 & 1
 \end{array} \right)
 \end{array}$$

These calculations give us the following product:

$$\underbrace{\left(\begin{array}{ccc}
 1 & 1 & 2 \\
 0 & 1 & 1
 \end{array} \right)}_A \cdot \underbrace{\left(\begin{array}{ccc}
 1 & -1 & -1 \\
 0 & 1 & -1 \\
 0 & 0 & 1
 \end{array} \right)}_C = \underbrace{\left(\begin{array}{ccc}
 1 & 0 & 0 \\
 0 & 1 & 0
 \end{array} \right)}_S$$

We have found a column operations matrix C that gives us the Smith normal form S . Now, simply remove the unneeded column:

$$\left(\begin{array}{ccc}
 1 & 1 & 2 \\
 0 & 1 & 1
 \end{array} \right) \cdot \left(\begin{array}{ccc}
 1 & -1 & +1 \\
 0 & 1 & -1 \\
 0 & 0 & 1
 \end{array} \right) = \left(\begin{array}{cc}
 1 & 0 \\
 0 & 1
 \end{array} \right)$$

Therefore, a right inverse for the matrix A is

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

You can check:

$$\underbrace{\left(\begin{array}{ccc}
 1 & 1 & 2 \\
 0 & 1 & 1
 \end{array} \right)}_A \cdot \underbrace{\left(\begin{array}{cc}
 1 & -1 \\
 0 & 1 \\
 0 & 0
 \end{array} \right)}_{\text{on the right}} = \left(\begin{array}{cc}
 1 & 0 \\
 0 & 1
 \end{array} \right)$$

Example 3. Let's actually find a different right inverse to the same matrix A in the last example by performing

different column operations on our way to Smith normal form:

$$\begin{array}{ccc}
 \left(\begin{array}{ccc} & \overset{-1 \cdot 1}{\curvearrowright} & \\ 1 & 1 & 2 \\ & \overset{-1 \cdot 1}{\curvearrowright} & \\ 0 & 1 & 1 \end{array} \right) & \rightarrow & \left(\begin{array}{ccc} 1 & 1 & 1 \\ 0 & \overset{-1 \cdot 1}{\curvearrowright} & 0 \\ 1 & \overset{-1 \cdot 0}{\curvearrowright} & \end{array} \right) \\
 \left(\begin{array}{ccc} 1 & 0 & 1 \\ 0 & \overset{-1 \cdot 1}{\curvearrowright} & 0 \\ 0 & 1 & \overset{-1 \cdot 0}{\curvearrowright} \end{array} \right) & \rightarrow & \left(\begin{array}{ccc} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & \curvearrowright & \end{array} \right) \\
 \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) & &
 \end{array}$$

Now, we perform these same column operations on the identity 3×3 matrix:

$$\begin{array}{ccc}
 \left(\begin{array}{ccc} & \overset{-1 \cdot 0}{\curvearrowright} & 0 \\ 1 & 0 & 0 \\ & \overset{-1 \cdot 1}{\curvearrowright} & 0 \\ 0 & 1 & 0 \\ & \overset{-1 \cdot 0}{\curvearrowright} & 1 \end{array} \right) & \rightarrow & \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & \overset{-1 \cdot 0}{\curvearrowright} & -1 \\ 0 & \overset{-1 \cdot (-1)}{\curvearrowright} & 1 \\ 0 & \overset{-1 \cdot 1}{\curvearrowright} & \end{array} \right) \\
 \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 2 & -1 \\ 0 & -1 & 1 \\ 0 & \overset{-1 \cdot 1}{\curvearrowright} & \end{array} \right) & \rightarrow & \left(\begin{array}{ccc} 1 & 0 & 0 \\ 1 & 2 & -1 \\ -1 & -1 & 1 \end{array} \right) \\
 \left(\begin{array}{ccc} 0 & 0 & 1 \\ -1 & 2 & 1 \\ 1 & -1 & -1 \end{array} \right) & &
 \end{array}$$

Now, we eliminate the unnecessary column:

$$\left(\begin{array}{cc|c} 0 & 0 & 1 \\ -1 & 2 & 1 \\ 1 & -1 & -1 \end{array} \right)$$

A right inverse for A is:

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

Indeed, you can check:

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

Non-uniqueness of Right Inverses

If a linear transformation is surjective and not bijective, then there may be many right inverses.

4.3.2 Left Inverses



Suppose that $f : D \rightarrow C$ is an injective linear transformation.

Injective Matrix Function

A matrix represents an injective linear transformation under the column interpretation if

the number of columns (i.e. the domain dimension) is equal to the dimension of the range (the rank).

Equivalently, the dimension of the kernel (i.e. the nullity) of the matrix is 0.

A left inverse $g : C \rightarrow D$ is obtained by looking at the top rows of the row operations matrix as we put the matrix of f into Smith normal form. Let $n = \dim(D)$ which is the number of *columns* of the matrix representing f .

$$\begin{pmatrix} \text{id}_C \\ 0's \end{pmatrix} = \underbrace{\begin{pmatrix} \text{First } n \text{ rows} \\ \text{Rest of the matrix} \end{pmatrix}}_{\text{Row Operations Matrix}} \cdot (\text{Matrix for } f)$$

$$\begin{pmatrix} \text{id}_C \\ 0's \end{pmatrix} = \underbrace{\begin{pmatrix} \text{First } n \text{ rows} \\ \text{Rest of the matrix} \end{pmatrix}}_{\text{Row Operations Matrix}} \cdot (\text{Matrix for } f)$$

$$\text{id}_C = \underbrace{\begin{pmatrix} \text{First } n \text{ rows} \end{pmatrix}}_{\text{Left Inverse}} \cdot (\text{Matrix for } f)$$



Example 4. Video *Finding a left inverse.* Let's find a left inverse of the matrix:

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

We perform *only row operations* on our way to Smith normal form:

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

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

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

We perform these same *row operations* to a 3×3 identity matrix because there are three rows in our beginning matrix.

$$\left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & -1 \cdot 1 & -1 \cdot 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \cdot 0 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{array} \right) \rightarrow$$

$$\left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & +1 \cdot 0 & -1 \\ -1 & 0 & 0 \\ 0 & +1 \cdot (-1) & +1 \cdot 0 \\ 1 & 0 & 1 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 1 & 0 & 0 \\ -1 \cdot 0 & 0 & -1 \cdot (-1) \\ 0 & -1 & 0 \\ +1 \cdot (-1) & -1 & +1 \cdot 0 \\ 1 & 0 & 1 \end{array} \right) \rightarrow$$

$$R = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & -1 & 0 \\ -1 & -1 & 1 \end{array} \right)$$

Now we know that:

$$\underbrace{\left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & -1 & 0 \\ -1 & -1 & 1 \end{array} \right)}_R \underbrace{\left(\begin{array}{cc} 1 & 1 \\ 0 & -1 \\ 1 & 0 \end{array} \right)}_A = \underbrace{\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{array} \right)}_S$$

Next, just eliminate the unnecessary row:

$$\left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & -1 & 0 \\ -1 & -1 & 1 \end{array} \right)$$

A right inverse is:

$$\left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & -1 & 0 \end{array} \right)$$

Indeed, you can check:

$$\left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & -1 & 0 \end{array} \right) \cdot \left(\begin{array}{cc} 1 & 1 \\ 0 & -1 \\ 1 & 0 \end{array} \right) = \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right)$$

4.3.3 Inverses

Full Rank

If a matrix representing a linear transformation is either injective or surjective, then the corresponding matrix is said to be of *full rank*. A matrix which is of full rank has a right or a left inverse.

A full-rank matrix that has both a right and a left inverse necessarily is a square matrix.

Theorem 4.3.2 A Unique Inverse

The right and left inverses of a full-rank square matrix are all the same. There is only one unique matrix that serves as both the right inverse and the left inverse.

Proof. See the theorem on unique inverses in 1.3.5. □

A^{-1}

If the function $f : D \rightarrow D$ that a matrix A represents has an inverse g , then the matrix which corresponds to g is notated as A^{-1} . We can also label g as f^{-1} . We have that $f \circ f^{-1} = f^{-1} \circ f = \text{id}_D$. We also have that $A \cdot A^{-1} = A^{-1} \cdot A = \text{id}$.

Theorem 4.3.3 Taking Inverses Reverses Order

Taking inverses of products of square matrices is the same as taking the product of the inverses in reverse order.

$$(ABC)^{-1} = C^{-1}B^{-1}A^{-1}$$

Proof. We simply illustrate the idea:

$$(ABC) \cdot \underbrace{(C^{-1}B^{-1}A^{-1})}_{\text{id}} = \underbrace{\underbrace{(BC)}_{\text{id}} \cdot \underbrace{(C^{-1}B^{-1})}_{\text{id}}}_{\text{id}} \cdot A^{-1} = A^{-1}$$

□

Theorem 4.3.4 Smith Normal Form of Isomorphism

The Smith normal form of a matrix is equal to the identity if and only if that matrix represents an isomorphism. In that case it has a unique inverse.

Example 5. Let's find the inverse of the matrix

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

If we find a right inverse, we are done. If we find a left inverse we are done. Whether we find a left or a right inverse, we will end up with exactly the same thing!

We must use:

- either just row operations (used for a left inverse)
- or just column operations (used for a right inverse)
- **But not both!**

Let's just use row operations:

$$\begin{array}{ccc} \left(\begin{array}{cc} 1 & 1 \\ 2 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & 1 \\ 0 & -1 \end{array} \right) \\ \text{(Row 1 - 2 * Row 2)} & & \text{(Row 2 - Row 1)} \\ \\ \left(\begin{array}{cc} 1 & 1 \\ 0 & -1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \\ \text{(Row 1 + Row 2)} & & \end{array}$$

Let's apply these same operations to a 2×2 identity matrix because there are two rows in A . Proceeding:

$$\begin{array}{ccc} \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & 0 \\ -2 & 1 \end{array} \right) \\ \text{(Row 1 - 2 * Row 2)} & & \text{(Row 2 + Row 1)} \\ \\ \left(\begin{array}{cc} 1 & 0 \\ -2 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} -1 & 1 \\ 2 & -1 \end{array} \right) \\ \text{(Row 1 + 2 * Row 2)} & & \end{array}$$

There are *no* rows to remove because the Smith normal form is the identity matrix!

Therefore, the inverse is:

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

We can check:

$$\underbrace{\begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix}}_{A^{-1}} \cdot \underbrace{\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}}_A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Example 6. Let's make the same computation in the last example by only doing column operations!

$$\begin{array}{ccc} \left(\begin{array}{cc} (-1 \cdot 1) & 1 \\ 1 & 1 \\ (-1 \cdot 2) & 1 \\ 2 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & 0 \\ 2 & (-1 \cdot 1) \\ (-1 \cdot 2) & -1 \end{array} \right) \\[10mm] \left(\begin{array}{cc} 1 & 0 \\ 2 & (-2 \cdot 0) \\ (-2 \cdot 1) & 1 \\ 0 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \end{array}$$

Now, let's apply these same column operations to a 2×2 identity matrix since there are two columns in A :

$$\begin{array}{ccc} \left(\begin{array}{cc} (-1 \cdot 1) & 0 \\ 1 & 0 \\ (-1 \cdot 0) & 1 \\ 0 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & (-1 \cdot 1) \\ 0 & 1 \end{array} \right) \\[10mm] \left(\begin{array}{cc} 1 & 1 \\ 0 & (-2 \cdot 1) \\ 0 & -1 \\ (-2 \cdot (-1)) & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} -1 & 1 \\ 2 & -1 \end{array} \right) \end{array}$$

Notice that we end up with exactly the same inverse!

Key Concepts from this Section

- **surjective matrix function:** (page 359) A matrix represents a surjective linear transformation under the column interpretation if the number of rows is equal to the dimension of the range (the rank).
- **right inverse of a linear transformation:** (page 360) Given a linear transformation $f : D \rightarrow C$, then a right inverse $g : C \rightarrow D$ is a linear transformation such that if we compose it *on the right* $f \circ g$ then we get: $f \circ g = \text{id}_C$. It is a map that comes “before.” In the column interpretation, we think of a matrix multiplication on the right.
- **theorem 4.3.1 :** (page 360) Suppose that a linear transformation is surjective and is given by the matrix A under the column interpretation. Then, it suffices *to only use column operations* to get the Smith normal form. So, if C is a matrix representing all of the column operations and S , the Smith normal form, $A \cdot C = S$.
- **non-uniqueness of right inverses:** (page 364) If a linear transformation is surjective and not bijective, then there may be many right inverses.
- **injective matrix function:** (page 364) A matrix represents an injective linear transformation under the column interpretation if

the number of columns (i.e. the domain dimension) is equal to the dimension of the range (the rank).

Equivalently, the dimension of the kernel (i.e. the nullity) of the matrix is 0.

- **full rank:** (page 367) If a matrix representing a linear transformation is either injective or surjective, then the corresponding matrix is said to be of *full rank*. A matrix which is of full rank has a right or a left inverse.
- **theorem 4.3.2 a unique inverse:** (page 367) The right and left inverses of a full-rank square matrix are all the same. There is only one unique matrix that serves as both the right inverse and the left inverse.
- **A^{-1} :** (page 367) If the function $f : D \rightarrow D$ that a matrix A represents has an inverse g , then the matrix which corresponds to g is notated as A^{-1} . We can also label g as f^{-1} . We have that $f \circ f^{-1} = f^{-1} \circ f = \text{id}_D$. We also have that $A \cdot A^{-1} = A^{-1} \cdot A = \text{id}$.
- **theorem 4.3.3 taking inverses reverses order:** (page 367) Taking inverses of products of square matrices is the same as taking the product of the inverses in reverse order.

$$(ABC)^{-1} = C^{-1}B^{-1}A^{-1}$$

- **theorem 4.3.4 smith normal form of isomorphism:** (page 367) The Smith normal form of a matrix is equal to the identity if and only if that matrix represents an isomorphism. In that case it has a unique inverse.

4.3.4 Exercises

Finding Left and Right Inverses

Injective linear transformations have left inverses, surjective linear transformations have right inverses, and bijective linear transformations have inverses.

Possible solutions are given—but yours could be different if it is a right or left inverse only—it all depends on which row or column operations you use! Regular inverses that are both right and left must match the given solution exactly.

You can double check your solution by multiplying to see if you get an identity matrix.

1. Find inverse:

$$\begin{pmatrix} 2 & 2 & -1 \\ 2 & -2 & -1 \\ -2 & 1 & -2 \end{pmatrix}$$

2. Find inverse:

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

3. Find right inverse:

$$\begin{pmatrix} 2 & -2 & -1 \\ -2 & -1 & 1 \end{pmatrix}$$

4. Find inverse:

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

5. Find inverse:

$$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 2 & -1 \\ 1 & -1 & -2 \end{pmatrix}$$

6. Find inverse:

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

7. Find right inverse:

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

8. Find left inverse:

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

9. Find left inverse:

$$\begin{pmatrix} 1 & 2 \\ -1 & -1 \\ 1 & -1 \end{pmatrix}$$

10. Find left inverse:

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

11. Find inverse:

$$\begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix}$$

12. Find left inverse:

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

13. Find inverse:

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

14. Find inverse:

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

15. Find right inverse:

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

16. Find inverse:

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

17. Find inverse:

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

18. Find inverse:

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

19. Find right inverse:

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

20. Find left inverse:

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

4.3.5 Solutions

1. $\begin{pmatrix} \frac{5}{24} & \frac{1}{8} & -\frac{1}{6} \\ \frac{1}{4} & -\frac{1}{4} & 0 \\ -\frac{1}{12} & -\frac{1}{4} & -\frac{1}{3} \end{pmatrix}$

2. $\begin{pmatrix} 0 & -1 & -\frac{1}{2} \\ 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{4} \end{pmatrix}$

3. Possible Solution: $\begin{pmatrix} \frac{1}{9} & -\frac{2}{9} \\ -\frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{9} & \frac{2}{9} \end{pmatrix}$

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

5. $\begin{pmatrix} \frac{5}{6} & -\frac{1}{2} & -\frac{1}{6} \\ -\frac{1}{6} & \frac{1}{2} & -\frac{1}{6} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}$

6. $\begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix}$

7. Possible Solution: $\begin{pmatrix} -\frac{1}{4} & 0 \\ \frac{1}{4} & -1 \\ -\frac{1}{2} & 1 \end{pmatrix}$

8. Possible Solution: $\begin{pmatrix} 2 & 2 & 1 \\ -2 & -3 & -1 \end{pmatrix}$

9. Possible Solution: $\begin{pmatrix} 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}$

10. Possible Solution: $\begin{pmatrix} -1 & 5 & -2 \\ 0 & 2 & -1 \end{pmatrix}$

11. $\begin{pmatrix} \frac{1}{2} & 0 \\ -1 & 1 \end{pmatrix}$

12. Possible Solution: $\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{4} & \frac{3}{4} & \frac{1}{4} \end{pmatrix}$

13. $\begin{pmatrix} \frac{2}{5} & 0 & -\frac{1}{5} \\ 0 & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{5} & -\frac{1}{2} & -\frac{1}{10} \end{pmatrix}$

14. $\begin{pmatrix} 1 & \frac{2}{3} & -\frac{4}{3} \\ -1 & -1 & 1 \\ -1 & -\frac{1}{3} & \frac{2}{3} \end{pmatrix}$

15. Possible Solution: $\begin{pmatrix} -\frac{1}{4} & -\frac{1}{4} \\ \frac{1}{8} & -\frac{3}{8} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

16. $\begin{pmatrix} 0 & 0 & 1 \\ -\frac{1}{2} & -\frac{1}{4} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{4} & -\frac{1}{2} \end{pmatrix}$

$$\mathbf{17.} \begin{pmatrix} 2 & -2 & -1 \\ 3 & -4 & -1 \\ 2 & -3 & -1 \end{pmatrix}$$

$$\mathbf{18.} \begin{pmatrix} 1 & 1 \\ 0 & -\frac{1}{2} \end{pmatrix}$$

$$\mathbf{19.} \text{ Possible Solution: } \begin{pmatrix} -\frac{3}{7} & \frac{2}{7} \\ -\frac{4}{7} & -\frac{2}{7} \\ \frac{2}{7} & \frac{1}{7} \end{pmatrix}$$

$$\mathbf{20.} \text{ Possible Solution: } \begin{pmatrix} -\frac{4}{7} & \frac{1}{7} & \frac{1}{7} \\ -\frac{1}{7} & \frac{2}{7} & \frac{2}{7} \end{pmatrix}$$

Changing Bases

4.4

4.4.1 Different Coordinate Axes: Change of Base	375
4.4.2 Expressing a Linear Transformation in Skewed Coordinates.	379
4.4.3 Expressing a Skewed Transformation in Standard Coordinates	380
4.4.4 Writing a Transformation in Terms of Ambient (Outside) Coordinates.	382
4.4.5 Relabeling Transformations	384
4.4.6 Different Bases from Input to Output	386
4.4.7 Exercises	391
4.4.8 Solutions	400

Questions to Guide Your Study:

- *What is the difference between a skewed basis and a standard basis?*
- *What is a pretending matrix and what is an unpretending matrix?*
- *How can these pretending and unpretending matrices be used when writing transformations from one basis to another?*

4.4.1 Different Coordinate Axes: Change of Base

Whenever we write down a vector as an ordered tuple like $v = (1, 4)$, we are expressing the coefficients of standard basis vectors e_1 and e_2 :

$$v = (1, 4) = 1e_1 + 4e_2.$$

So the coordinates 1 and 4 just tell us *coefficients* of basis vectors. What if we used another basis like $a = (1, 1)$ and $b = (2, 3)$? Then writing $(2, -1)_{ab}$ means:

$$(2, -1)_{ab} = 2a - b = 2 \cdot (1, 1) - (2, 3) = (0, -1)$$

The coordinate pair $(3, -1)_{ab}$ is a *skewed* version of $(0, -1)$.

This rewriting from ab -coordinates to standard coordinates

$$(2, -1)_{ab} \mapsto (0, -1)$$

is like we stop pretending that a is e_1 and b is e_2 and then say what the vector really is in standard e_1 and e_2 coordinates.

Coordinates in Other Bases

Suppose that a_1, a_2, \dots, a_n is a basis for \mathbb{R}^n . Then if $v = k_1a_1 + k_2a_2 + \dots + k_na_n$, we write

$$v = (k_1, k_2, \dots, k_n)_{a_1a_2\dots a_n}.$$

This very process of changing from ab coordinates back to standard coordinates itself is a linear transformation. Let's think about the matrix which describes it. The “ e_1 ” of the domain is $(1, 0)_{ab}$ which is really a . *But matrices only understand standard basis vectors.* The matrix *thinks* that e_1 itself is coming into it when $a = (1, 0)_{ab}$ is coming into it. Then, the matrix outputs $a = (1, 1)$ in standard coordinates. So, the matrix takes $(1, 0)$ (pretending to be a) and then outputs $(1, 1)$ (the real version of what a really is). Similarly, the matrix takes in $(0, 1)$ (pretending to be b) and then outputs $(2, 3)$.

$$\begin{pmatrix} & 1 & 2 \\ & 1 & 3 \\ \uparrow & & \uparrow \\ (1, 0)_{ab} & & (0, 1)_{ab} \end{pmatrix}$$

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

The Unpretending Matrix

The unpretending matrix (under the column interpretation) *from* a basis a_1, a_2, \dots, a_n is simply a matrix where the columns correspond to the basis vectors:

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}.$$

If $v = (k_1, k_2, \dots, k_n)_{a_1a_2\dots a_n}$ then $A \cdot v$ is the representation of v in standard coordinates.



Example 1. Video *Changing skewed coordinates back to standard coordinates.* Suppose that we have $a = (1, -1)$ and $b = (1, 2)$. Then the unpretending matrix is simply:

$$\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix} \quad \begin{matrix} \uparrow & \uparrow \\ (1, 0)_{ab} & (0, 1)_{ab} \end{matrix}$$

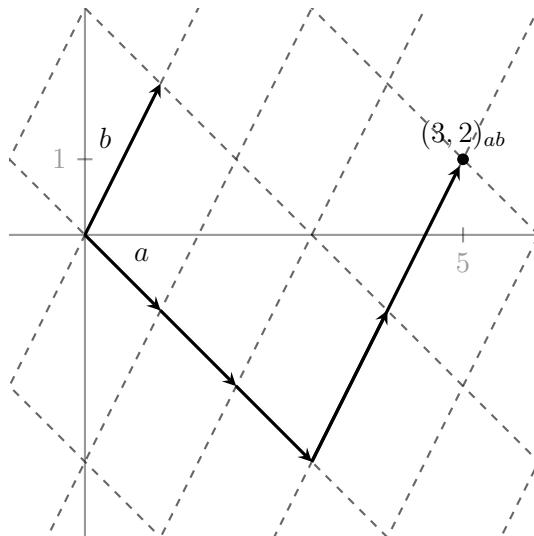
Suppose that we have the following point plotted in ab -coordinates:

$$(3, 2)_{ab} = 3a + 2b$$

Now, to see what it is in standard coordinates, we use the unpretending matrix:

$$\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$$

Therefore, $(3, 2)_{ab} = (5, 1)$ as illustrated in the following picture:



The Pretending Matrix

The pretending matrix is just the *inverse* of the unpretending matrix. It takes a vector in standard coordinates (i.e. how it really is) and outputs what the vector is in skewed coordinates which are written in a way where they seem to “pretend” that they are in terms of standard coordinates.

If U is the unpretending matrix, then $P = U^{-1}$.



Example 2. *Changing from standard coordinates to skewed coordinates.* Now, let's see how we could convert a point like $(5, 1)$ given in standard coordinates into the ab -coordinates of the last example. We building the pretending matrix. This is simply the *inverse* of the unpretending one. The way we have thus far in the book of finding the inverse matrix is to perform either *just* row operations or *just* column operations—but not both!

$$\begin{array}{ccc} \left(\begin{array}{cc} 1 & 1 \\ -1 & 2 \end{array} \right) & \rightarrow & \left(\begin{array}{cc} 1 & 1 \\ 0 & 3 \end{array} \right) \\ \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) & \rightarrow & \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \end{array}$$

To get the inverse, we perform these same steps in the order they occur to the 2×2 identity matrix:

$$\begin{array}{ccc} \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) & \rightarrow & \left(\begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right) \\ \left(\begin{array}{cc} 1 & 0 \\ \frac{1}{3} & \frac{1}{3} \end{array} \right) & \rightarrow & \left(\begin{array}{cc} \frac{2}{3} & -\frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \end{array} \right) \end{array}$$

So our pretending matrix is:

$$P = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix} = \frac{1}{3} \cdot \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$$

Now, to see what $(5, 1)$ would be in ab -coordinates, we can use this pretending matrix:

$$\frac{1}{3} \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 1 \end{pmatrix} = \frac{1}{3} \cdot \begin{pmatrix} 9 \\ 6 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$$

That is,

$$(5, 1) = (3, 2)_{ab}$$

which is just what we saw in the last example.

Labeling Finite Dimensional Vector Spaces as \mathbb{R}^n

By choosing a basis for a finite dimensional \mathbb{R} -vector space V and pretending this basis is the standard one, we naturally get coordinates with respect to that matrix. Hence, without loss of generality, we can notate V as \mathbb{R}^n for some n .

4.4.2 Expressing a Linear Transformation in Skewed Coordinates.

Matrix in Skewed Coordinates

Suppose that A is a matrix which represents a linear transformation according to standard coordinates. If U and P are a pair of unpretending and pretending matrices for a skewed basis under the column interpretation, then $P \cdot A \cdot U$ is the matrix that represents the linear transformation in the skewed coordinates.

$$\xleftarrow{\text{Pretend}} P \cdot A \cdot \xleftarrow{\text{Unpretend}} U$$



Example 3. *Expressing a linear transformation in skewed coordinates* In standard coordinates, under a column interpretation, we can express clockwise rotation by 90° as

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

since $e_1 \mapsto (0, -1)$ and $e_2 \mapsto (1, 0)$. Let's work with the skewed coordinates given by the basis

$$\{ a = (1, -1), b = (1, 2) \}.$$

We use the change of basis matrices that we found in [example 1](#) and [example 2](#):

Change of basis from ab -coordinates to standard: $U = \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}$

Change of basis from standard to ab -coordinates: $P = U^{-1} = \frac{1}{3} \cdot \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$

Change to ab
coordinates:

$$U^{-1}$$

Rotate:

$$A$$

Change to standard
coordinates:

$$U$$

$$\underbrace{\frac{1}{3} \cdot \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}}_{U^{-1}} \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}}_U = \frac{1}{3} \cdot \begin{pmatrix} -1 & 5 \\ -2 & 1 \end{pmatrix}$$

Trying it out, suppose that we want to rotate $(3, 2)_{ab}$:

$$\frac{1}{3} \cdot \begin{pmatrix} -1 & 5 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \frac{1}{3} \cdot \begin{pmatrix} 7 \\ -4 \end{pmatrix}$$

Thus, we obtain $\left(\frac{7}{3}, \frac{-4}{3}\right)_{ab}$. If we want, we can see what this looks like in standard coordinates:

$$\underbrace{\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}}_U \cdot \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix} \quad \text{rotates to} \quad \underbrace{\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}}_U \cdot \frac{1}{3} \cdot \begin{pmatrix} 7 \\ -4 \end{pmatrix} = \begin{pmatrix} 1 \\ -5 \end{pmatrix}$$

This is exactly what we should expect since $(5, 1)$ will change to $(1, -5)$ under a clockwise rotation of 90° .

4.4.3 Expressing a Skewed Transformation in Standard Coordinates

Matrix in Standard Coordinates

Suppose that A is a matrix which represents a linear transformation according to skewed coordinates. If U and P are a pair of unpretending and pretending matrices for a skewed basis under the column interpretation, then $U \cdot A \cdot P$ is the matrix that represents the linear transformation in *standard* coordinates.

$$\underbrace{\begin{matrix} U \\ \xleftarrow{\text{Unpretend}} \end{matrix}} \cdot A \cdot \underbrace{\begin{matrix} P \\ \xleftarrow{\text{Pretend}} \end{matrix}}$$



Example 4. Expressing a linear transformation in standard coordinates Suppose that the matrix

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

represents a linear transformation with respect to ab coordinates where $a = (0, 1)$ and $b = (-1, 1)$. Notice that a and b are a basis and so must be linearly independent (as they are). Then:

$$U = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \quad P = U^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

Therefore, this linear transformation in standard coordinates is given as:

$$\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}}_P = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Let's think about what all of this means. The original matrix A sends a to its first column (which is written in ab -coordinates). This first column is $(1, -1)_{ab} = a - b$. The original matrix also sends b to $a - b$.

Now, how does this rule behave on $e_1 = (1, 0)$ and $e_2 = (0, 1)$? We can write $(1, 0) = \underbrace{(0, 1)}_a - \underbrace{(-1, 1)}_b$.

How can we get this quickly? Just look at the first column of the pretending matrix P : it shows how to write $(1, 0)$ in ab -coordinates! Notice that $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ as the first column of P tells us that $(1, 0)$ goes to $1 \cdot a - 1 \cdot b$. Ok, so let's use our knowledge of what our linear transformation does to a and b to see what it will do to $(1, 0)$. We see that $a \mapsto a - b$ and $b \mapsto a - b$ gives:

$$(1, 0) = \underbrace{a}_{\substack{\downarrow \\ a - b}} - \underbrace{b}_{\substack{\downarrow \\ a - b}} \mapsto (a - b) - (a - b) = (0, 0)$$

Similarly, from the second column $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ of P , we see that $(0, 1) = a \mapsto a - b = \underbrace{(0, 1)}_a - \underbrace{(-1, 1)}_b = (1, 0)$.

Wait! We found out what the columns of the linear transformation in standard coordinates should be from scratch:

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

Essentially, all we were doing was performing the necessary matrix multiplication—but thinking about what each part of the multiplication was doing concretely!

Using the Pretending Matrix

Let a, b be two linearly independent vectors in \mathbb{R}^2 . Hence, they form a basis for \mathbb{R}^2 . Let

$$P = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$

be the pretending matrix for these skewed coordinates. The first column of the matrix tells us how to write $e_1 = (1, 0)$ in terms of the vectors a and b . That is,

$$e_1 = k_{11}a + k_{21}b$$

The second column of the matrix P tells us how to write $e_2 = (0, 1)$ in terms of the vectors a and b :

$$e_2 = k_{12}a + k_{22}b$$

Example 5. Suppose that we have the basis $a = (1, 1)$ and $b = (2, -1)$. Then:

$$U = \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} \quad P = U^{-1} = \begin{pmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{1}{3} & -\frac{1}{3} \end{pmatrix}$$

The columns of this pretending matrix tell us:

$$(1, 0) = \frac{1}{3} \cdot (a + b) \quad (0, 1) = \frac{1}{3} \cdot (2a - b)$$

4.4.4 Writing a Transformation in Terms of Ambient (Outside) Coordinates.

Suppose that we have a transformation f written in terms of ab coordinates where $a, b \in \mathbb{R}^3$. So $V = \langle a, b \rangle$ is 2-dimensional subspace of \mathbb{R}^3 . It is a plane. What if f rotates this plane and stretches it? Can we extend the transformation f to *all* of \mathbb{R}^3 so that it still performs the same function on the plane in consideration with the same spin and stretch but it also changes up all of \mathbb{R}^3 too? We would like this extension to be a linear transformation still—so parallelograms will map to parallelograms. We also want to express this linear transformation in terms of standard coordinates. There is more than one way to do this. Here is the basic schematic:

Extending a Transformation

Suppose that $a, b \in \mathbb{R}^3$ and let $V = \langle a, b \rangle$. Suppose that A is a matrix in ab coordinates representing a linear transformation $f : V \rightarrow V$. To find a linear transformation $g : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ such that g does what f does on V that is written in terms of standard coordinates, we proceed as follows:

$$\underbrace{\begin{pmatrix} U \\ & L \end{pmatrix}}_{\text{Unpretend Left Inverse of } U} \cdot A \cdot \underbrace{\begin{pmatrix} a & b \end{pmatrix}}_{\text{Standard Coordinates}}$$

We take the standard coordinates to what they are in ab coordinates. Then we apply A . Last, we translate back to standard coordinates.

The unpretending matrix $\begin{pmatrix} a & b \end{pmatrix}$ where a and b are columns is a 3×2 matrix representing an injective linear transformation. The left inverse of U will be a 2×3 matrix. Since there is more than one left inverse, there is more than one way to find our desired linear transformation g .



Example 6. *From 2-dimensional subspace to \mathbb{R}^3* Suppose that we have a 2-dimensional subspace of \mathbb{R}^3 given as $V = \langle a, b \rangle$ where

$$a = (1, 0, 1) \quad b = (-2, 1, 0)$$

That is, V is the plane spanned by a and b . Let

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_{ab}$$

represent a transformation on V in terms of ab -coordinates. It literally just swaps the vectors a and b . Can we extend this to a transformation $\mathbb{R}^3 \rightarrow \mathbb{R}^3$ which is written with respect to standard coordinates? We follow the schematic above. We find U and a left inverse L for U :

$$U = \begin{pmatrix} 1 & -2 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \quad L = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Now we compute:

$$\underbrace{\begin{pmatrix} 1 & -2 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_M \cdot \underbrace{\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}}_L$$

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

Notice that when we plug $a = (1, 0, 1)$ into this matrix function, we get:

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

which is b ! That is, a was sent to b as desired. Now let's plug in b :

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

to see that we get a . So a and b switched places as desired! This transformation is $\mathbb{R}^3 \rightarrow \mathbb{R}^3$ and not just $V \rightarrow V$. What if we had chosen a different left inverse? This idea still would have worked. Another left inverse to U is:

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

Then, we would have:

$$\underbrace{\begin{pmatrix} 1 & -2 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_M \cdot \underbrace{\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \end{pmatrix}}_L = \begin{pmatrix} -2 & -3 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Again, as desired we have:

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

4.4.5 Relabeling Transformations

An isomorphism relabels one basis as another. What if both bases are skewed and we know how we want to relabel one basis as another? How do we construct the matrix?

Relabeling Transformations

Suppose that we have two bases for \mathbb{R}^2 : a, b and c, d . Let P_{ab}, U_{ab} be the pretending/unpretending pair of matrices for a, b and let P_{cd}, U_{cd} be the pretending/unpretending pair of matrices for c, d .

Then the following matrix product relabels a as c and b as d :

$$\begin{array}{c} U_{cd} \quad \cdot \quad P_{ab} \\ \xleftarrow{\text{Unpretend}} \quad \xleftarrow{\text{Pretend}} \\ c \leftrightarrow e_1 \leftrightarrow a \\ d \leftrightarrow e_2 \leftrightarrow b \end{array}$$

The Pretending matrix P_{ab} takes a and writes it as $(1, 0)$ as if $(1, 0)$ described a in ab -coordinates. But if we say there is no pretending, no ab -coordinates and everything is in standard coordinates, then P_{ab} just sends a to e_1 and b to e_2 .



Example 7. Relabeling Transformation. Suppose that we have two different bases for \mathbb{R}^2 :

$$\mathbb{R}^2 = \langle \underbrace{(1, 1)}_a, \underbrace{(0, -1)}_b \rangle \quad \mathbb{R}^2 = \langle \underbrace{(-1, 1)}_c, \underbrace{(1, 0)}_d \rangle$$

Let's form the matrix of a linear transformation that maps a to c and b to d . First, we compute:

$$U_{cd} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \quad P_{ab} = U_{ab}^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}^{-1} = \underbrace{\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}}$$

This matrix is its own
inverse this time!

Let's just double check this self-inverse:

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

Ok, now we compute:

$$\underbrace{\begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}}_{U_{cd}} \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}}_{P_{ab}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Now try it out:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}_{\substack{a \\ c}} = \underbrace{\begin{pmatrix} -1 \\ 1 \end{pmatrix}}_{\substack{c \\ d}}$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 0 \\ -1 \end{pmatrix}}_{\substack{b \\ d}} = \underbrace{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{\substack{d \\ d}}$$

just as desired!

4.4.6 Different Bases from Input to Output

What if we wanted to write down a matrix that describes an action $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ in terms of an input basis and a different output basis?

Different Bases from Input to Output

Let $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be a linear transformation described by a matrix A according to standard coordinates.

Suppose that we have two bases for \mathbb{R}^2 : a, b and c, d . Let P_{ab}, U_{ab} be the pretending/unpretending pair of matrices for a, b and let P_{cd}, U_{cd} be the pretending/unpretending pair of matrices for c, d .

Then the following matrix product expresses the linear transformation f in terms of an input basis a and b and a different output basis c and d :

$$\xleftarrow{\text{Pretend}} P_{cd} \cdot A \cdot \xleftarrow{\text{Unpretend}} U_{ab}$$

$$f(a)_{cd} \leftrightarrow f(a) \leftrightarrow a \leftrightarrow (1, 0)_{ab}$$

$$f(b)_{cd} \leftrightarrow f(b) \leftrightarrow b \leftrightarrow (0, 1)_{ab}$$

Example 8. Let's again use the bases from the last example:

$$\mathbb{R}^2 = \langle \underbrace{(1, 1)}_a, \underbrace{(0, -1)}_b \rangle \quad \mathbb{R}^2 = \langle \underbrace{(-1, 1)}_c, \underbrace{(1, 0)}_d \rangle$$

Suppose that $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ swaps the x -axis with the y -axis so is given by the matrix

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

under a column interpretation in standard coordinates. Now, let's suppose that we have the vector $(1, 2)_{ab}$

(which is the same as $a - 2b$) and would like to run it through this linear transformation f and then output the result in cd -coordinates. We use the method prescribed above. First, we compute:

$$U_{ab} = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \quad P_{cd} = U_{cd}^{-1} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Now, we have:

$$\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}}_{P_{cd}} \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}}_{U_{ab}} = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}$$

So, we go back to our question:

$$(1, 2)_{ab} \mapsto (\ ? \)_{cd}$$

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

Let's step through this piece by piece. First $(1, 2)_{ab}$ is written in standard coordinates as

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}}_{U_{ab}} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Now, we run this through f to output $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$. Finally, rewrite this in cd -coordinates as:

$$\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}}_{P_{cd}} \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Key Concepts from this Section

- **skewed:** (page 375) Choosing a different coordinate representation other than the standard basis vectors is called a *skewed* coordinate representation.
- **coordinates in other bases:** (page 376) Suppose that a_1, a_2, \dots, a_n is a basis for \mathbb{R}^n . Then if $v = k_1a_1 + k_2a_2 + \dots + k_na_n$, we write

$$v = (k_1, k_2, \dots, k_n)_{a_1a_2\dots a_n}.$$

- **the unpretending matrix:** (page 376) The unpretending matrix (under the column interpretation) *from*

a basis a_1, a_2, \dots, a_n is simply a matrix where the columns correspond to the basis vectors:

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}.$$

If $v = (k_1, k_2, \dots, k_n)_{a_1 a_2 \dots a_n}$ then $A \cdot v$ is the representation of v in standard coordinates.

- **the pretending matrix:** (page 377) The pretending matrix is just the *inverse* of the unpretending matrix. It takes a vector in standard coordinates (i.e. how it really is) and outputs what the vector is in skewed coordinates which are written in a way where they seem to “pretend” that they are in terms of standard coordinates.

If U is the unpretending matrix, then $P = U^{-1}$.

- **labeling finite dimensional vector spaces as \mathbb{R}^n :** (page 378) By choosing a basis for a finite dimensional \mathbb{R} -vector space V and pretending this basis is the standard one, we naturally get coordinates with respect to that matrix. Hence, without loss of generality, we can notate V as \mathbb{R}^n for some n .
- **matrix in skewed coordinates:** (page 379) Suppose that A is a matrix which represents a linear transformation according to standard coordinates. If U and P are a pair of unpretending and pretending matrices for a skewed basis under the column interpretation, then $P \cdot A \cdot U$ is the matrix that represents the linear transformation in the skewed coordinates.

$$\begin{array}{c} P \quad \cdot A \cdot \quad U \\ \xleftarrow{\text{Pretend}} \qquad \qquad \qquad \xleftarrow{\text{Unpretend}} \end{array}$$

- **matrix in standard coordinates:** (page 380) Suppose that A is a matrix which represents a linear transformation according to skewed coordinates. If U and P are a pair of unpretending and pretending matrices for a skewed basis under the column interpretation, then $U \cdot A \cdot P$ is the matrix that represents the linear transformation in *standard* coordinates.

$$\begin{array}{c} U \quad \cdot A \cdot \quad P \\ \xleftarrow{\text{Unpretend}} \qquad \qquad \qquad \xleftarrow{\text{Pretend}} \end{array}$$

- **using the pretending matrix:** (page 381) Let a, b be two linearly independent vectors in \mathbb{R}^2 . Hence, they form a basis for \mathbb{R}^2 . Let

$$P = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$

be the pretending matrix for these skewed coordinates. The first column of the matrix tells us how to write $e_1 = (1, 0)$ in terms of the vectors a and b . That is,

$$e_1 = k_{11}a + k_{21}b$$

The second column of the matrix P tells us how to write $e_2 = (0, 1)$ in terms of the vectors a and b :

$$e_2 = k_{12}a + k_{22}b$$

- **extending a transformation:** (page 382) Suppose that $a, b \in \mathbb{R}^3$ and let $V = \langle a, b \rangle$. Suppose that A is a matrix in ab coordinates representing a linear transformation $f : V \rightarrow V$. To find a linear transformation $g : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ such that g does what f does on V that is written in terms of standard coordinates, we proceed as follows:

$$\begin{array}{ccc} U & \cdot A \cdot & L \\ \xleftarrow{\text{Unpretend}} & & \xleftarrow{\text{Left Inverse of } U} \end{array}$$

We take the standard coordinates to what they are in ab coordinates. Then we apply A . Last, we translate back to standard coordinates.

The unpretending matrix $\begin{pmatrix} a & b \end{pmatrix}$ where a and b are columns is a 3×2 matrix representing an injective linear transformation. The left inverse of U will be a 2×3 matrix. Since there is more than one left inverse, there is more than one way to find our desired linear transformation g .

- **relabeling transformations:** (page 384) Suppose that we have two bases for \mathbb{R}^2 : a, b and c, d . Let P_{ab} , U_{ab} be the pretending/unpretending pair of matrices for a, b and let P_{cd} , U_{cd} be the pretending/unpretending pair of matrices for c, d . Then the following matrix product relabels a as c and b as d :

$$\begin{array}{ccc} U_{cd} & \cdot & P_{ab} \\ \xleftarrow{\text{Unpretend}} & \xleftarrow{\text{Pretend}} & \\ c \leftrightarrow e_1 \leftrightarrow a & & \\ d \leftrightarrow e_2 \leftrightarrow b & & \end{array}$$

The Pretending matrix P_{ab} takes a and writes it as $(1, 0)$ as if $(1, 0)$ described a in ab -coordinates. But if we say there is no pretending, no ab -coordinates and everything is in standard coordinates, then P_{ab} just sends a to e_1 and b to e_2 .

- **different bases from input to output:** (page 386) Let $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be a linear transformation described by a matrix A according to standard coordinates.

Suppose that we have two bases for \mathbb{R}^2 : a, b and c, d . Let P_{ab} , U_{ab} be the pretending/unpretending pair of matrices for a, b and let P_{cd} , U_{cd} be the pretending/unpretending pair of matrices for c, d .

Then the following matrix product expresses the linear transformation f in terms of an input basis a and b and a different output basis c and d :

$$\begin{array}{c} P_{cd} \cdot A \cdot U_{ab} \\ \xleftarrow{\text{Pretend}} \qquad \qquad \xleftarrow{\text{Unpretend}} \end{array}$$

$$f(a)_{cd} \leftrightarrow f(a) \leftrightarrow a \leftrightarrow (1, 0)_{ab}$$

$$f(b)_{cd} \leftrightarrow f(b) \leftrightarrow b \leftrightarrow (0, 1)_{ab}$$

4.4.7 Exercises

Rewriting Matrices with Respect to Skewed Coordinates

The following transformations are given as matrices with respect to standard coordinates in the column interpretation. For each of the following, give the matrix which describes this same transformation with respect to the skewed coordinates a and b .

1. $a = (2, 2)$ $b = (2, -2)$

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

2. $a = (2, -2)$ $b = (-2, 1)$

$$\begin{pmatrix} -2 & -1 \\ -2 & -1 \end{pmatrix}$$

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

$$\begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}$$

4. $a = (2, -1)$ $b = (0, -1)$

$$\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$$

5. $a = (1, 2)$ $b = (1, -1)$

$$\begin{pmatrix} 2 & 1 \\ -2 & -2 \end{pmatrix}$$

6. $a = (-2, -1)$ $b = (2, -2)$

$$\begin{pmatrix} -1 & 2 \\ 1 & -2 \end{pmatrix}$$

7. $a = (-2, -2)$ $b = (0, -1)$

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

8. $a = (2, 2)$ $b = (1, -1)$

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

9. $a = (-2, 2)$ $b = (2, 1)$

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

10. $a = (-1, -2)$ $b = (1, -1)$

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

11. $a = (-2, 2)$ $b = (2, 1)$

$$\begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix}$$

12. $a = (2, 1)$ $b = (1, 2)$

$$\begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$$

13. $a = (-2, -1)$ $b = (1, -2)$

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

14. $a = (1, 0)$ $b = (0, 1)$

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

Rewriting Matrices with Respect to Standard Coordinates

The following transformations are given as matrices with respect to the skewed coordinates a and b . For each of the following, give the matrix which describes this same transformation with respect to *standard coordinates*.

15. $a = (2, -1)$ $b = (0, 2)$

$$\begin{pmatrix} -2 & 1 \\ -1 & 0 \end{pmatrix}_{ab}$$

16. $a = (-2, 1)$ $b = (-1, 2)$

$$\begin{pmatrix} -2 & 2 \\ 0 & 1 \end{pmatrix}_{ab}$$

17. $a = (1, -1)$ $b = (-1, -2)$

$$\begin{pmatrix} 2 & -1 \\ 2 & 2 \end{pmatrix}_{ab}$$

18. $a = (-2, -2)$ $b = (1, -2)$

$$\begin{pmatrix} -2 & -1 \\ 2 & -2 \end{pmatrix}_{ab}$$

19. $a = (-1, -2)$ $b = (-2, -1)$

$$\begin{pmatrix} -2 & -1 \\ -1 & 2 \end{pmatrix}_{ab}$$

20. $a = (1, 0)$ $b = (-1, 1)$

$$\begin{pmatrix} 0 & -1 \\ 2 & -2 \end{pmatrix}_{ab}$$

21. $a = (0, 2)$ $b = (2, 0)$

$$\begin{pmatrix} -2 & -1 \\ -1 & 0 \end{pmatrix}_{ab}$$

22. $a = (1, 0)$ $b = (-2, 1)$

$$\begin{pmatrix} 1 & 1 \\ 0 & -2 \end{pmatrix}_{ab}$$

23. $a = (2, 0)$ $b = (2, -2)$

$$\begin{pmatrix} 2 & 2 \\ -2 & 2 \end{pmatrix}_{ab}$$

24. $a = (-2, 0)$ $b = (1, -2)$

$$\begin{pmatrix} -2 & -1 \\ 1 & -1 \end{pmatrix}_{ab}$$

25. $a = (-2, 0)$ $b = (2, 2)$

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}_{ab}$$

26. $a = (0, -1)$ $b = (2, -1)$

$$\begin{pmatrix} 0 & 0 \\ -2 & -2 \end{pmatrix}_{ab}$$

27. $a = (0, 1)$ $b = (2, -2)$

$$\begin{pmatrix} 1 & -2 \\ 1 & 2 \end{pmatrix}_{ab}$$

28. $a = (2, 1)$ $b = (-1, 0)$

$$\begin{pmatrix} -1 & 1 \\ -1 & 2 \end{pmatrix}_{ab}$$

Isomorphisms for a Relabeling

For each of the following, two bases of \mathbb{R}^2 are given: $\{a, b\}$ and $\{c, d\}$. Create a matrix that describes a linear transformation under a column interpretation that relabels a as c and b as d . This linear transformation will be an isomorphism.

29. Relabel $a = (0, 1)$ $b = (-2, 2)$
as $c = (-1, -2)$ $d = (-1, 0)$.

30. Relabel $a = (1, -1)$ $b = (1, 2)$
as $c = (-2, -2)$ $d = (1, -1)$.

31. Relabel $a = (1, 1)$ $b = (2, 0)$
as $c = (1, 0)$ $d = (0, -2)$.

32. Relabel $a = (2, -2)$ $b = (-1, 2)$
as $c = (1, -2)$ $d = (0, 1)$.

33. Relabel $a = (-2, -1)$ $b = (-2, -2)$
as $c = (-2, 2)$ $d = (2, -1)$.

34. Relabel $a = (0, 1)$ $b = (-2, -2)$
as $c = (-1, 1)$ $d = (2, -1)$.

35. Relabel $a = (2, -1)$ $b = (2, 2)$
as $c = (2, -2)$ $d = (-1, 0)$.

36. Relabel $a = (1, 0)$ $b = (2, -1)$
as $c = (1, -2)$ $d = (2, 1)$.

37. Relabel $a = (1, 0)$ $b = (1, 2)$
as $c = (0, -1)$ $d = (-2, 1)$.

38. Relabel $a = (-1, 2)$ $b = (1, 1)$
as $c = (-2, -2)$ $d = (2, 0)$.

- 39.** Relabel $a = (-2, -1)$ $b = (-2, 0)$
as $c = (-2, 1)$ $d = (1, -2)$.

- 40.** Relabel $a = (0, -2)$ $b = (1, 2)$
as $c = (-1, 1)$ $d = (-2, 1)$.

- 41.** Relabel $a = (1, 0)$ $b = (1, 1)$
as $c = (1, -2)$ $d = (1, -1)$.

- 42.** Relabel $a = (2, 0)$ $b = (2, -2)$
as $c = (-1, 1)$ $d = (0, -2)$.

- 43.** Relabel $a = (-1, 2)$ $b = (0, -1)$
as $c = (0, 2)$ $d = (-1, 0)$.

- 44.** Relabel $a = (1, -1)$ $b = (-2, 0)$
as $c = (2, -1)$ $d = (-1, 2)$.

- 45.** Relabel $a = (-1, 0)$ $b = (2, -2)$
as $c = (-2, -1)$ $d = (-2, 0)$.

- 46.** Relabel $a = (1, -1)$ $b = (0, 2)$
as $c = (-1, -2)$ $d = (0, 1)$.

- 47.** Relabel $a = (1, -1)$ $b = (0, -2)$
as $c = (1, -2)$ $d = (-2, 1)$.

- 48.** Relabel $a = (-2, -1)$ $b = (2, 0)$
as $c = (1, 2)$ $d = (0, 1)$.

Extending Subspace Transformations

For each of the following, find a linear transformation $\mathbb{R}^3 \rightarrow \mathbb{R}^3$ whose restriction to the subspace $\langle a, b \rangle$ is given by the given transformation in ab coordinates.

- 49.** Transformation on ab coordinates:

$$\begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}_{ab}$$

$$a = (-1, -1, -2) \quad b = (-1, -1, 2)$$

- 50.** Transformation on ab coordinates:

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

$$a = (1, 0, 0) \quad b = (2, -2, 2)$$

- 51.** Transformation on ab coordinates:

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

$$a = (2, 2, 2) \quad b = (2, 1, -2)$$

- 52.** Transformation on ab coordinates:

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

$$a = (1, -2, -2) \quad b = (2, 0, -1)$$

53. Transformation on ab coordinates:

$$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}_{ab}$$

$$a = (0, -1, 1) \quad b = (-2, 0, -2)$$

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

$$a = (1, 2, 0) \quad b = (0, 2, 1)$$

55. Transformation on ab coordinates:

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}_{ab}$$

$$a = (2, 2, -2) \quad b = (2, -2, 1)$$

$$\begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}_{ab}$$

$$a = (-2, -2, 0) \quad b = (2, -1, -2)$$

57. Transformation on ab coordinates:

$$\begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}_{ab}$$

$$a = (-2, -1, -2) \quad b = (-1, -2, -2)$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}_{ab}$$

$$a = (2, -1, -2) \quad b = (-2, 1, -2)$$

59. Transformation on ab coordinates:

$$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}_{ab}$$

$$a = (1, 2, -1) \quad b = (-1, -1, 1)$$

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}_{ab}$$

$$a = (-2, -1, 0) \quad b = (2, -2, -1)$$

Rewriting Transformations with Different Input and Output Bases

The following matrices are written in standard coordinates according to a column interpretation. For each of the following, rewrite the matrix to be with respect to the input basis $\{a, b\}$ and the output basis $\{c, d\}$.

61. $a = (-1, -1)$ $b = (-2, 0)$
 $c = (2, -1)$ $d = (-1, 1)$

$$\begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix}$$

62. $a = (-2, -1)$ $b = (1, 2)$
 $c = (1, 0)$ $d = (2, 2)$

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

63. $a = (0, -1)$ $b = (-1, -1)$
 $c = (-2, 2)$ $d = (1, -2)$

$$\begin{pmatrix} -2 & -2 \\ 1 & -1 \end{pmatrix}$$

64. $a = (-2, 0)$ $b = (-1, 1)$
 $c = (2, -1)$ $d = (2, -2)$

$$\begin{pmatrix} 2 & 2 \\ 0 & -2 \end{pmatrix}$$

65. $a = (-1, 0)$ $b = (-1, -1)$
 $c = (2, 0)$ $d = (0, -1)$

$$\begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix}$$

66. $a = (0, -1)$ $b = (2, 0)$
 $c = (0, 2)$ $d = (2, 2)$

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$$

67. $a = (2, -2)$ $b = (2, -1)$
 $c = (-1, -1)$ $d = (2, 1)$

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

68. $a = (2, 2)$ $b = (0, -2)$
 $c = (-1, -1)$ $d = (-1, -2)$

$$\begin{pmatrix} -1 & 2 \\ 1 & 1 \end{pmatrix}$$

69. $a = (-2, 1)$ $b = (-1, 0)$
 $c = (1, -2)$ $d = (0, -1)$

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

70. $a = (2, 0)$ $b = (-2, -1)$
 $c = (-2, 2)$ $d = (2, 0)$

$$\begin{pmatrix} 2 & -1 \\ -2 & -2 \end{pmatrix}$$

Rewriting Rotations with Expansions/Compressions in Terms of Skewed Coordinates

Write the linear transformation that corresponds to the composition of transformations (in the order given) $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ with respect to the *ordered* basis given by a and b :

71. $a = (-1, 0)$ $b = (1, -2)$

- x and y values: Compress by a factor of 2.
- Rotate by 45° .

72. $a = (0, -1)$ $b = (-2, 1)$

- y values : Stretch by a factor of 3.
- Reflect across y axis.

73. $a = (-2, 2)$ $b = (-2, -2)$

- y values : Compress by a factor of 3.

74. $a = (1, 0)$ $b = (0, -2)$

- Rotate by 150° .
- y values : Compress by a factor of 3.

75. $a = (1, -2)$ $b = (2, -1)$

- Rotate by 30° .
- y values : Stretch by a factor of 2.

76. $a = (-1, -2)$ $b = (-2, 1)$

- y values : Stretch by a factor of 2.
- Reflect across y axis.

77. $a = (0, -1)$ $b = (-2, 1)$

- Rotate by 30° .
- Reflect across x axis.
- x and y values: Stretch by a factor of 2.

78. $a = (-2, 1)$ $b = (1, 2)$

- Reflect across x axis.

79. $a = (0, -2)$ $b = (-1, -1)$

- Reflect across x axis.

80. $a = (-2, -1)$ $b = (-2, 0)$

- Reflect across x axis.
- Rotate by 150° .

81. $a = (-1, 1)$ $b = (2, -1)$

- Rotate by 120° .

82. $a = (2, 0)$ $b = (0, -2)$

- x and y values: Stretch by a factor of 3.
- Reflect across y axis.

83. $a = (1, 0)$ $b = (1, 1)$

- Rotate by 30° .

84. $a = (2, 2)$ $b = (-2, 2)$

- Rotate by -45° .
- x values : Stretch by a factor of 3.

85. $a = (-1, -2)$ $b = (-2, -1)$

- Reflect across x axis.

86. $a = (0, 2)$ $b = (-2, 2)$

- Reflect across x axis.
- Rotate by 150° .
- x values : Compress by a factor of 3.

87. $a = (1, -2)$ $b = (-1, -1)$

- Reflect across x axis.
- Rotate by 45° .

88. $a = (-1, -2)$ $b = (2, -2)$

- Reflect across x axis.

89. $a = (2, -1)$ $b = (-2, 0)$

- x and y values: Compress by a factor of 2.
- Rotate by 45° .
- Reflect across y axis.

90. $a = (1, 1)$ $b = (-1, -2)$

- Reflect across y axis.

4.4.8 Solutions

1. $\begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & -\frac{1}{4} \end{pmatrix} \cdot \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 2 & -2 \end{pmatrix} = \begin{pmatrix} -2 & 0 \\ 0 & 0 \end{pmatrix}$

2. $\begin{pmatrix} -\frac{1}{2} & -1 \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} -2 & -1 \\ -2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & -\frac{9}{2} \\ 4 & -6 \end{pmatrix}$

3. $\begin{pmatrix} 0 & -1 \\ -\frac{1}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -2 & 4 \\ -2 & 4 \end{pmatrix}$

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

5. $\begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ -2 & -2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} -\frac{2}{3} & \frac{1}{3} \\ \frac{14}{3} & \frac{2}{3} \end{pmatrix}$

6. $\begin{pmatrix} -\frac{1}{3} & -\frac{1}{3} \\ \frac{1}{6} & -\frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} -1 & 2 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} -2 & 2 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & -3 \end{pmatrix}$

7. $\begin{pmatrix} -\frac{1}{2} & 0 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & 0 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 4 & 0 \end{pmatrix}$

8. $\begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -2 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} -\frac{3}{2} & -\frac{1}{4} \\ 5 & -\frac{1}{2} \end{pmatrix}$

9. $\begin{pmatrix} -\frac{1}{6} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \\ -2 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} \frac{2}{3} & \frac{5}{6} \\ \frac{8}{3} & \frac{1}{3} \end{pmatrix}$

10. $\begin{pmatrix} -\frac{1}{3} & -\frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} \\ -1 & 1 \\ -2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} -\frac{2}{3} & -\frac{4}{3} \\ \frac{4}{3} & -\frac{1}{3} \end{pmatrix}$

11. $\begin{pmatrix} -\frac{1}{6} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{5}{3} \\ -\frac{2}{3} & \frac{8}{3} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} -2 & 2 \\ 2 & 1 \end{pmatrix} =$

12. $\begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{4}{3} \\ \frac{5}{3} & \frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} =$

13. $\begin{pmatrix} -\frac{2}{5} & -\frac{1}{5} \\ \frac{1}{5} & -\frac{2}{5} \\ -2 & 1 \\ -1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & -2 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} -\frac{8}{5} & -\frac{11}{5} \\ -\frac{6}{5} & -\frac{2}{5} \end{pmatrix}$

14. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & -1 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & 2 \end{pmatrix}$

15. $\begin{pmatrix} 2 & 0 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{1}{4} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} -\frac{3}{2} & 1 \\ -\frac{1}{4} & -\frac{1}{2} \end{pmatrix}$

16. $\begin{pmatrix} -2 & -1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} -2 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -\frac{13}{3} & -\frac{14}{3} \\ \frac{8}{3} & \frac{10}{3} \end{pmatrix}$

17. $\begin{pmatrix} 1 & -1 \\ -1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{1}{3} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -3 & 3 \end{pmatrix}$

18. $\begin{pmatrix} -2 & 1 \\ -2 & -2 \end{pmatrix} \cdot \begin{pmatrix} -2 & -1 \\ 2 & -2 \end{pmatrix} = \begin{pmatrix} -\frac{1}{3} & -\frac{1}{6} \\ \frac{1}{3} & -\frac{1}{3} \end{pmatrix} = \begin{pmatrix} -2 & -1 \\ 2 & -2 \end{pmatrix}$

19. $\begin{pmatrix} -1 & -2 \\ -2 & -1 \end{pmatrix} \cdot \begin{pmatrix} -2 & -1 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} \\ -\frac{2}{3} & \frac{1}{3} \end{pmatrix} = \begin{pmatrix} \frac{10}{3} & -\frac{11}{3} \\ \frac{5}{3} & -\frac{10}{3} \end{pmatrix}$

20. $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 2 & -2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -2 & -1 \\ 2 & 0 \end{pmatrix}$

21. $\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & -1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & -2 \end{pmatrix}$

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

23. $\begin{pmatrix} 2 & 2 \\ 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ -2 & 2 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} 0 & -4 \\ 2 & 4 \end{pmatrix}$

24. $\begin{pmatrix} -2 & 1 \\ 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} -2 & -1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{2} & -\frac{1}{4} \\ 0 & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} -\frac{5}{2} & -\frac{7}{4} \\ 1 & -\frac{1}{2} \end{pmatrix}$

25. $\begin{pmatrix} -2 & 2 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -1 & 2 \end{pmatrix}$

26. $\begin{pmatrix} 0 & 2 \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ -2 & -2 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{2} & -1 \\ \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 0 & -2 \end{pmatrix}$

27. $\begin{pmatrix} 0 & 2 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ -4 & -1 \end{pmatrix}$

28. $\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}$

29. $\begin{pmatrix} -\frac{1}{2} & -1 \\ -2 & -2 \end{pmatrix}$

30. $\begin{pmatrix} -1 & 1 \\ -\frac{5}{3} & \frac{1}{3} \end{pmatrix}$

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

32. $\begin{pmatrix} 1 & \frac{1}{2} \\ -1 & 0 \end{pmatrix}$

33. $\begin{pmatrix} 3 & -4 \\ -\frac{5}{2} & 3 \end{pmatrix}$

34. $\begin{pmatrix} 0 & -1 \\ -\frac{1}{2} & 1 \end{pmatrix}$

35. $\begin{pmatrix} \frac{1}{2} & -1 \\ -\frac{2}{3} & \frac{2}{3} \end{pmatrix}$

36. $\begin{pmatrix} 1 & 0 \\ -2 & -5 \end{pmatrix}$

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

38. $\begin{pmatrix} 2 & 0 \\ \frac{2}{3} & -\frac{2}{3} \end{pmatrix}$

39. $\begin{pmatrix} -\frac{1}{2} & 3 \\ 1 & -3 \end{pmatrix}$

40. $\begin{pmatrix} -3 & \frac{1}{2} \\ 2 & -\frac{1}{2} \end{pmatrix}$

41. $\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$

42. $\begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{3}{2} \end{pmatrix}$

43. $\begin{pmatrix} 2 & 1 \\ -2 & 0 \end{pmatrix}$

44. $\begin{pmatrix} \frac{1}{2} & -\frac{3}{2} \\ -1 & 0 \end{pmatrix}$

45. $\begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}$

46. $\begin{pmatrix} -1 & 0 \\ -\frac{3}{2} & \frac{1}{2} \end{pmatrix}$

47. $\begin{pmatrix} 2 & 1 \\ -\frac{5}{2} & -\frac{1}{2} \end{pmatrix}$

48. $\begin{pmatrix} 0 & -1 \\ \frac{1}{2} & -3 \end{pmatrix}$

49. Possible Solution:

$$\begin{pmatrix} -1 & -1 \\ -1 & -1 \\ -2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} -\frac{3}{8} & -\frac{1}{8} & -\frac{1}{4} \\ -\frac{1}{8} & -\frac{3}{8} & \frac{1}{4} \end{pmatrix}$$

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

50. Possible Solution:

$$\begin{pmatrix} 1 & 2 \\ 0 & -2 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{1}{3} & -\frac{2}{3} \\ 0 & -\frac{1}{6} & \frac{1}{3} \end{pmatrix}$$

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

51. Possible Solution:

$$\begin{pmatrix} 2 & 2 \\ 2 & 1 \\ 2 & -2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{10} & \frac{1}{5} & \frac{1}{5} \\ \frac{1}{5} & \frac{1}{15} & -\frac{4}{15} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{4}{5} & \frac{14}{15} & \frac{4}{15} \\ \frac{7}{10} & \frac{11}{15} & \frac{1}{15} \\ \frac{2}{5} & \frac{2}{15} & -\frac{8}{15} \end{pmatrix}$$

52. Possible Solution:

$$\begin{pmatrix} 1 & 2 \\ -2 & 0 \\ -2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{13} & -\frac{5}{13} & -\frac{2}{13} \\ \frac{6}{13} & \frac{4}{13} & -\frac{1}{13} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{6}{13} & \frac{4}{13} & -\frac{1}{13} \\ -\frac{12}{13} & -\frac{8}{13} & \frac{2}{13} \\ -\frac{12}{13} & -\frac{8}{13} & \frac{2}{13} \end{pmatrix}$$

53. Possible Solution:

$$\begin{pmatrix} 0 & -2 \\ -1 & 0 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 & 1 \\ \frac{1}{2} & -1 & -1 \end{pmatrix}$$

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

54. Possible Solution:

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

$$= \begin{pmatrix} 0 & 0 & 0 \\ \frac{2}{5} & \frac{4}{5} & -\frac{8}{5} \\ \frac{1}{5} & \frac{2}{5} & -\frac{4}{5} \end{pmatrix}$$

55. Possible Solution:

$$\begin{pmatrix} 2 & 2 \\ 2 & -2 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -\frac{1}{2} & -1 \\ 0 & -1 & -1 \end{pmatrix}$$

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

56. Possible Solution:

$$\begin{pmatrix} -2 & 2 \\ -2 & -1 \\ 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{6} & -\frac{1}{3} & 0 \\ \frac{1}{6} & -\frac{1}{6} & -\frac{1}{4} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{3} & \frac{2}{3} & 0 \\ -\frac{1}{6} & -\frac{1}{3} & 0 \\ -\frac{1}{3} & -\frac{2}{3} & 0 \end{pmatrix}$$

57. Possible Solution:

$$\begin{pmatrix} -2 & -1 \\ -1 & -2 \\ -2 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} -\frac{2}{5} & \frac{3}{5} & -\frac{2}{5} \\ \frac{3}{5} & -\frac{2}{5} & -\frac{2}{5} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{7}{5} & -\frac{3}{5} & -\frac{8}{5} \\ 1 & 0 & -2 \\ \frac{8}{5} & -\frac{2}{5} & -\frac{12}{5} \end{pmatrix}$$

58. Possible Solution:

$$\begin{pmatrix} 2 & -2 \\ -1 & 1 \\ -2 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{3}{8} & \frac{1}{4} & -\frac{1}{4} \\ -\frac{5}{8} & -\frac{3}{4} & -\frac{1}{4} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{7}{4} & \frac{5}{2} & \frac{3}{2} \\ -\frac{7}{8} & -\frac{5}{4} & -\frac{3}{4} \\ -\frac{3}{4} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

59. Possible Solution:

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

$$= \begin{pmatrix} -3 & 1 & -1 \\ -5 & 1 & -2 \\ 3 & -1 & 1 \end{pmatrix}$$

60. Possible Solution:

$$\begin{pmatrix} -2 & 2 \\ -1 & -2 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -\frac{5}{12} & -\frac{1}{6} & -\frac{1}{2} \\ \frac{1}{6} & -\frac{1}{3} & 0 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{4}{3} & \frac{4}{3} & 2 \\ -\frac{7}{12} & \frac{1}{6} & -\frac{1}{2} \\ -\frac{5}{12} & -\frac{1}{6} & -\frac{1}{2} \end{pmatrix}$$

$$\mathbf{61.} \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 0 & 0 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & -2 \\ -1 & 0 \end{pmatrix} =$$

$$\mathbf{62.} \begin{pmatrix} 1 & -1 \\ 0 & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} -2 & -2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 \\ -1 & 2 \end{pmatrix} =$$

$$\begin{pmatrix} 7 & -8 \\ -\frac{1}{2} & 1 \end{pmatrix}$$

63. $\begin{pmatrix} -1 & -\frac{1}{2} \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} -2 & -2 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -\frac{5}{2} & -4 \\ -3 & -4 \end{pmatrix}$

64. $\begin{pmatrix} 1 & 1 \\ -\frac{1}{2} & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} -2 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -4 & -2 \\ 2 & 2 \end{pmatrix}$

65. $\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 2 & 1 \end{pmatrix}$

66. $\begin{pmatrix} -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & -2 \\ 0 & 2 \end{pmatrix}$

67. $\begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} -14 & -9 \\ -8 & -5 \end{pmatrix}$

68. $\begin{pmatrix} -2 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 2 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 6 \\ -2 & -2 \end{pmatrix}$

69. $\begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & -2 \\ 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & -2 \end{pmatrix}$

70. $\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 \\ -2 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 & -2 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ 0 & \frac{3}{2} \end{pmatrix}$

71. $\begin{pmatrix} -1 & -\frac{1}{2} \\ 0 & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{4}\sqrt{2} & \frac{1}{4}\sqrt{2} \\ -\frac{1}{4}\sqrt{2} & \frac{1}{4}\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} \frac{1}{8}\sqrt{2} & \frac{5}{8}\sqrt{2} \\ -\frac{1}{8}\sqrt{2} & \frac{3}{8}\sqrt{2} \end{pmatrix}$

72. $\begin{pmatrix} -\frac{1}{2} & -1 \\ -\frac{1}{2} & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 & -2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & -4 \\ 0 & -1 \end{pmatrix}$

73.
$$\begin{pmatrix} -\frac{1}{4} & \frac{1}{4} \\ -\frac{1}{4} & -\frac{1}{4} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} -2 & -2 \\ 2 & -2 \end{pmatrix} = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

74.
$$\begin{pmatrix} 1 & 0 \\ 0 & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{2}\sqrt{3} & \frac{1}{6} \\ -\frac{1}{2} & -\frac{1}{6}\sqrt{3} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2}\sqrt{3} & -\frac{1}{3} \\ \frac{1}{4} & -\frac{1}{6}\sqrt{3} \end{pmatrix}$$

75.
$$\begin{pmatrix} -\frac{1}{3} & -\frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2}\sqrt{3} & 1 \\ -\frac{1}{2} & \sqrt{3} \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} \frac{7}{6}\sqrt{3} + 1 & \frac{1}{3}\sqrt{3} + 1 \\ -\frac{1}{3}\sqrt{3} - \frac{3}{2} & \frac{1}{3}\sqrt{3} - 1 \end{pmatrix}$$

76.
$$\begin{pmatrix} -\frac{1}{5} & -\frac{2}{5} \\ -\frac{2}{5} & \frac{1}{5} \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} -1 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} \frac{7}{5} & -\frac{6}{5} \\ -\frac{6}{5} & -\frac{2}{5} \end{pmatrix}$$

77.
$$\begin{pmatrix} -\frac{1}{2} & -1 \\ -\frac{1}{2} & 0 \end{pmatrix} \cdot \begin{pmatrix} \sqrt{3} & -1 \\ -1 & -\sqrt{3} \end{pmatrix} \cdot \begin{pmatrix} 0 & -2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -\sqrt{3} - \frac{1}{2} & 2\sqrt{3} - \frac{3}{2} \\ -\frac{1}{2} & \sqrt{3} + \frac{1}{2} \end{pmatrix}$$

78.
$$\begin{pmatrix} -\frac{2}{5} & \frac{1}{5} \\ \frac{1}{5} & \frac{2}{5} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} \frac{3}{5} & -\frac{4}{5} \\ -\frac{4}{5} & -\frac{3}{5} \end{pmatrix}$$

79.
$$\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$$

80.
$$\begin{pmatrix} 0 & -1 \\ -\frac{1}{2} & 1 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{2}\sqrt{3} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2}\sqrt{3} \end{pmatrix} \cdot \begin{pmatrix} -2 & -2 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2}\sqrt{3} + 1 & 1 \\ -\sqrt{3} - \frac{3}{4} & -\frac{1}{2}\sqrt{3} - 1 \end{pmatrix}$$

81.
$$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{2} & \frac{1}{2}\sqrt{3} \\ -\frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} \frac{3}{2}\sqrt{3} - \frac{1}{2} & -\frac{5}{2}\sqrt{3} \\ \sqrt{3} & -\frac{3}{2}\sqrt{3} - \frac{1}{2} \end{pmatrix}$$

82.
$$\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} -3 & 0 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} -3 & 0 \\ 0 & 3 \end{pmatrix}$$

83. $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2}\sqrt{3} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2}\sqrt{3} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2}\sqrt{3} + \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2}\sqrt{3} - \frac{1}{2} \end{pmatrix}$

84. $\begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ -\frac{1}{4} & \frac{1}{4} \end{pmatrix} \cdot \begin{pmatrix} \frac{3}{2}\sqrt{2} & -\frac{1}{2}\sqrt{2} \\ \frac{3}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} 2 & -2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} \frac{3}{2}\sqrt{2} & -\frac{3}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \end{pmatrix}$

85. $\begin{pmatrix} \frac{1}{3} & -\frac{2}{3} \\ -\frac{2}{3} & \frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & -2 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} -\frac{5}{3} & -\frac{4}{3} \\ \frac{4}{3} & \frac{5}{3} \end{pmatrix}$

86. $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & 0 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{6}\sqrt{3} & \frac{1}{2} \\ \frac{1}{6} & \frac{1}{2}\sqrt{3} \end{pmatrix} \cdot \begin{pmatrix} 0 & -2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2}\sqrt{3} + \frac{1}{2} & \frac{2}{3}\sqrt{3} + \frac{1}{3} \\ -\frac{1}{2} & -\frac{1}{6}\sqrt{3} - \frac{1}{2} \end{pmatrix}$

87. $\begin{pmatrix} \frac{1}{3} & -\frac{1}{3} \\ -\frac{2}{3} & -\frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & -\frac{1}{2}\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} -\frac{2}{3}\sqrt{2} & -\frac{1}{3}\sqrt{2} \\ -\frac{1}{6}\sqrt{2} & \frac{2}{3}\sqrt{2} \end{pmatrix}$

88. $\begin{pmatrix} -\frac{1}{3} & -\frac{1}{3} \\ \frac{1}{3} & -\frac{1}{6} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 2 \\ -2 & -2 \end{pmatrix} = \begin{pmatrix} -\frac{1}{3} & -\frac{4}{3} \\ -\frac{2}{3} & \frac{1}{3} \end{pmatrix}$

89. $\begin{pmatrix} 0 & -1 \\ -\frac{1}{2} & -1 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{4}\sqrt{2} & \frac{1}{4}\sqrt{2} \\ \frac{1}{4}\sqrt{2} & \frac{1}{4}\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} 2 & -2 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -\frac{1}{4}\sqrt{2} & \frac{1}{2}\sqrt{2} \\ \frac{1}{8}\sqrt{2} & \frac{1}{4}\sqrt{2} \end{pmatrix}$

90. $\begin{pmatrix} 2 & -1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -3 & 4 \\ -2 & 3 \end{pmatrix}$

Topology of Graphs and

4.5

Surfaces

4.5.1 Connected Components of a Digraph	410
4.5.2 Cell Complexes and Boundaries	413
4.5.3 Interlude on Gluing Diagrams	418
4.5.4 Equivalent Paths	425
4.5.5 Exercises	436
4.5.6 Solutions	443

Questions to Guide Your Study:

- *What is a connected component of a digraph?*
- *How can the incidence matrix of a digraph tell us how many connected components there are?*
- *What is a cell complex and how does it generalize a digraph?*
- *What are 0-cells, 1-cells and 2-cells? What are faces?*
- *What is and how do you find the boundary of an edge? a face?*
- *What is a gluing diagram and how can you use it to help find boundaries?*
- *What is a torus? What is a Klein bottle?*
- *What is an orientable surface?*
- *What is the edge boundary map ∂_1 and the face boundary map ∂_2 ? How do you express them as matrices?*
- *What information can the face boundary map ∂_2 tell us?*
- *What does the quotient vector space $\ker(\partial_1)/\ker(\partial_2)$ tell us? If we think of it as a quotient \mathbb{Z} -module instead what additional information can we gain?*

4.5.1 Connected Components of a Digraph



Video

Imagine all of the vertices of a digraph representing basis vectors. Then, we would like to merge or combine two of these if there is an edge between them. Continuing such a process until we cannot anymore will result in only vertex remaining if there are paths of edges between from any vertex to any other. If the process results in two vertices, that means that there are two clumpings of vertices that have paths between each other but do not have any paths between the two clumpings. In that case, we would say that there are two *connected components*.

Connected Components

A connected component is a grouping of vertices such that any vertex outside this grouping is *not* connected via a path of edges to any within the grouping. Further, any two vertices in the grouping are connected via a path of edges.

Notice that what we are doing is *merging basis vectors* together. The number of basis vectors is the dimension of the vector space. So if we merge some together, we get a smaller dimension. If we merge all vertices that are connected via an edge and we keep doing this until we cannot merge anymore, the resulting dimension will be precisely the number of connected components. Now, how do we perform this merging? The idea is *quotient space magic*.

Remember that in a quotient space, we pretend that a whole subspace is equivalent to the zero vector? The subspace that we pretend is the zero vector is precisely the space spanned by things we want to be zero to make the merge that we want. For instance, suppose that the vector space with the vertices of a digraph serving as basis vectors is called V . If we would like the vertices $v_1 \in V$ and $v_2 \in V$ to be merged together, this means that we would like $v_1 = v_2$ which is the same thing as $v_1 - v_2 = 0_V$. That is, we would like $v_1 - v_2$ to be in the subspace that we will pretend acts like 0.

Now wait—if there is an edge between v_1 and v_2 , then we would like $v_1 - v_2$ to go to zero. Let's create a matrix whose range as a function includes $v_1 - v_2$. That is, if there are 5 vertices, the first column of the matrix could be

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

where we could think of the 1 in the v_1 position as referring to the tip of an arrow edge and the -1 in the v_2 position as referring to the tail. *This looks very familiar!* If we quotient V out by the range of the incidence matrix, the dimension of the resulting vector space will be the number of connected components!

Theorem 4.5.1

Let $f : E \rightarrow V$ be the function that represents the incidence matrix where E is the vector space whose basis vectors are the edges of a digraph and V is the vector space of vertices of the same graph. Then the dimension of the quotient vector space $V/f(E)$ is the number of connected components.

Now to find this dimension, we will use the following nice property:

Theorem 4.5.2

Let W be a subspace of a vector space V . Then:

$$\dim(V) = \dim(W) + \dim(V/W)$$

Proof. Let w_1, \dots, w_m be a basis for W that has dimension m . Suppose that V has dimension n . Now, take any vector $w_{m+1} \in V \setminus W$. That is w_{m+1} is in V but not in W . Now, w_1, \dots, w_m are linearly independent vectors that *do not* span

$$W_1 = \langle w_1, w_2, \dots, w_{m+1} \rangle.$$

Hence, the dimension of W_1 is larger than m . It must be $m + 1$. Continuing this process inductively, we add on one dimension each time we add a vector not in the current span until we get to V . We claim that when we change the $n - m$ appended vectors w_{m+1}, \dots, w_n into

$$w_{m+1} + W, \dots, w_n + W,$$

we get a basis for the quotient space V/W . This would show that

$$\underbrace{\dim(W)}_m + \underbrace{\dim(V/W)}_{n-m} = \underbrace{\dim(V)}_n$$

as desired.

So, let's take a look at these $n - m$ vectors in V/W . The span of these vectors includes $v + W$ for any $v \in V$. That is, they span all of V/W . So we are off to a good start. We just need to show that they are linearly independent. Remember that W is the zero vector of V/W . So let's assume that

$$a_{m+1}(w_{m+1} + W) + \cdots + a_n(w_n + W) = W$$

and show that we necessarily have that

$$a_{m+1}, \dots, a_n = 0.$$

Use the idea that $k \cdot W = W$ for any scalar k and the fact that $W + W = W$. These set operations are due to the fact that W is a vector space. These properties also allow us to assume that anything in W can behave like 0—these are properties that 0 has: $k \cdot 0 = 0$ and $0 + 0 = 0$.

So, assuming that $a_{m+1}(w_{m+1} + W) + \dots + a_n(w_n + W) = W$, gives us:

$$a_{m+1}w_{m+1} + \dots + a_nw_n \in W.$$

This tells us that:

$$a_{m+1}w_{m+1} + \dots + a_nw_n = b_1w_1 + \dots + b_mw_m$$

for some scalars b_1, \dots, b_m . Hence:

$$a_{m+1}w_{m+1} + \dots + a_nw_n - b_1w_1 - \dots - b_mw_m = 0$$

Yet since w_1, \dots, w_n are linearly independent, all of the scalars $a_{m+1}, \dots, a_n, b_1, \dots, b_m$ must be 0. That is, we have shown that a_{m+1}, \dots, a_n must all be zero just based on the assumption that a linear combination of $w_{m+1} + W, \dots, w_n + W$ with them is the “zero vector” $0_{V/W}$ in V/W . This means that these vectors are linearly independent. Therefore, they make up a basis for V/W . \square

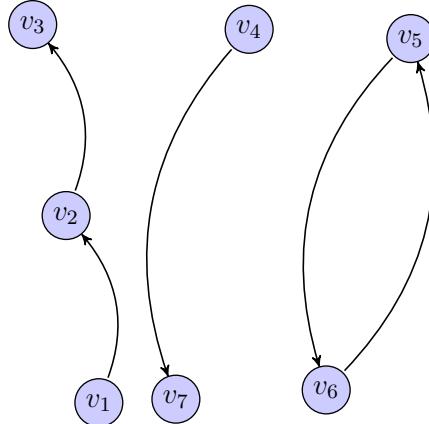
Connected Components Strategy

Suppose that $f : E \rightarrow V$ is the map describing the incidence matrix for a digraph. Then, to find the number of connected components, simply find the *range dimension* of the incidence matrix and apply the following:

$$\underbrace{\dim(V)}_{\text{number of vertices}} = \underbrace{\dim(f(E))}_{\text{range dimension}} + \underbrace{\dim(V/f(E))}_{\text{number of connected components}}$$

Let's look at an example:

Example 1. Suppose we have the following digraph:



We could come up with an incidence matrix as follows:

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

Find its Smith normal form:

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

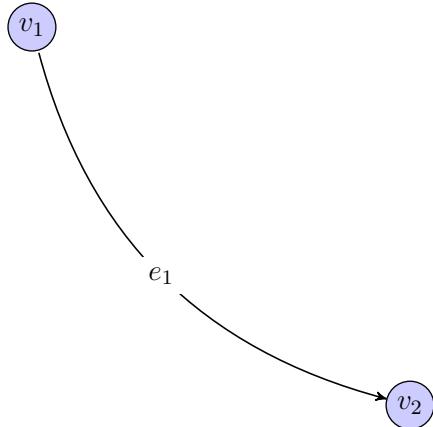
We can see by the number of 1's that the range of this incidence matrix is 4. The dimension of V is the number of vertices which is 7 (this is also the number of rows of the incidence matrix). Therefore, we compute $7 - 4 = 3$ connected components which is exactly what we saw at the beginning.

4.5.2 Cell Complexes and Boundaries

Matrix techniques can be used to explore more than just a graph of vertices and edges. We can study two-dimensional surfaces or even three-dimensional spaces and how they sit in a four-dimensional environment—even if we may not be able to visualize such a thing. But we can still have a lot of data that describes it. For our purposes we will go no further than two-dimensional surfaces. For a 2-part video example of what we will be doing in this section as it relates to the surface of a sphere, see:



First of all, let's look at a directed line segment:



The image of e_1 via the function describing the incidence matrix is $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$ or in other symbols, $v_2 - v_1$. We say that $v_2 - v_1$ is the *boundary* of e_1 . This boundary is notated as $\partial(e_1) = v_2 - v_1$. The subscript of 1 signifies that we are taking the boundary of something 1-dimensional (i.e. edges).

Boundary of an Edge

The boundary of an edge e with a tail at a vertex v and a tip at vertex w is $v - w$. We often use the notation

$$\partial_1(e) = v - w.$$

The function $\partial_1 : E \rightarrow V$ is defined to be a linear transformation. This means in particular that it is additive. Hence,

$$\partial_1(e_1 + e_2) = \partial_1(e_1) + \partial_1(e_2).$$

The function that the *incidence matrix* describes is $\partial_1 : E \rightarrow V$.

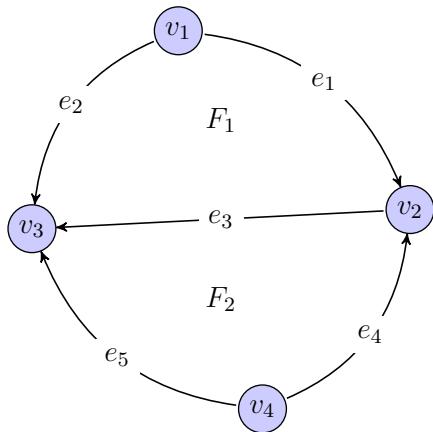
The edge e_1 with a boundary made of two vertices is called a **1-cell**. The two vertices v_1 and v_2 which make up its boundary are called **0-cells**.

Notice a 1-cell (an edge) has a boundary which is the difference of *two* 0-simplices (two points). We can think of the 1-cells as being basis vectors for a vector space E (edges) and the 0-cells as being basis vectors for a vector space V (vertices). Ok, let's go beyond vertices and edges now and talk about 2-cells, sometimes called **faces**. The goal is to generalize a digraph to something called a *cell complex*.

2-cell

A 2-cell can be loosely thought of as a piece of a flat disc (i.e. filled in circle) that has been stretched, pulled and deformed so that its outside circle boundary aligns and glues to edges that wrap around it. Often a 2-cell is called a *face*.

Faces connect edges just like edges connect vertices.



Example 2. In the diagram above, the face (2-cell) F_1 connects the three edges e_1 , e_2 and e_3 together. The face F_2 connects the three edges e_3 , e_4 , and e_5 together.

Cell Complex

A cell complex is formed with 1-cells connecting 0-cells, 2-cells connecting 1-cells, and so forth. It generalizes the notion of a digraph where edges connect vertices. This is good for studying 2-dimensional surfaces.

Vector Space of Faces

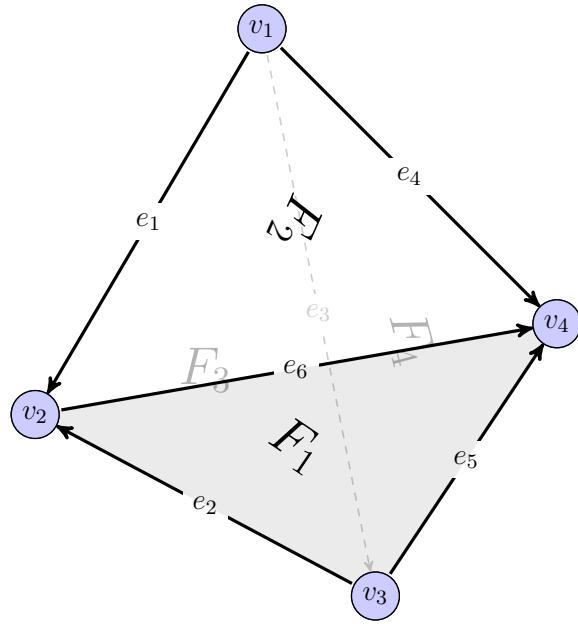
Let the individual faces (2-cells) of a cell complex represent basis vectors for a vector space F .

Just like edges have a direction, so do faces! But this time we call it an orientation. There are two possible orientations: *above or below*.

Face Orientations

We call a face positively oriented (looking at it from above) if its boundary is found by tracing out the edges it connects in a counterclockwise path. We call a face negatively oriented (looking at it from beneath) if its boundary is found by tracing out the edges it connects in a clockwise path.

We are now thinking about boundaries of a 2-cell. We will use the notation ∂_2 . The subscript of 2 reminds us that we are taking the boundary of something 2-dimensional (i.e. a 2-cell). We have that $\partial_2 : F \rightarrow E$ is a linear transformation from *faces* to *edges*. For instance, consider the following cell complex describing the outside surface of a tetrahedron. It has four faces. Two appear in front and two appear behind.



If we would like the cell complex to describe the *outside* surface of the tetrahedron, then we would like from our current outside vantage point the faces F_1 and F_2 to be positively oriented and the faces behind, F_3 and F_4 , to be negatively oriented. However, if we were to travel to the other side of the cell complex and look, this would switch. Yet still, it is customary to just imagine that the outside faces are all positively oriented and we just travel around the tetrahedron to see each face from the outside. In this interpretation, the inside walls of the tetrahedron, are all negatively oriented if we assume that our vantage point is from the outside. Hence, the 2-cells that wrap around and close up a space are often thought of as outside or inside instead of on top or beneath. Using these ideas, let's compute the boundaries of the four faces assuming a positive orientation for the outside surface. This means that we travel to a face on the outside look at it and think of going counterclockwise along its boundary. In this way, the whole surface we are thinking about (the outside) has one and only one orientation: positive.

Oriented Surface

A surface in which each 2-cell has the same orientation. By default, this orientation is assumed to be positive. This means that taking the boundary of each 2-cell when we look at it in front of us is done by traveling counterclockwise around the 2-cell.

So, now to our calculations:

$$\partial_2(F_1) = e_5 - e_6 - e_2$$

Notice that we are traveling counterclockwise around the outside of F_1 . When we traverse an edge backwards, we take its negative.

$$\partial_2(F_2) = e_1 + e_6 - e_4$$

Now let's look at the faces F_3 and F_4 . We can either travel to the other side of the tetrahedron to see a counterclockwise boundary or we can just see through to their underside and take the clockwise boundary path—this is just because they appear on the opposite side of the tetrahedron.

$$\partial_2(F_3) = e_3 + e_2 - e_1$$

$$\partial_2(F_4) = e_4 - e_5 - e_3$$

We have enough information to build a matrix for $\partial_2 : F \rightarrow E$.

$$\partial_2 : \begin{array}{c} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \end{array} \left(\begin{array}{cccc} 0 & 1 & -1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ -1 & 1 & 0 & 0 \end{array} \right) \begin{array}{c} \partial_2(F_1) \\ \partial_2(F_2) \\ \partial_2(F_3) \\ \partial_2(F_4) \end{array}$$

Face Boundary Matrix

This is the matrix for the boundary map $\partial_2 : F \rightarrow E$.

Edge Boundary Matrix

This is the matrix for the boundary map $\partial_1 : E \rightarrow V$. It is the same as the incidence matrix.

Theorem 4.5.3

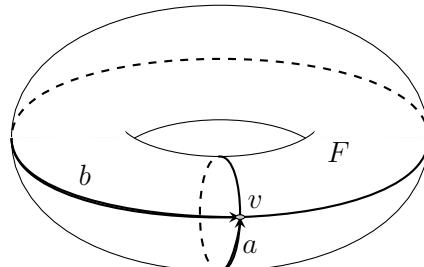
The composition $\partial_1 \circ \partial_2 : F \rightarrow V$ is simply the zero linear transformation that sends everything to 0.

Proof. A rigorous proof of this fact using definitions is left as an exercise to the reader. But it should be clear that the boundary of a face itself is like a circle which keeps going around and around and has no end. *It has no boundary.* \square

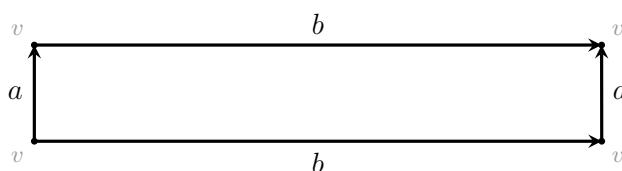
In like manner, think of a “3-cell” which is like a deformed sphere or box made up of faces on its boundary. The faces on the boundary completely close up the 3-cell. Therefore, the boundary of this boundary of faces is zero. *The boundary of the boundary is always zero for cell complexes—even as we go to successively higher and higher unseen dimensions!*

4.5.3 Interlude on Gluing Diagrams

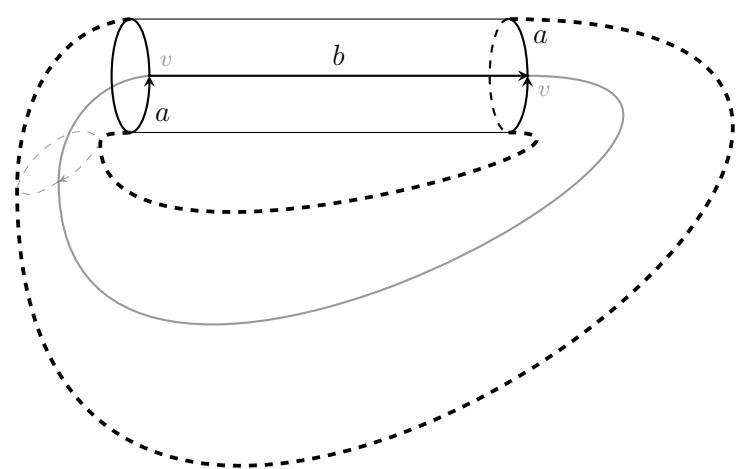
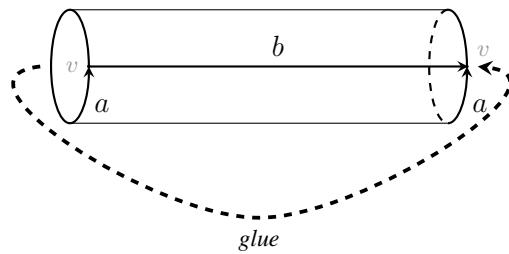
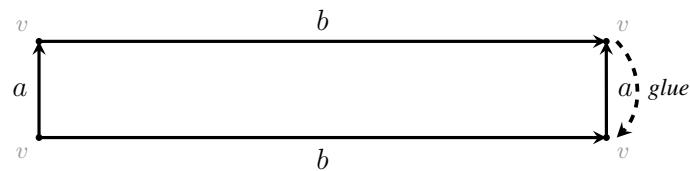
Consider the following cell complex made up of one vertex v (0-cell), two edges a and b (1-cells) and one face F (2-cell). It is called a torus (or a donut):



Conveniently, instead of having to draw out the cell complex as it appears in 3-space we can use the following *gluing diagram*:



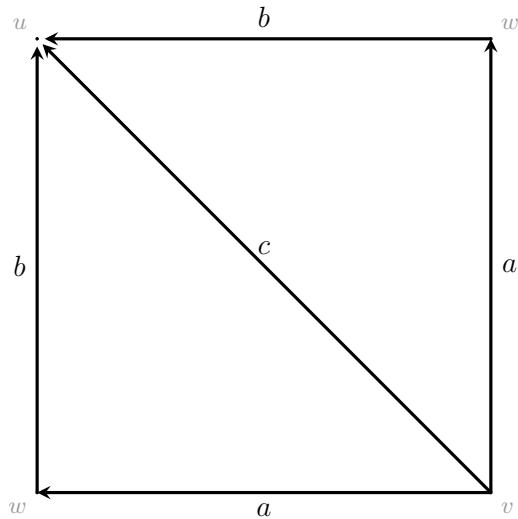
The way this diagram works is that we take a 2-cell represented by the rectangle and then we glue the arrows \xrightarrow{b} and \xleftarrow{b} together so that the tips and the tails match:



Gluing Diagram

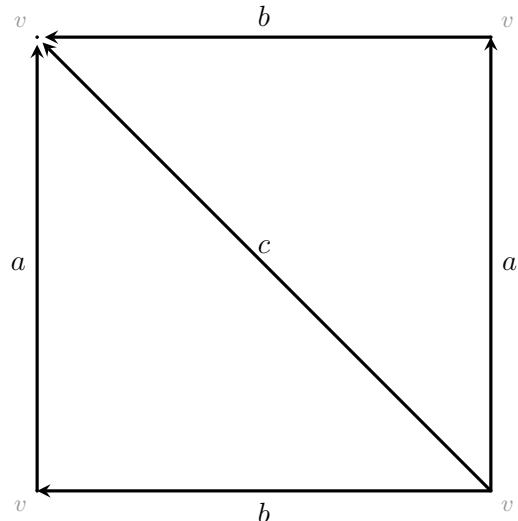
A diagram that shows how to create a cell complex from gluing pieces that are labeled the same along their arrows. *You are allowed to bend and stretch the pieces.*

Example 3. Here is a gluing diagram (after some bending) for a sphere:

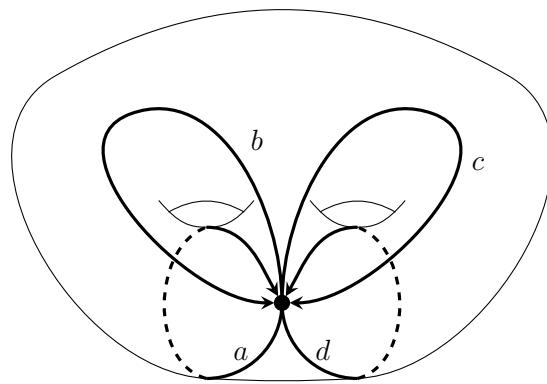


It has two 2-cells depicted as triangles and it has three 0-cells v , w , and u . Closing up, gluing the shape, and then stretching out to a sphere will reveal three distinct points v and w and u .

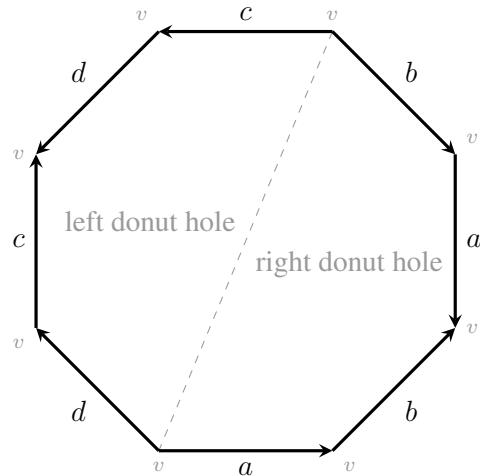
Example 4. Here is another gluing diagram for the one-holed torus (donut) that uses two 2-cells:



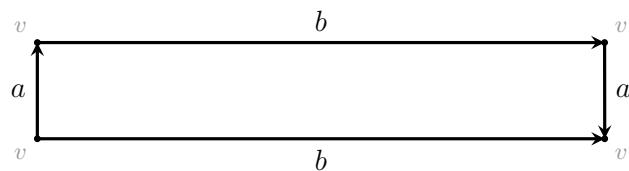
Example 5. Consider a 2-holed donut (i.e. a two-holed torus):



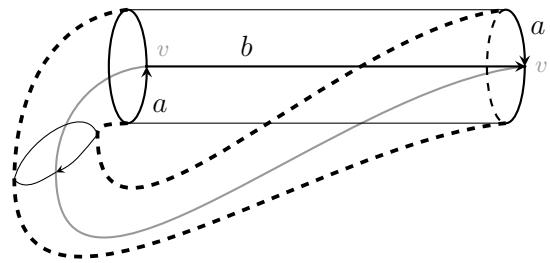
Notice that one can traverse the outside of this surface from any point off of the loops shown to any other point off of the loops shown *without ever crossing a loop*. Get a 2-holed donut and try it out if you like. The idea is that there is only one 2-cell that is glued onto these loops. A gluing diagram then would be the following:



Example 6. Now what if we took the same gluing diagram that we have for a one hole torus and switched arrow directions on two opposing sides:



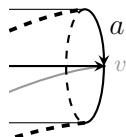
Then, upon gluing, we would have:



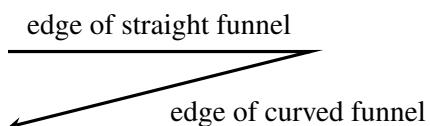
which is in contrast to how we glued for the one-holed donut (torus).

This is a little funny: we are gluing to the *other side* of the loop than we should have to get a torus. The only way to do this is to assume that we can pass the surface invisibly through the other one. If we allow for a fourth spatial dimension, this would be no problem just as a two-dimensional creature cannot pass over a circle boundary in a plane, but a three-dimensional creature can go outside of the plane to hop over. Nonetheless, we simply imagine that it can invisibly pass through. Once it is through though, we have glued it to the wrong side of the loop.

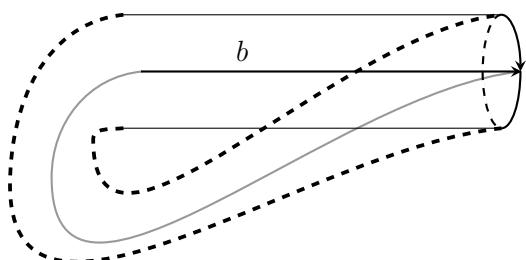
Consequences? We have *a bottle* with an opening we can put some liquid in that can pass through an extra dimension. Let's think about this opening:



The rim of the bottle is sharp:

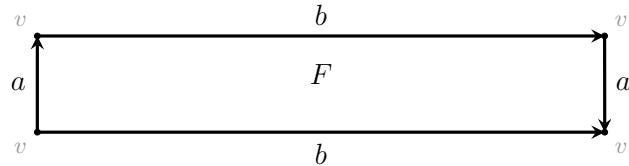


Imagine that a dimensionally capable ant follows the arrow *b*, starting at the tail of the arrow on the inside of the curved funnel:



When the ant reaches the arrow tip, it is coming out of the straight funnel and then proceeds over the rim to now be on the *outside* of the curved funnel. Again, the ant follows the arrow b —but *now on the outside of the curved funnel!* That is, this surface includes *both* sides! Underneath and on top. The gluings on the 2-cell give the 2-cell and the whole surface *both orientations!* It is like taking an infinitely thin piece of paper and thinking of both sides of the paper as being one surface. Such a surface is *nonorientable*.

Let's consider the boundary of the 2-cell F from the gluing diagram;



If we think of the 2-cell as being positively oriented with respect to this diagram (a view from overhead going counterclockwise around the boundary), we obtain starting from the lower right corner:

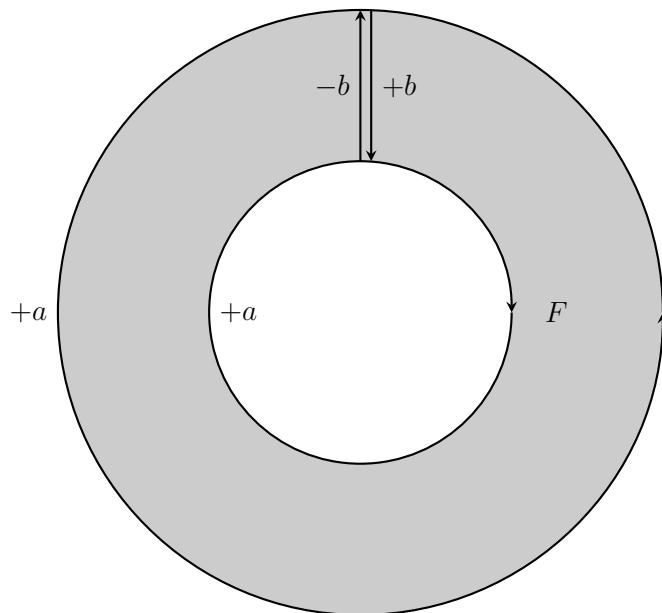
$$\partial_2(F) = -a - b - a + b = -2a$$

If we think of the 2-cell as being negatively oriented, we go clockwise:

$$\partial_2(F) = -b + a + b + a = 2a$$

Changing the sign of the image of a basis vector does not affect dimensions of range, kernel, etc. that are needed in the analysis of this funny nonorientable surface. Hence, to make the map ∂_2 work, we simply choose an orientation and stick with it.

We can think of the underside of F (i.e. the negative orientation) as being like an annulus (a disc with an inner disc removed) where the a 's are glued together so that $2a$ (running a twice) really does bound the whole surface:



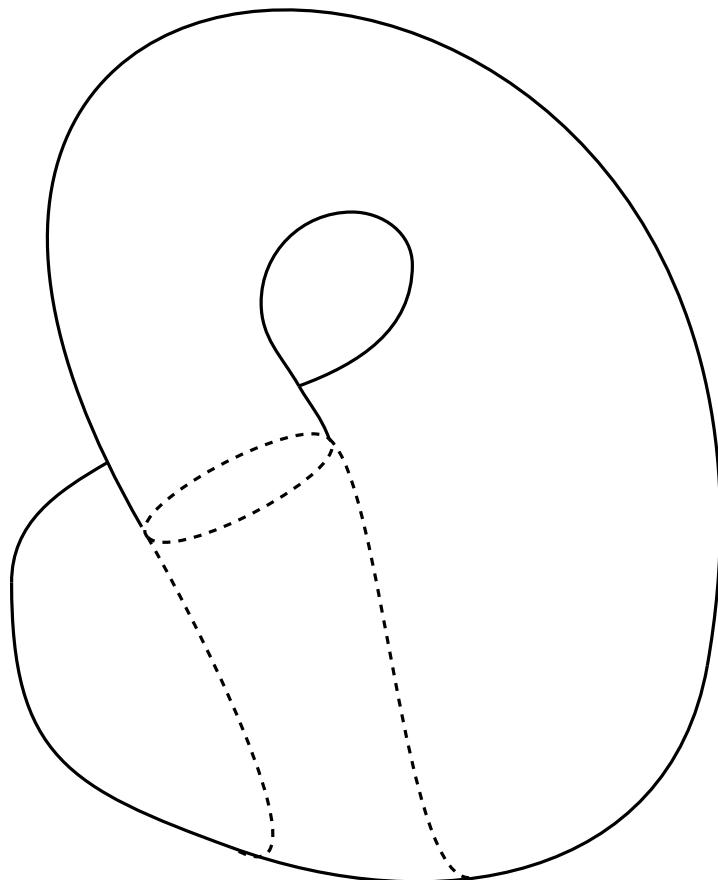
Nonorientable Surface

A surface is nonorientable if there is a 2-cell in its cell complex that can be thought of with both orientations—both sides of the 2-cell are on the surface.

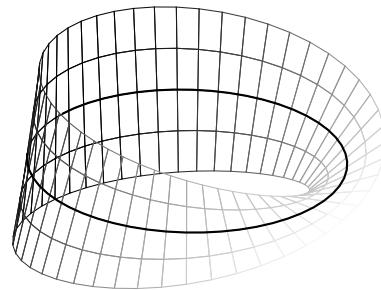
Klein Bottle

The nonorientable surface of the last example is called a *Klein bottle*.

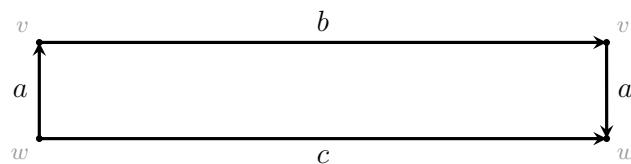
Here is a depiction of a Klein bottle with the opening at the bottom:



Example 7. A Möbius band is another example of a nonorientable surface:

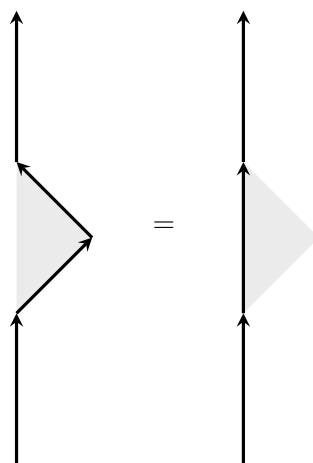


This band is formed by taking a strip of paper and twisting the ends once before gluing according to the following diagram:

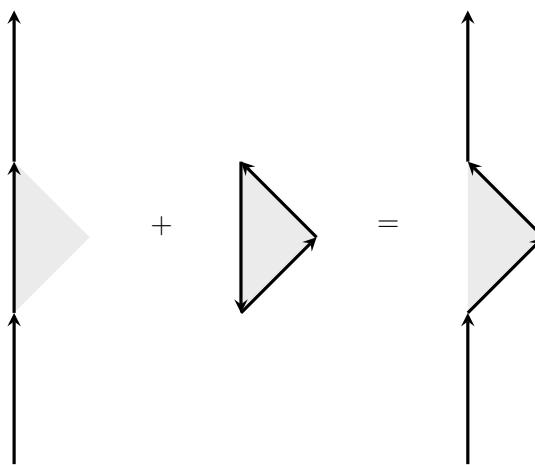


4.5.4 Equivalent Paths

No matter which cell complex structure we choose to use on a surface, one thing will always be the same: the *classes* of paths that differ by a boundary. For instance:



Both paths are considered the same because to make one path into the other, just push one part through a 2-cell. Or, think, remembering that opposite direction arrows cancel:



If we are not concerned with scaling paths by real scalars, that is fine—what about just by integers? This means we are just adding—or rather concatenating in any order—whole multiples of paths. So instead of vector spaces, which are \mathbb{R} -modules, we are dealing with **\mathbb{Z} -modules**. But we can still use matrices. Our goal is to find classes of equivalent paths on the surface. These can be used to analyze and categorize the surface.

Remember that to find the number of connected components, we found the dimension of the quotient vector space $V/\partial_1(E)$.

Now, every “vector” in the quotient \mathbb{Z} -module $E/\partial_2(F)$ (same as quotient vector space—except with different scalars) represents one of our equivalent paths on the surface. The idea is that in this quotient we pretend or rather force everything in the image $\partial_2(F)$, i.e. things that are boundaries of faces (i.e. 2-cells) to be 0—to not matter any more algebraically. Even if we were to put in a million 2-cells to consider all the paths we want, *there will be the same number of classes of equivalent paths*. This result allows us to study equivalent classes of continuous paths that can be morphed from one into the other without cutting or splitting via a *very simple cell complex structure*. We can build the matrix for ∂_2 according to *any* cell complex and be well on our way! In particular, we look at the Smith normal form. This will make sense as we work through some examples! We are scratching the surface of the study of the *topology* of surfaces.

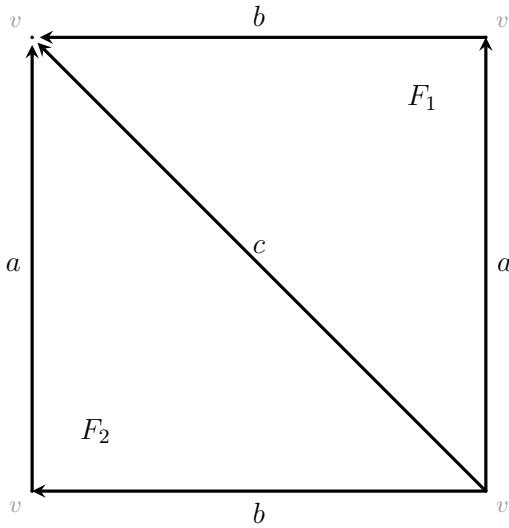
Topology

Topology is a vast topic in mathematics. For us, it suffices to say that it is the study of how to classify things according to how they continuously morph or deform. For instance, a two-holed torus cannot be morphed continuously into a one-holed donut and vice versa.

More specifically, however, one considers equivalent classes of not any paths but loops. These can be found in $\ker(\partial_1)$: \mathbb{Z} -linear combinations of edges that have 0 boundary. So, one often takes the quotient $\ker(\partial_1)/\partial_2(F)$. Yet, this is hardly necessary if in our cell complex structure we have only used *only one vertex*—then all of E is in $\ker(\partial_1)$ —every edge (1-cell) is a loop with 0 boundary!



Example 8. Let's look at the torus given by the following cell complex structure:



Notice that we only have one 0-cell. This means that all 1-cells are loops themselves. Now, let's build the matrix for ∂_2 .

$$\partial_2 : \begin{matrix} a \\ b \\ c \end{matrix} \left(\begin{array}{cc} 1 & -1 \\ 1 & -1 \\ -1 & 1 \end{array} \right) \begin{matrix} \partial_2(F_1) \\ \partial_2(F_2) \end{matrix}$$

Notice that the Smith normal form of this matrix is:

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

so that its range has dimension 1. We take $E = \langle a, b, c \rangle$ as an \mathbb{R} -vector space which has dimension 3. When we quotient by the range $\partial_2(F)$, we get that:

$$\dim(E/\partial_2(F)) = 2.$$

This corresponds to the idea that equivalent loops are built from ones like a and like b . For instance, we could go around the circumference of the donut hole (b) 3 times and then go around a loop that goes through the donut hole and then back around 4 times. Such a path would be represented by $3b + 4a$. The classes of paths

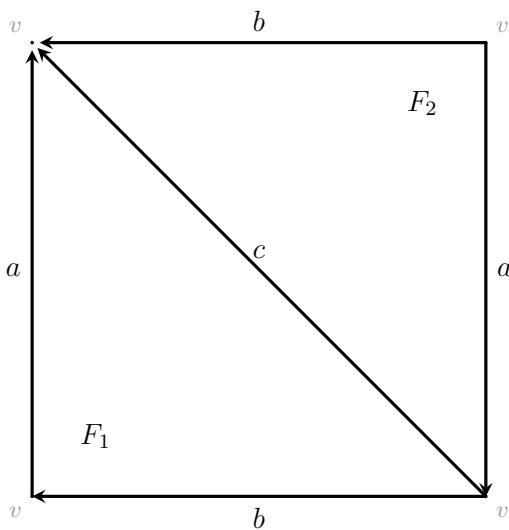
only depend on two linearly independent paths.

But there is something important to remember: this Smith normal form is achievable by only using integer scalings! Also, $3b + 4a$ is like $(3, 4) \in \mathbb{Z}^2$. So we are thinking of E , F and $E/\partial_2(F)$ as \mathbb{Z} -modules. We are studying the different ways we can wrap a string around the donut before tying together the beginning of the string with the end. This is done with whole number of wrappings. To reverse a wrapping is take its negative—so indeed this really is information about a \mathbb{Z} -module. The only thing we need to be careful about is to only use \mathbb{Z} -module row operations and column operations! The word *dimension* is now replace by the word \mathbb{Z} -rank.

To get path information, use only operations which involve scalars in \mathbb{Z} .

Let's see an example where this is useful:

Example 9. Let's study equivalent loops on the Klein bottle given by the following gluing diagram:



$$\partial_2 : \begin{array}{c} a \\ b \\ c \end{array} \left(\begin{array}{cc} 1 & -1 \\ 1 & 1 \\ -1 & -1 \end{array} \right)$$

$$\partial_2(F_1) \quad \partial_2(F_2)$$

By only performing row operations with scalars in \mathbb{Z} we obtain:

$$\begin{array}{c}
 \left(\begin{array}{cc} 1 & -1 \\ & (-1 \cdot 1) \\ 1 & 1 \\ & (-1 \cdot (-1)) \\ -1 & -1 \end{array} \right) \longrightarrow \left(\begin{array}{cc} 1 & -1 \\ & (+1 \cdot 1) \\ 0 & 2 \\ & (+1 \cdot (-1)) \\ -1 & -1 \end{array} \right) \longrightarrow \\
 \left(\begin{array}{cc} 1 & -1 \\ 0 & 2 \\ 0 & 0 \end{array} \right)
 \end{array}$$

Now, we perform only one column operation to achieve what we can for Smith normal form with scalars in \mathbb{Z} :

$$\left(\begin{array}{cc} 1 & -1 \\ 0 & 2 \\ 0 & 0 \end{array} \right) \longrightarrow \left(\begin{array}{cc} 1 & 0 \\ 0 & 2 \\ 0 & 0 \end{array} \right)$$

This tells us that our column operations matrix is

$$c : \mathbb{Z}^2 \rightarrow F \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Remember that we want the image of ∂_2 to behave like 0 in the quotient $E/\partial_2(F)$. We call all these images boundaries—paths that represent boundaries are the ones that behave like 0 in this quotient. In particular, it takes the first column $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ of c which stands for $1 \cdot F_1 + 0 \cdot F_2 = F_1$ and sends it to $a + b - c$ which is a boundary.

It also takes the second column of c , $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ which stands for $F_1 + F_2$ and sends it to $\underbrace{(a + b - c)}_{\partial_2(F_1)} + \underbrace{(-a + b - c)}_{\partial_2(F_2)} = 2b - 2c$ which is considered to be a boundary.

This boundary $2b - 2c = 2(b - c)$ is double the path $b - c$. Now, the path $b - c$ is actually equivalent to $-a$ since

$$a + b - c \underset{\text{as paths}}{\sim} 0$$

$$b - c \underset{\text{as paths}}{\sim} -a$$

So $-a$ and consequently a itself when doubled is a boundary. *But we already saw this in a previous example with a simpler cell complex for the Klein bottle!*

The Smith normal form is a map $r \circ \partial_2 \circ c$. Let's think isomorphically about the classes of equivalent paths which can be thought of as elements of the **quotient \mathbb{Z} -module** $E/\partial_2(F)$. The row operations map $r : E \rightarrow \mathbb{Z}^3$ is an isomorphism. This same isomorphism helps us change our view of $E/\partial_2(F)$.

Remember that a quotient \mathbb{Z} -module is the same as a quotient vector space except all the rescalings must be from \mathbb{Z} *starting* with standard basis vectors. There is no way to get $(\pi, \sqrt{3})$ from \mathbb{Z} -linear combinations of $e_1 = (1, 0)$ and $e_2 = (0, 1)$. All \mathbb{Z} -modules that are generated via linear combinations of 2 things turn out to look a lot like a quotient of \mathbb{Z}^2 —that is, chunks in \mathbb{Z}^2 are the pieces we are considering. Isomorphisms of \mathbb{Z} -modules are the same as isomorphisms of vector spaces *except* we only require that the isomorphism function be scalable with respect to integers.

We are talking about an isomorphic picture of the quotient \mathbb{Z} -module $E/\partial_2(F)$ via the **isomorphism** r . Indeed, r itself *induces* the following isomorphism sending chunks in one quotient to chunks in the other:

$$\mathbb{Z}^3/r(\partial_2(F)) \xleftarrow{r} E/\partial_2(F)$$

This is how r acts on chunks:

$$r\left((k_1, k_2, k_3) + \partial_2(F) \right) = r(k_1, k_2, k_3) + r(\partial_2(F))$$

This means that we can focus on

$$\mathbb{Z}^3/r(\partial_2(F))$$

to “see” the classes on equivalent paths. The Smith normal form tells us precisely what $r(\partial_2(F))$ is since c itself is surjective onto all of F . So we have that $r(\partial_2(F))$ is the same as

$$\text{range(Smith normal form)} = \underbrace{\langle (1, 0, 0), (0, 2, 0) \rangle}_{\text{Span of the columns}}.$$

This means in our isomorphic view point in \mathbb{Z}^3 that $(1, 0, 0) = e_1$ should be thought of as a zero element and $(0, 2, 0) = 2e_2$ should also be thought of as a zero element. What does this leave us to be nonzero?

$$ke_2 \quad (\text{where } k \text{ is an odd integer}) \quad \text{and} \quad e_3$$

In fact, $ke_2 = (k+2)e_2$ since $(k+2)e_2 - ke_2 = 2e_2 = 0$. This means by induction that all odd loops of e_2 are actually considered to be the same loop—you can unravel the loops into each other. So, we could say that the quotient \mathbb{Z} -module $E/\partial_2(F)$ behaves like pairs

$$\underbrace{(\text{odd or even wraps one way}, \text{different numbers of wraps another way})}_{\begin{array}{c} 0=\text{even} \\ 1=\text{odd} \end{array}} \underbrace{\mathbb{Z}}_{\mathbb{Z}}$$

As a Cartesian product, this looks like:

$$\{0, 1\} \times \mathbb{Z}$$

There are different ways of notating $\{0, 1\}$. We can think of it as the quotient \mathbb{Z} -module $\mathbb{Z}/2\mathbb{Z}$ where our two chunks are evens = $2\mathbb{Z}$ or a shift of evens by 1 (i.e. odds) = $1 + 2\mathbb{Z}$. We could also think of it as \mathbb{F}_2 which we considered when we were looking at examples of fields. We will use:

$$\mathbb{Z}/2\mathbb{Z}$$

The group $\mathbb{Z}/2\mathbb{Z}$ is the set $\{0, 1\}$ with the additions:

$$0 + 0 = 1 \quad 0 + 1 = 1 + 0 = 1 \quad 1 + 1 = 0$$

Isomorphically, every equivalent path according to our cell complex can be thought of as an element in this \mathbb{Z} -module $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Since there is only one free \mathbb{Z} in the set cartesian product \times , we say that the free \mathbb{Z} -rank (instead of using the word *dimension*) is 1. This type of \mathbb{Z} -module cannot be thought of as a \mathbb{R} -vector space without eliminating $\mathbb{Z}/2\mathbb{Z}$ (which is the same thing as \mathbb{F}_2). So, sometimes going to scalars in \mathbb{R} causes us to lose valuable information about the equivalence classes of paths.

This $\mathbb{Z}/2\mathbb{Z}$ is kind of fun: odd number of wraps in one way on the surface can all be unraveled into the same wrap and all even numbers in that way can be undone completely!

We talk about equivalent paths when we treat the image of ∂_2 as 0. We talk about equivalent points (i.e. connected by a series of edges) when we treat the image of ∂_1 as 0. *Connected components are like classes of equivalent points!* So...does this go further???

Though not important for our purposes, we introduce some terminology for the reader that is interested in exploring further. We call the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ of the last example the *first homology group* of the cell complex for the Klein bottle. Remember that E itself in our example only consisted of loops. This ensured that $E = \ker(\partial_1)$ which is necessary for the quotient $E/\partial_2(F)$ to be given this name. In general:

Homology Groups

Given a cell complex with \mathbb{Z} -modules C_n corresponding to a \mathbb{Z} -module with \mathbb{Z} -basis given by the n -cells, we can create boundary maps:

$$\cdots \longrightarrow C_3 \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\partial_0} \{0\}$$

where ∂_0 is the map that sends everything to the only element in its codomain: 0. We define the n th homology group as the \mathbb{Z} -module quotient:

$$\ker(\partial_n)/\partial_{n+1}(C_{n+1})$$

We note that we have two equivalent notations for range: $\partial_{n+1}(C_{n+1}) = \text{range}(\partial_{n+1})$.

Example 10. For a cell complex, the 0th homology group is $C_0/\text{range}(\partial_1)$. The free-rank (i.e. like dimension) of this quotient \mathbb{Z} -module is the number of connected components. In this case, $C_0 = V$ and ∂_1 can be described by the incidence matrix.

Different Complexes Yet the Same Homology

Homology groups for cell complexes that represent the same object always coincide isomorphically! This means that we could have used a different cell complex for the Klein bottle and we would have gotten the same first homology group! This goes along with the idea of “equivalent paths” that can morph or unravel into each other. Different Cell Complexes just explore different paths which could be equivalent to ones in other complexes.

Homology groups are useful for categorizing all kinds of high dimensional objects—not only geometric objects, but a plethora of abstract objects. These are abstract objects for which you can associate not a cell complex necessarily, but a series of groups with a series of boundary maps such that composing two consecutive maps together gives you the constant 0 function. Mathematicians use homology groups to discover relationships between all kinds of mathematical ideas. This is just one of the many uses of *linear algebra*!

A thorough study of homology groups is beyond the scope of this text. The interested reader is encouraged to explore this topic further. See [11].

Key Concepts from this Section

- **connected components:** (page 410) A connected component is a grouping of vertices such that any vertex outside this grouping is *not* connected via a path of edges to any within the grouping. Further, any two vertices in the grouping are connected via a path of edges.

- **theorem 4.5.1 :** (page 410) Let $f : E \rightarrow V$ be the function that represents the incidence matrix where E is the vector space whose basis vectors are the edges of a digraph and V is the vector space of vertices of the same graph. Then the dimension of the quotient vector space $V/f(E)$ is the number of connected components.
- **theorem 4.5.2 :** (page 411) Let W be a subspace of a vector space V . Then:

$$\dim(V) = \dim(W) + \dim(V/W)$$

- **connected components strategy:** (page 412) Suppose that $f : E \rightarrow V$ is the map describing the incidence matrix for a digraph. Then, to find the number of connected components, simply find the *range dimension* of the incidence matrix and apply the following:

$$\underbrace{\dim(V)}_{\text{number of vertices}} = \underbrace{\dim(f(E))}_{\text{range dimension}} + \underbrace{\dim(V/f(E))}_{\text{number of connected components}}$$

- **∂ :** (page 414) The symbol ∂_1 is used to denote the idea of taking the boundary of an edge. The subscript of 1 signifies that we are taking the boundary of something 1-dimensional (i.e. edges).
- **boundary of an edge:** (page 414) The boundary of an edge e with a tail at a vertex v and a tip at vertex w is $v - w$. We often use the notation

$$\partial_1(e) = v - w.$$

The function $\partial_1 : E \rightarrow V$ is defined to be a linear transformation. This means in particular that it is additive. Hence,

$$\partial_1(e_1 + e_2) = \partial_1(e_1) + \partial_1(e_2).$$

The function that the *incidence matrix* describes is $\partial_1 : E \rightarrow V$.

- **1-cell:** (page 414) A 1-cell is an edge (which is *one*-dimensional).
- **0-cells:** (page 414) A 0-cell is just a vertex (a point).
- **faces:** (page 414) A face is a 2-cell in a cell complex.
- **2-cell:** (page 414) A 2-cell can be loosely thought of as a piece of a flat disc (i.e. filled in circle) that has been stretched, pulled and deformed so that its outside circle boundary aligns and glues to edges that wrap around it. Often a 2-cell is called a *face*.

- **cell complex:** (page 415) A cell complex is formed with 1-cells connecting 0-cells, 2-cells connecting 1-cells, and so forth. It generalizes the notion of a digraph where edges connect vertices. This is good for studying 2-dimensional surfaces.
- **vector space of faces:** (page 415) Let the individual faces (2-cells) of a cell complex represent basis vectors for a vector space F .
- **face orientations:** (page 415) We call a face positively oriented (looking at it from above) if its boundary is found by tracing out the edges it connects in a counterclockwise path. We call a face negatively oriented (looking at it from beneath) if its boundary is found by tracing out the edges it connects in a clockwise path.
- **oriented surface:** (page 416) A surface in which each 2-cell has the same orientation. By default, this orientation is assumed to be positive. This means that taking the boundary of each 2-cell when we look at it in front of us is done by traveling counterclockwise around the 2-cell.
- **face boundary matrix:** (page 417) This is the matrix for the boundary map $\partial_2 : F \rightarrow E$.
- **edge boundary matrix:** (page 417) This is the matrix for the boundary map $\partial_1 : E \rightarrow V$. *It is the same as the incidence matrix.*
- **theorem 4.5.3 :** (page 418) The composition $\partial_1 \circ \partial_2 : F \rightarrow V$ is simply the zero linear transformation that sends everything to 0.
- **gluing diagram:** (page 419) A diagram that shows how to create a cell complex from gluing pieces that are labeled the same along their arrows. *You are allowed to bend and stretch the pieces.*
- **nonorientable surface:** (page 424) A surface is nonorientable if there is a 2-cell in its cell complex that can be thought of with both orientations—both sides of the 2-cell are on the surface.
- **klein bottle:** (page 424) The nonorientable surface of the last example is called a *Klein bottle*.
- **\mathbb{Z} -modules:** (page 426) A \mathbb{Z} -module is the same as a vector space except that the scalars are in \mathbb{Z} which is not a field—so that there are some rescalings which are nonreversible.
- **topology:** (page 426) Topology is a vast topic in mathematics. For us, it suffices to say that it is the study of how to classify things according to how they continuously morph or deform. For instance, a two-holed torus cannot be morphed continuously into a one-holed donut and vice versa.
- **quotient \mathbb{Z} -module:** (page 430) Remember that a quotient \mathbb{Z} -module is the same as a quotient vector space except it all the rescalings must be from \mathbb{Z} and that we *start* with standard basis vectors. There is no way to get $(\pi, \sqrt{3})$ from \mathbb{Z} -linear combinations of $e_1 = (1, 0)$ and $e_2 = (0, 1)$. All \mathbb{Z} -modules that are generated via linear combinations of 2 things turn out to look a lot like a quotient of \mathbb{Z}^2 —that is, chunks in \mathbb{Z}^2 are the pieces we are considering.

- **isomorphism:** (page 430) Isomorphisms of \mathbb{Z} -modules are the same as isomorphisms of vector spaces except we only require that the isomorphism function be scalable with respect to integers.
- **$\mathbb{Z}/2\mathbb{Z}$:** (page 431) The group $\mathbb{Z}/2\mathbb{Z}$ is the set $\{0, 1\}$ with the additions:

$$0 + 0 = 1 \quad 0 + 1 = 1 + 0 = 1 \quad 1 + 1 = 0$$

- **homology groups:** (page 431) Given a cell complex with \mathbb{Z} -modules C_n corresponding to a \mathbb{Z} -module with \mathbb{Z} -basis given by the n -cells, we can create boundary maps:

$$\dots \longrightarrow C_3 \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\partial_0} \{0\}$$

where ∂_0 is the map that sends everything to the only element in its codomain: 0. We define the n th homology group as the \mathbb{Z} -module quotient:

$$\ker(\partial_n)/\partial_{n+1}(C_{n+1})$$

We note that we have two equivalent notations for range: $\partial_{n+1}(C_{n+1}) = \text{range}(\partial_{n+1})$.

- **different complexes yet the same homology:** (page 432) Homology groups for cell complexes that represent the same object always coincide isomorphically! This means that we could have used a different cell complex for the Klein bottle and we would have gotten the same first homology group! This goes along with the idea of “equivalent paths” that can morph or unravel into each other. Different Cell Complexes just explore different paths which could be equivalent to ones in other complexes.

4.5.5 Exercises

Connected Components

1. Suppose that an incidence matrix for a digraph with 1000 vertices has rank 264. How many connected components does the digraph have?
2. Suppose that a digraph with 1,000,000 vertices has 312 connected components. What is the rank of the incidence matrix?

Use the Smith normal form of the given incidence matrix to determine how many connected components there are of the associated digraph.

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

4.
$$\begin{pmatrix} -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

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

6.
$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

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

8.
$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

9.
$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

10.
$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

11.
$$\begin{pmatrix} -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

12.
$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

13.
$$\begin{pmatrix} -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

14.
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

15.
$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

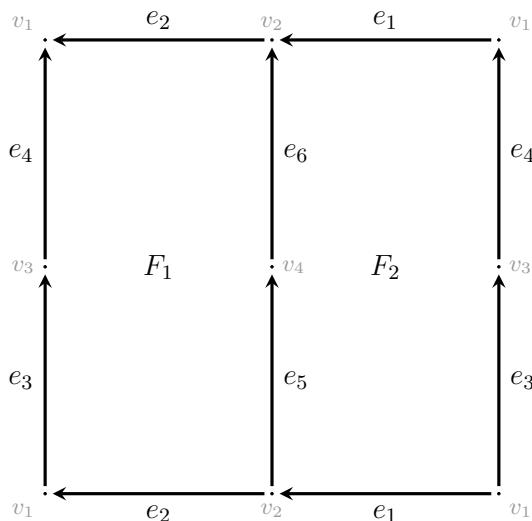
16.
$$\begin{pmatrix} -1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

17.
$$\begin{pmatrix} -1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

18.
$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{pmatrix}$$

Finding Matrices for ∂_1 and ∂_2

19. Consider the following cell complex structure of the torus:



- (a) Compute the matrix for ∂_1 (i.e. the incidence matrix).
- (b) Find the Smith normal form of this matrix for ∂_1 .
- (c) Use this Smith normal form to verify that the number of connected components is 1. That is, a torus is a connected object: *you can travel on the torus from one place to any other on the torus.*

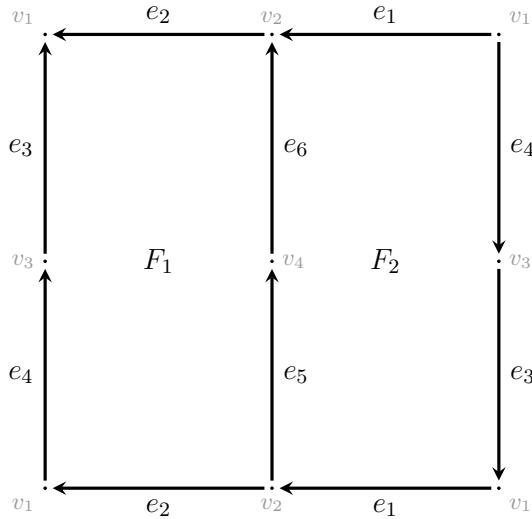
- (d) Compute the reduced row echelon form of the matrix for ∂_1 .
- (e) Use the column shortcut for finding a basis for the kernel of ∂_1 . You should get:

$$a = (1, 1, 0, 0, 0, 0) \quad b = (0, 0, 1, 1, 0, 0) \quad c = (0, 0, 0, 0, 1, 1)$$

- (f) Compute the matrix for ∂_2 .
- (g) Notice that only one vector spans the range of ∂_2 . Show that this vector can be written as $b - c$.
- (h) Explain why $\{a, c, b - c\}$ forms a basis for $\ker(\partial_1)$.

- (i) Use this last basis to illustrate why the chunk elements in the quotient vector space $\ker(\partial_1)/\text{range}(\partial_2)$ can be indexed by pairs $(k_1, k_2)_{ac} = k_1a + k_2c$. Since all of our work could have been done with operations *only using rescaling in \mathbb{Z}* , this verifies *even from this complex of the torus* that the equivalent classes of windings around the donut come from two independent windings: around the circumference of the hole *and* windings that go through the hole just as in the reading when we used a different complex.

- 20.** Consider the following cell complex of the Klein bottle which is similar to the cell complex of the last exercise:



- (a) Show that the kernel of ∂_1 is spanned by the same vectors

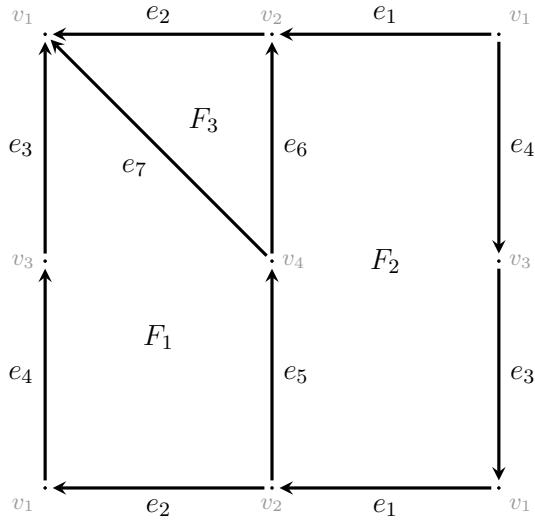
$$a = (1, 1, 0, 0, 0, 0) \quad b = (0, 0, 1, 1, 0, 0) \quad c = (0, 0, 0, 0, 1, 1)$$

as in the last exercise.

- (b) Verify that $\{a, b - c, c\}$ forms a \mathbb{Z} -basis for $\ker(\partial_1)$ thought of as a \mathbb{Z} -module.

- (c) Show that $\text{range}(\partial_2)$ has a \mathbb{Z} -basis of $\{b + c, b - c\}$.
- (d) Since $b + c$ and $b - c$ are linearly independent and $c = \frac{1}{2}(b + c) - \frac{1}{2}(b - c)$, explain why c is not in the \mathbb{Z} -span of $\{b + c, b - c\}$ but that $2c$ is the minimal multiple of c that is.
- (e) Explain why the \mathbb{Z} -module quotient $\ker(\partial_1)/\text{range}(\partial_2)$ can be thought of as $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Note that this is the same result that we got in the reading for a different cell complex for the Klein-bottle.

21. Consider the following modification to the cell complex for the Klein bottle:



- (a) Find the matrix for ∂_1 .
- (b) Find the reduced row echelon form of ∂_1 .
- (c) Show that a basis for $\ker(\partial_1)$ is:
- $$a = (1, 1, 0, 0, 0, 0, 0) \quad b = (0, 0, 1, 1, 0, 0, 0) \quad c = (0, 0, 0, 0, 1, 1, 0) \quad d = (1, 0, 0, 0, 1, 0, 1)$$
- (d) Find the matrix for ∂_2 .
- (e) Verify that the columns of ∂_2 are $d - a - b$, $-b - c$ and $a + c - d$. These vectors make up a \mathbb{Z} -basis for $\text{range}(\partial_2)$.
- (f) Show that $\{a, d - a - b, b, a + c - d\}$ makes a \mathbb{Z} -basis for $\ker(\partial_1)$.
- (g) Verify that b cannot be written as a \mathbb{Z} -linear combination of $d - a - b$, $-b - c$ and $a + c - d$ but that $2b$ can. You can find a linear combination in \mathbb{R} that is not in \mathbb{Z} and use the uniqueness of the linear independence.
- (h) Explain how just like we had in the last exercise that the \mathbb{Z} -module quotient $\ker(\partial_1)/\text{range}(\partial_2)$ can be thought of as $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We always get this same result for the Klein bottle no matter the cell complex!

Proof Practice and a Fun Fact

22. All digraphs with finitely many edges and vertices with the additional condition that you can place them flat on a plane *without any edges crossing* can also be put flat on a ball without any edges crossing. This gives a cell complex with faces for a sphere. One face is the “outside” of the digraph. **Let’s for now, just take our scalars in \mathbb{R} so we will be working with \mathbb{R} -vector spaces.**

- (a) Choose an appropriate cell complex for a sphere. Show that $\ker(\partial_1) = \text{range}(\partial_2)$. This relationship will hold for *any* cell complex describing a sphere! This is because homology groups of a sphere do not depend on the specific cell complex structure—just that the cell complex describes a sphere.
- (b) Suppose that you take a digraph with finitely many edges and vertices. Assume that the edges and vertices *are not glued but distinct*—this is a digraph. Further, suppose that the digraph can be pictured on a plane such that no edge crosses any other edge so that the edges form boundaries of distinct regions of the plane. Now take this digraph and paste it on the surface of a sphere. All edges and points are distinct. The regions of the sphere are now 2-cells, the edges are 1-cells and the points are 0-cells. We have a cell complex for a sphere. Let C be the collection of all 2-cells *except* for the one that describes the region that is *outside*—that is, since the digraph is finite, when it was in the plane, the infinite region outside the digraph has now become a 2-cell on the sphere. So then with this outer face removed, we have C . Prove that the collection:

$$\{\partial_2(r) : r \in C\}$$

spans $\text{range}(\partial_2)$. You just have to explain why $\partial_2(\text{outer face})$ is in the span of this $\{\partial_2(r) : r \in C\}$.

- (c) Prove that $\{\partial_2(r) : r \in C\}$ is a set of linearly independent vectors. Proceed by *induction* as you build the digraph creating *just* one more face (2-cell) at a time remembering that no edges are glued together. Describe how you can proceed in such a way that you have to add a new edge each time a face is added. Let r_n be the n th 2-cell that you have joined as you build your collection toward C . Assume that $\{r_1, \dots, r_n\}$ is a linearly independent collection. Realize that r_{n+1} uses an edge that has not been used before. That edge is linearly independent to the other edges that are being used. Hence, a linear combination with $\{r_1, \dots, r_n, r_{n+1}\}$ that equals the zero vector must have 0 as the scalar coefficient of r_{n+1} because we know that r_{n+1} cannot be in the span of $\{r_1, \dots, r_n, r_{n+1}\}$. There is not much more to do! Why must all the other scalar coefficients be 0? What is the base case?
- (d) Let n_v be the number of vertices for the digraph, n_e be the number of edges and n_f the number of faces (2-cells) in our cell complex. Then, use what we have shown so far to conclude that

$$\dim(\ker(\partial_1)) = n_f - 1$$

- (e) Use any appropriate cell complex for a sphere and show that $\dim(V/\text{range}(\partial_1)) = 1$. *This is true for any cell complex describing a sphere—by our fact about homology groups!* Use this fact to conclude

that

$$\dim(\text{range}(\partial_1)) = n_v - 1$$

- (f) Now we know that the dimension of the kernel and the dimension of the range of ∂_1 add together to equal the number of columns of the incidence matrix (i.e. the matrix for ∂_1). Remember how this worked with the Smith normal form. The number of columns in the incidence matrix is equal to n_e . Use these ideas to prove Euler's Characteristic Formula for digraphs that can be drawn in a plane without any crossings (called *planar graphs*) as we have described:

$$n_f - n_e + n_v = 2.$$

This formula allows one to check to see if a digraph can't be drawn in the plane without any crossings! This formula can be used to prove theorems that describe colorings in map making.

4.5.6 Solutions

- 1.** Let f be the map which the incidence matrix describes and V the vector space spanned by the vertices as basis elements. Then the number of connected components is:

$$\dim(V/\text{range}(f)) = \underbrace{1000}_{\text{number of vertices}} - \underbrace{264}_{\dim(\text{range}(f))} = 736$$

- 2.** Let f be the map which the incidence matrix describes and V the vector space spanned by the vertices as basis elements. Then, the number of connected components (312) is equal to

$$\dim(V/\text{range}(f)) = \underbrace{\dim(V)}_{1,000,000} - \underbrace{\dim(\text{range}(f))}_{\text{rank}}$$

This implies that the rank is: 999,688.

3. 3

4. 3

5. 4

6. 5

7. 4

8. 4

9. 5

10. 3

11. 4

12. 4

13. 3

14. 4

15. 5

16. 4

17. 2

18. 3

19. Solutions/hints by parts:

$$(a) \begin{pmatrix} -1 & 1 & -1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

$$(b) \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- (c) The rank of the Smith normal form is 3. The number of vertices is 4. Hence, the number of connected components is $4 - 3 = 1$.

$$(d) \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- (e) There are three nonpivot columns. Extending and changing these by the trick gives the result.

$$(f) \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ -1 & 1 \\ -1 & 1 \\ 1 & -1 \\ 1 & -1 \end{pmatrix}$$

- (g) Look at the second column: this is $b - c$. The first column is just the negative of this.

- (h) Notice that these three vectors span $\langle a, b, c \rangle$ which has dimension 3 so they must be a basis. In particular: $(b - c) + c = b$ so that $b \in \langle a, c, b - c \rangle$.
- (i) Lets describe the chunk that an element $k_1a + k_2c + k_3(b - c) \in \ker(\partial_1)$ lies in: it lies in the chunk $k_1a + k_2c + \langle b - c \rangle$. This chunk can be indexed as (k_1, k_2) .

20. Solutions/hints by parts:

- (a) The matrix for ∂_1 is the same as in the last exercise *except* the third and fourth columns are negated. The reduced row echelon form for the matrix for ∂_1 is the same as in the last exercise so the column trick yields the same basis for the kernel.
- (b) You just need an integer linear combination (i.e. the scalars are integers) to get b : $1 \cdot (b - c) + 1 \cdot c = b$.

(c) You can get this from the matrix for ∂_2 :

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

- (d) The scalars that we used are unique in \mathbb{R} to give us c by linear independence. Since $\mathbb{Z} \subset \mathbb{R}$, there is no possible way to get c as a linear combination of $b + c$ and $b - c$. The smallest number we can multiply both sides by to get integer scalars is 2. Hence, $2c$ is the minimal multiple of c that is in the \mathbb{Z} -span of $b + c$ and $b - c$.
- (e) Note that $\text{range}(\partial_2)$, as a \mathbb{Z} -module, is spanned by $b + c$ and $b - c$. In the quotient $\ker(\partial_1)/\text{range}(\partial_2)$, this span is thought of as 0. Remember that $\ker(\partial_1)$ has $\{a, b - c, c\}$ as a \mathbb{Z} -basis. Let's go through these and see how things change when the \mathbb{Z} -span of $b + c$ and $b - c$ becomes 0. The vector a and all \mathbb{Z} -multiples of it are not in this span and so remain nonzero. The vector $b - c$ is in this span and so disappears (i.e. equals 0). The vector c is not in this span and so remains nonzero—but all even multiples of it are. All odd multiples therefore become c since $(2k+1) \cdot c = \underbrace{2k \cdot c}_0 + c$. This means that the quotient is looking like the set addition $\mathbb{Z} \cdot a + \{0, c\}$. We can describe this set addition in terms of pairs (coefficient of a paired with the coefficient of c) to look like: $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

21. Solutions/hints by parts:

(a)
$$\begin{pmatrix} -1 & 1 & 1 & -1 & 0 & 0 & 1 \\ 1 & -1 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & -1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- (c) There are four nonpivot columns. Extending and changing these by the trick gives the result.

(d)
$$\begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 1 \\ -1 & -1 & 0 \\ -1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}$$

- (e) This can be done with direct computation of $d - a - b$, $-b - c$ and $a + c - d$.
- (f) Note that $b = -\frac{1}{2} \cdot (d - a - b) - \frac{1}{2} \cdot (-b - c) + \frac{1}{2} \cdot (a + c - d)$.
- (g) Think of the basis for $\ker(\partial_1)$ as $\{a, d - a - b, b, a + c - d\}$. In the quotient with $\text{range}(\partial_2)$ which is spanned by $d - a - b$, $-b - c$ and $a + c - d$, we have that $d - a - b$ and $a + c - d$ vanish. We also know that $2b$ vanishes since $2b$ is in the \mathbb{Z} -span of these vectors. But b is not in the \mathbb{Z} -span. Hence, the reasoning is the same as in the solution to the last exercise.

22. Solutions/hints by parts:

- (a) Just make sure your cell complex really does describe a sphere!
- (b) Note that by adding together everything in $\{\partial_2(r) : r \in C\}$, adjacent regions have edges in their boundaries that go in opposite directions and so cancel out. Draw this out to verify. Everything cancels except for what is outermost which ends up being the negative of boundary for the outer face.
- (c) *In the construction of adding one face at a time:* we do not want gaps appearing that are faces themselves. So add faces by stacking—if a gap would be created, then add in the gap face first. If that would create a different gap face, add that one in first and so on...there are only finitely many faces to consider so that this is a finite process and we can always add in a face that will not produce a gap! *Why must the other coefficients be 0?* All the other coefficients must be 0 because we have just forced the rest of the linear combination—namely one between r_1 through r_n to be 0 because the coefficient of r_{n+1} had to be 0. By the linear independence of r_1 through r_n , we have that their scalar coefficients must be 0's too. Hence we have completed the induction steps that r_1 through r_n being linearly independent implies that r_1 through r_{n+1} must be. *The base case:* r_1 by itself is a linearly independent set.

- (d) We know that

$$\dim(\ker(\partial_1)) = \dim(\text{range}(\partial_2)) = \text{the number of vectors in } C = n_f - 1$$

- (e) Just make sure you use a correct cell complex! Remember that

$$\dim(V/\text{range}(\partial_1)) = \dim(V) - \dim(\text{range}(\partial_1))$$

- (f) We have:

$$n_e = \underbrace{n_f - 1}_{\dim(\ker(\partial_1))} + \underbrace{n_v - 1}_{\dim(\text{range}(\partial_1))}$$

Rearranging this equation gives Euler's Characteristic Formula.

Chapter 4 Selected Review Questions

Section 4.1

Can you find Smith normal form?

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

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

Can you find row and column operations matrices associated to Smith normal form?

- (a) Find the row operations matrix.
- (b) Find the column operations matrix.

3. add $-1 \cdot (\text{column 3})$ to column 1
swap rows 2 and 3
swap columns 2 and 3
add $-1 \cdot (\text{row 1})$ to row 3
add $1 \cdot (\text{column 3})$ to column 4
add $2 \cdot (\text{row 1})$ to row 3

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

4. swap rows 1 and 2
swap columns 2 and 1
swap rows 2 and 4
add $2 \cdot (\text{column 2})$ to column 3
swap rows 4 and 2

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

Can you interpret Smith normal form?

- (a) Find the rank of the matrix.

- (b) Find the nullity (i.e. kernel dimension) in a column interpretation.
- (c) Find the nullity (i.e. kernel dimension) in a row interpretation.
- (d) Determine whether the matrix function in a column interpretation is injective and/or surjective.
- (e) Determine whether the matrix function in a row interpretation is injective and/or surjective.

$$5. A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$6. A = \begin{pmatrix} 0 & 2 & -1 \\ 0 & 3 & -2 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$7. A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \\ -1 & 1 & 0 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Can you interpret Smith normal form?

- (a) Find the rank of the matrix.
- (b) Find the nullity (i.e. kernel dimension) in a column interpretation.
- (c) Find the nullity (i.e. kernel dimension) in a row interpretation.
- (d) Determine whether the matrix function in a column interpretation is injective and/or surjective.
- (e) Determine whether the matrix function in a row interpretation is injective and/or surjective.

$$8. A = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$9. A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & -1 & 0 \end{pmatrix} \rightarrow S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Section 4.2

Can you use reduced row echelon form to find a collection of columns which spans the column space (i.e. the range of the matrix thought of as a function under the column interpretation)?

10.
$$\begin{pmatrix} -6 & -8 & -12 \\ 0 & 1 & 0 \\ 3 & 4 & 6 \end{pmatrix}$$

11.
$$\begin{pmatrix} -3 & 3 & -3 & -3 & 0 \\ -1 & -2 & -1 & -1 & -3 \\ -1 & 3 & -1 & -1 & 2 \\ 6 & -4 & 6 & 6 & 3 \\ 3 & -3 & 3 & 3 & 0 \end{pmatrix}$$

Can you solve a dependent system of equations using reduced row echelon form and either the column operations matrix or the column technique to find a basis for the kernel?

12.
$$\begin{array}{rcl} x & -y & -z + 2w = -1 \\ & & w = 0 \\ 2x & -2y & -2z = -2 \\ x & -y & -z = -1 \end{array}$$

13.
$$\begin{array}{rcl} x & -2z & = 1 \\ y & +z & = 1 \\ x & -2z & = 1 \end{array}$$

14.
$$\begin{array}{rcl} x + y + 3z + 11w & -9t & = 7 \\ z + 3w & -3t & = 2 \\ u + 3t & & = -2 \end{array}$$

Can you find a fiber of a linear transformation?

15. $f^{-1}(0, 1, -2)$

$$\begin{pmatrix} 1 & -2 & 6 & -3 & -3 \\ 0 & 1 & -2 & 1 & 1 \\ -1 & 0 & -2 & 1 & 1 \end{pmatrix}$$

16. $f^{-1}(1, 1, -2)$

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

17. $f^{-1}(2, 0, 2)$

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

18. $f^{-1}(2, 2, 2)$

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 2 & 0 \end{pmatrix}$$

Section 4.3

Can you find left or right inverses or just inverses?

19. Find inverse:

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

20. Find left inverse:

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

21. Find right inverse:

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

22. Find inverse:

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

Section 4.4

Can you rewrite a matrix so it is with respect to *ab*-coordinates?

23. $a = (0, -2)$ $b = (2, -2)$

$$\begin{pmatrix} 0 & -2 \\ 2 & -2 \end{pmatrix}$$

24. $a = (-2, 1)$ $b = (2, 1)$

$$\begin{pmatrix} -2 & 1 \\ 2 & 1 \end{pmatrix}$$

Can you rewrite a matrix which is with respect to *ab*-coordinates so that it is with respect to standard coordinates?

25. $a = (2, 0)$ $b = (2, 2)$

$$\begin{pmatrix} 0 & 0 \\ -1 & 2 \end{pmatrix}_{ab}$$

26. $a = (-1, -2)$ $b = (0, 1)$

$$\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}_{ab}$$

Can you write a matrix whose input is in *ab*-coordinates and whose output is in *cd*-coordinates?

27. $a = (2, 1)$ $b = (1, -2)$
 $c = (-2, 0)$ $d = (0, -2)$

$$\begin{pmatrix} -1 & 2 \\ 2 & -1 \end{pmatrix}$$

28. $a = (-2, 1)$ $b = (1, -2)$
 $c = (2, 0)$ $d = (2, -2)$

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

Can you write a matrix which relabels one basis as another: $a \mapsto c, b \mapsto d$?

- 29.** Relabel $a = (-1, -1)$ $b = (1, 0)$
as $c = (-2, -2)$ $d = (0, 2)$.

- 30.** Relabel $a = (2, 0)$ $b = (2, -2)$
as $c = (-2, 2)$ $d = (-1, 0)$.

Section 4.5

Can you determine how many connected components a digraph has by considering the number of rows and the rank of the incidence matrix?

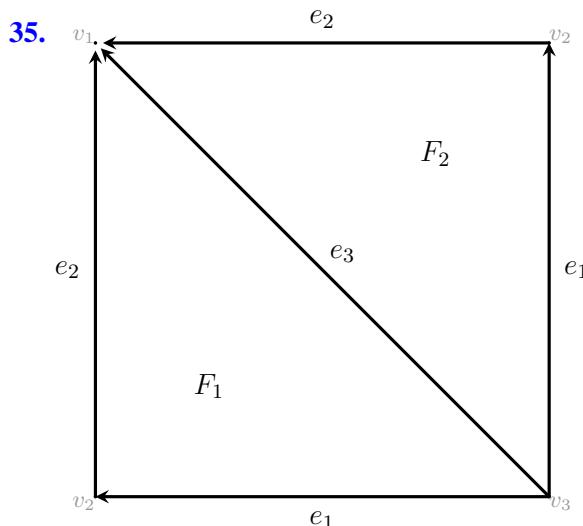
- 31.** rank= 4, rows= 7

- 32.** rank= 104, rows= 150

33.
$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

34.
$$\begin{pmatrix} -1 & -1 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Can you come up with the matrices for ∂_1 and ∂_2 given a cell complex depicted as a gluing diagram?



Solutions/Hints

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

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

3. Solutions by part:

(a)
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

4. Solutions by part:

(a)
$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

5. Solutions by part:

(a) 3

(b) 1

(c) 2

(d) Column interpretation: not injective, not surjective

(e) Row Interpretation: not injective, not surjective

6. Solutions by part:

- (a) 2
- (b) 1
- (c) 0
- (d) Column interpretation: not injective, surjective
- (e) Row Interpretation: injective, not surjective

7. Solutions by part:

- (a) 3
- (b) 0
- (c) 2
- (d) Column interpretation: injective, not surjective
- (e) Row Interpretation: not injective, surjective

8. Solutions by part:

- (a) 2
- (b) 2
- (c) 2
- (d) Column interpretation: not injective, not surjective
- (e) Row Interpretation: not injective, not surjective

9. Solutions by part:

- (a) 2
- (b) 1
- (c) 0
- (d) Column interpretation: not injective, surjective
- (e) Row Interpretation: injective, not surjective

10. r.r.e.f.

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$(-6, 0, 3), \quad (-8, 1, 4)$$

11. r.r.e.f.

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

$$(-3, -1, -1, 6, 3), \quad (3, -2, 3, -4, -3), \\ (0, -3, 2, 3, 0)$$

12. r.r.e.f.

$$\left(\begin{array}{cccc|c} 1 & -1 & -1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z, w) =$$

$$\{ \quad (-1, 0, 0, 0) + a \cdot (1, 1, 0, 0) + b \cdot \\ (1, 0, 1, 0) : a, b \in \mathbb{R} \}$$

13. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & -2 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (1, 1, 0) + a \cdot (2, -1, 1) : a \in \mathbb{R} \}$$

14. r.r.e.f.

$$\left(\begin{array}{ccccc|c} 1 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 3 & 0 & -3 \\ 0 & 0 & 0 & 0 & 1 & 3 \end{array} \right)$$

All Solutions:

$$(x, y, z, w, u, t) =$$

$$\{ \quad (1, 0, 2, 0, -2, 0) + a \cdot \\ (-1, 1, 0, 0, 0, 0) + b \cdot (-2, 0, -3, 1, 0, 0) + \\ c \cdot (0, 0, 3, 0, -3, 1) : a, b, c \in \mathbb{R} \}$$

15. r.r.e.f.

$$\left(\begin{array}{ccccc|c} 1 & 0 & 2 & -1 & -1 & 2 \\ 0 & 1 & -2 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

$$\{ (2, 1, 0, 0, 0) + a \cdot (-2, 2, 1, 0, 0) + b \cdot \\ (1, -1, 0, 1, 0) + c \cdot (1, -1, 0, 0, 1) : \\ a, b, c \in \mathbb{R} \}$$

16. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

$$\{ (1, 1, 0) + a \cdot (-2, -2, 1) : a \in \mathbb{R} \}$$

17. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{array} \right)$$

$(2, 0, 2)$

18. r.r.e.f.

$$\left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right)$$

$f^{-1}(2, 2, 2) = \emptyset$

19. $\left(\begin{array}{ccc} -\frac{2}{5} & 0 & -\frac{1}{5} \\ \frac{1}{5} & -\frac{1}{2} & -\frac{2}{5} \\ 0 & \frac{1}{2} & 0 \end{array} \right)$

20. Possible Solution: $\left(\begin{array}{ccc} \frac{4}{5} & 1 & \frac{2}{5} \\ \frac{2}{5} & 0 & \frac{1}{5} \end{array} \right)$

21. Possible Solution: $\left(\begin{array}{cc} -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} \\ -1 & -\frac{3}{2} \end{array} \right)$

22. $\left(\begin{array}{ccc} 0 & 1 & 1 \\ \frac{1}{2} & 0 & 0 \\ -\frac{1}{2} & 1 & 2 \end{array} \right)$

23. $\left(\begin{array}{cc} -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & 0 \\ 0 & 2 \\ -2 & -2 \end{array} \right) \cdot \left(\begin{array}{cc} 0 & -2 \\ 2 & -2 \end{array} \right) \cdot \left(\begin{array}{cc} -4 & -6 \\ 2 & 2 \end{array} \right) =$

24. $\left(\begin{array}{cc} -\frac{1}{4} & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{2} \\ -2 & 2 \\ 1 & 1 \end{array} \right) \cdot \left(\begin{array}{cc} -2 & 1 \\ 2 & 1 \end{array} \right) = \left(\begin{array}{cc} -\frac{11}{4} & \frac{13}{4} \\ -\frac{1}{4} & \frac{7}{4} \end{array} \right)$

25. $\left(\begin{array}{cc} 2 & 2 \\ 0 & 2 \end{array} \right) \cdot \left(\begin{array}{cc} 0 & 0 \\ -1 & 2 \end{array} \right) \cdot \left(\begin{array}{cc} \frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} \end{array} \right) = \left(\begin{array}{cc} -1 & 3 \\ -1 & 3 \end{array} \right)$

26. $\left(\begin{array}{cc} -1 & 0 \\ -2 & 1 \end{array} \right) \cdot \left(\begin{array}{cc} 1 & 1 \\ 2 & 1 \end{array} \right) \cdot \left(\begin{array}{cc} -1 & 0 \\ -2 & 1 \end{array} \right) = \left(\begin{array}{cc} 3 & -1 \\ 2 & -1 \end{array} \right)$

27. $\left(\begin{array}{cc} -\frac{1}{2} & 0 \\ 0 & -\frac{1}{2} \end{array} \right) \cdot \left(\begin{array}{cc} -1 & 2 \\ 2 & -1 \end{array} \right) \cdot \left(\begin{array}{cc} 2 & 1 \\ 1 & -2 \end{array} \right) = \left(\begin{array}{cc} 0 & \frac{5}{2} \\ -\frac{3}{2} & -2 \end{array} \right)$

28. $\left(\begin{array}{cc} \frac{1}{2} & \frac{1}{2} \\ 0 & -\frac{1}{2} \end{array} \right) \cdot \left(\begin{array}{cc} 0 & 1 \\ 1 & -1 \end{array} \right) \cdot \left(\begin{array}{cc} -2 & 1 \\ 1 & -2 \end{array} \right) = \left(\begin{array}{cc} -1 & \frac{1}{2} \\ \frac{3}{2} & -\frac{3}{2} \end{array} \right)$

29. $\left(\begin{array}{cc} 0 & 2 \\ 2 & 0 \end{array} \right)$

30. $\left(\begin{array}{cc} -1 & -\frac{1}{2} \\ 1 & 1 \end{array} \right)$

31. 3 connected components.**32.** 46 connected components.

33. 3**34.** 4**35.** The matrix for ∂_1 is:

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

The matrix for ∂_2 is:

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

Part II

The Symmetries of Matrices

Projections 5

Transposes, Symmetric Matrices, and Lengths

5.1

5.1.1 Matrix Transposes	461
5.1.2 Notation and Terminology for Row Vectors (Duals)	463
5.1.3 Symmetric Matrices	464
5.1.4 Projection Length	465
5.1.5 Orthogonality	470
5.1.6 The Laplacian Symmetric Matrix (Optional)	472
5.1.7 Exercises	479
5.1.8 Solutions	483

Questions to Guide Your Study:

- *What is a transpose of a matrix?*
- *How does a transpose help us convert the row interpretation linear transformation to a column interpretation and vice versa?*
- *What are some properties of matrix transposes?*
- *What is a symmetric matrix?*
- *How do you compute the length of a vector?*
- *What is the dot product and what does it tell us?*
- *How do you find the orthogonal projection length of one vector onto another?*
- *What does it mean for two vectors to be orthogonal?*
- *What does it mean for two subspaces to be orthogonal?*

5.1.1 Matrix Transposes



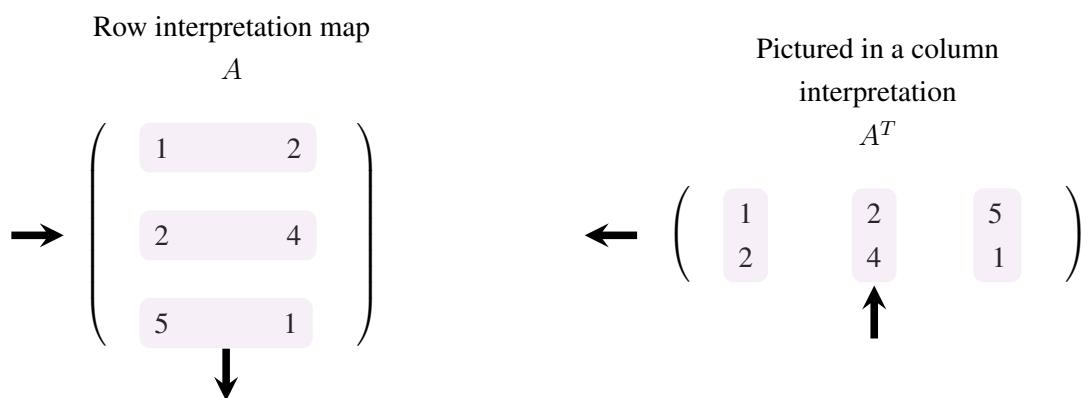
The following illustrates the operation of taking a transpose notated as A^T :

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \\ 5 & 1 \end{pmatrix} \quad A^T = \begin{pmatrix} 1 & 2 & 5 \\ 2 & 4 & 1 \end{pmatrix}$$

Transpose of a Matrix

The transpose of a matrix A is a matrix A^T such that the list of ordered rows from top to bottom of A^T is the same as the list of ordered columns from left to right of A . Equivalently, the list of ordered rows of A from top to bottom is the same as the list of ordered columns of A^T from left to right.

The row interpretation of multiplying by a matrix A often yields a *different* linear transformation than the column interpretation of multiplying by A . In fact, the codomain and the domain themselves switch places. Yet, what if we wanted to write the linear transformation that we get from a row interpretation of A as a matrix under the column interpretation? The solution is: *take a transpose!*



Example 1. Let $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ represent the matrix A above under its row interpretation. Then $f(1, 1, 0) = (3, 6)$ is calculated by:

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

or

$$A^T \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 5 \\ 2 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \end{pmatrix}$$

The product AB under a row interpretation means first apply A as a function and *then* B . So if we want to write this in a column interpretation, we would say:

- *first apply the function given by the row interpretation of A in a column interpretation (so A^T)*
- *next apply the function given by the row interpretation of B in a column interpretation (so B^T)*

The product $B^T A^T$ interpreted in a column interpretation would yield this row interpretation function of AB since we now are saying: first apply the column interpretation of A^T as a function and then apply the column interpretation of B^T as a function.

Transposes Reverse the Order of Multiplication

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

Example 2.

$$\left(\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \right)^T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 2 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \\ 2 & 0 \end{pmatrix}$$

Example 3. $(ABCD)^T = D^T C^T B^T A^T$

Column Interpretation Convention

Unless otherwise indicated, we will usually assume a column interpretation as the standard notation for matrices describing linear transformations.

Example 4. The row vector $\begin{pmatrix} 2 & 0 & -1 \end{pmatrix}$ is the transpose of the column vector $\begin{pmatrix} 2 \\ 0 \\ -1 \end{pmatrix}$. If we write

$v = (2, 0, -1)$, we will use our convention to interpret the vector v as a column. Then v^T will represent a row vector.

Theorem 5.1.1 Transposes and Inverses

Let A be a square matrix which has an inverse. Then, $(A^{-1})^T = (A^T)^{-1}$

Proof.

$$AA^{-1} = \text{id} \implies (AA^{-1})^T = \text{id}^T = \text{id} \implies (A^{-1})^T A^T = \text{id}$$

Therefore the inverse matrix to A^T is $(A^{-1})^T$. This is precisely the statement that $(A^T)^{-1} = (A^{-1})^T$. \square

5.1.2 Notation and Terminology for Row Vectors (Duals)

Example 5. Let $v = (2, 0, -1) \in \mathbb{R}^3$. Then assuming a column interpretation, the matrix $v^T = \begin{pmatrix} 2 & 0 & -1 \end{pmatrix}$ is a 1×3 matrix which represents a function $\mathbb{R}^3 \rightarrow \mathbb{R}$. That is, v^T lives in the vector space of functions from $\mathbb{R}^3 \rightarrow \mathbb{R}$. Naturally, this vector space has the same structure as the space of column vectors representing \mathbb{R}^3 : *we just turn things on the side!*

Dual Vectors are Transposed Vectors

Given a finite dimensional vector space V , we will naturally think of it as a space of column vectors. With a choice of basis pretending to be the standard one, we can think of V as \mathbb{R}^n for some n . If we write V^* , we will think of it as the same vector space V , but where all of the vectors are rows. These row vectors under a column interpretation are functions $\mathbb{R}^n \rightarrow \mathbb{R}$. We say V^* is the dual vector space of V . We convert from V to V^* simply by $v \mapsto v^T$.

v^*

Think of v as a column vector. We can also write v^T as v^* and call it the *dual vector* corresponding to v .

Another way of writing V^* is $\text{Hom}_{\mathbb{R}}(V, \mathbb{R})$ which means the vector space of linear transformations $V \rightarrow \mathbb{R}$.

Example 6. In particular if $V = \mathbb{R}^2$ and $v = (2, 4) \in V$, then we think of v as a column $\begin{pmatrix} 2 \\ 4 \end{pmatrix}$ and can write $v^T = \begin{pmatrix} 2 & 4 \end{pmatrix} \in V^*$. In this particular case, $V^* = \text{Hom}_{\mathbb{R}}(\mathbb{R}^2, \mathbb{R})$, the vector space of linear transformations $\mathbb{R}^2 \rightarrow \mathbb{R}$. Notice that under the column interpretation, the matrix $v^T = \begin{pmatrix} 2 & 4 \end{pmatrix}$ is a function $\mathbb{R}^2 \rightarrow \mathbb{R}$. Hence,

$v^T \in \text{Hom}_{\mathbb{R}}(\mathbb{R}^2, \mathbb{R})$.

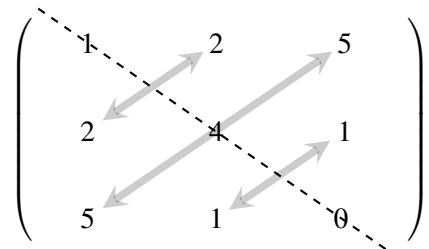
Matrices as Maps and Dual Maps

Take a matrix A which represents a function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ under a column interpretation of column vectors. Then this same matrix defines a function $f^* : \mathbb{R}^{m*} \rightarrow \mathbb{R}^{n*}$ of row vectors. That is, the function f^* is just the row interpretation map of A that takes row vectors to row vectors *in the usual way* where we have **not taken the transpose of A : just the vectors!** The function f^* is called the *dual map* to f .

The function f^* is the “companion” row interpretation map of the *same* matrix that describes the column interpretation map f .

5.1.3 Symmetric Matrices

Consider the symmetry of the following matrix:



This symmetry can also be thought of as the idea that $A^T = A$:

$$\left(\begin{array}{ccc} 1 & 2 & 5 \\ 2 & 4 & 1 \\ 5 & 1 & 0 \end{array} \right) \quad \left(\begin{array}{c|c|c} 1 & 2 & 5 \\ 2 & 4 & 1 \\ 5 & 1 & 0 \end{array} \right)$$

Symmetric Matrix

A symmetric matrix is a matrix such that $A^T = A$. Such a matrix is necessarily a square matrix (i.e. a $n \times n$ matrix for some n).

Theorem 5.1.2 Symmetric Products

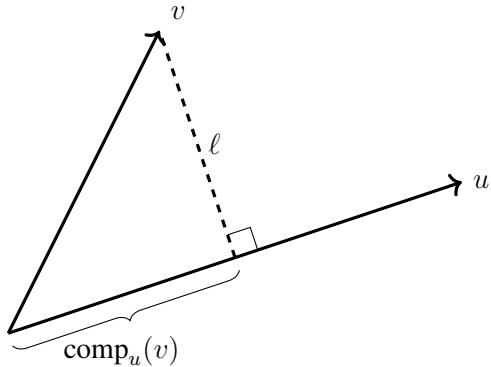
For any matrix A , the products AA^T and A^TA are always symmetric.

Proof. You can do this one! Just remember that $(A^T)^T = A$ and that when you apply the transpose of a matrix to a product it reverses order. What you want to show is that $(AA^T)^T = AA^T$ and $(A^TA)^T = A^TA$. \square

Example 7. The matrix product $\underbrace{\begin{pmatrix} 1 \\ 2 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} 1 & 2 \\ 1 & 4 \end{pmatrix}}_{A^T} = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ is a symmetric matrix.

5.1.4 Projection Length

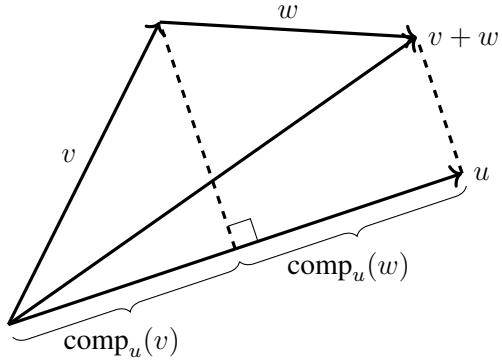
We want a way to talk about projecting one vector onto another as depicted in the following:

**comp_u(v)**

Take two vectors u and v in \mathbb{R}^n . Their span $\langle u, v \rangle$ form a plane. Draw arrows for u and v in that plane such that both of their tails are at the origin. Draw a line ℓ perpendicular to the vector u that passes through the tip of v . The distance from the origin to the intersection of ℓ and u is called the component of v along u . It is like measuring the shadow cast by v if u were the ground and light were shining straight down at a perpendicular angle to this ground. We denote this projection length $\text{comp}_u(v)$.

The next illustration demonstrates the idea that

$$\text{comp}_u(v + w) = \text{comp}_u(v) + \text{comp}_u(w)$$



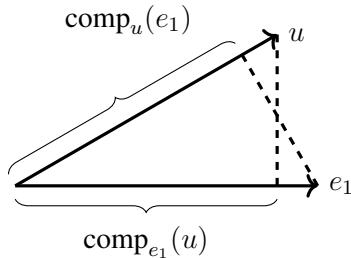
In particular, we can choose a subspace spanned by all three vectors u , v , and w . The picture is then a good illustration if that span has dimension 2 and so appears in a plane. But what if the span has dimension 3? The illustration still works if we imagine that the dotted lines are planes perpendicular to u and we are looking head on so that the planes appear thin in our view. This tells us that comp_u is an additive function. In fact, it is also scalable.

Theorem 5.1.3 Projection Length is a Linear Transformation

Given a vector $u \in \mathbb{R}^n$, the function $\text{comp}_u : \mathbb{R}^n \rightarrow \mathbb{R}$ is a linear transformation.

Since comp_u is a linear transformation $\mathbb{R}^n \rightarrow \mathbb{R}$, we can describe it as $1 \times n$ matrix according to a column interpretation. We simply need to determine where the standard basis vectors are sent by this map.

To simplify matters, let's assume that u has the same length as all of the standard basis vectors which all have length 1. Now, let's choose e_1 and see what happens. We draw the plane $\langle u, e_1 \rangle$ and picture the vectors in it:



Elementary geometry yields from two congruent triangles that $\text{comp}_{e_1}(u) = \text{comp}_u(e_1)$. How can we use this? If $u = (a, b, c)$, then $\text{comp}_{e_1}(u) = a$ since the x -coordinate a itself is the projection length of u along the x -axis. Observe that by default we picture the standard basis vectors by right angles to each other. This means that $(0, b, 0)$ and $(0, 0, c)$ have 0 projection length along u . Since comp_{e_1} is additive,

$$\text{comp}_{e_1}(u) = \underbrace{\text{comp}_{e_1}(a, 0, 0)}_a + \underbrace{\text{comp}_{e_1}(0, b, 0)}_0 + \underbrace{\text{comp}_{e_1}(0, 0, c)}_0 = a$$

Hence, $\text{comp}_u(e_1) = a$. By a symmetric argument we deduce that $\text{comp}_u(e_2) = b$ and $\text{comp}_u(e_3) = c$. That is, the matrix for comp_u is $\begin{pmatrix} a & b & c \end{pmatrix}$. This is just u^T itself if u is a column vector!

Orthogonal Projection Length

Suppose that $u \in \mathbb{R}^n$ is a vector of length 1. Then, the orthogonal projection length of a vector $v \in \mathbb{R}^n$ is defined as $\text{comp}_u(v)$. The function $\text{comp}_u : \mathbb{R}^n \rightarrow \mathbb{R}$ is given by the row $1 \times n$ matrix u^T if u itself describes a $n \times 1$ column vector.

Example 8. Let $u = \left(\frac{\sqrt{3}}{2}, \frac{1}{2} \right)$. Then, u is a vector of length 1. We can compute the orthogonal projection length of $v = (2, 2)$ as follows:

$$u^T v = \left(\frac{\sqrt{3}}{2} \quad \frac{1}{2} \right) \cdot \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \sqrt{3} + 1$$

Length of a Vector

We define the length of a vector v to be $|\text{comp}_u(v)| = |u^T v|$ where $u = kv$ for a scalar k so that kv has length 1. That is, v has been rescaled to a unit vector u . So the length of a vector is the orthogonal projection of a vector onto a rescaled version of itself that has length 1. The length, also known as *magnitude* of the vector v is denoted as $|v|$.

The length of the vector v is precisely the same notion as absolute value—the distance from 0. It is the distance from the tip of the vector to the origin. Hence, we use the same notation $|v|$ as we do for absolute value. The length of a vector v is also often called its magnitude. Now if u has length 1, then $|u| = u^T u = 1$ since u does not need to be rescaled—it is already of length 1. Now if on the other hand we only know that $u^T u = 1$, is it necessarily true that u has length 1? Well, we know that $|u| = (ku)^T u$ for some k and this is $|u| = k(\underbrace{u^T u}_1) = k$. Yet the scalar $k \geq 0$ is precisely the one so that ku has length 1. That is, $|ku| = 1$. So, we have two equations:

$$\begin{aligned} |u| &= k \\ |ku| &= 1 \end{aligned}$$

Multiplying the first equation by k we have $|ku| = k^2$. Using the equation $|ku| = 1$, we deduce that $k^2 = 1$ so that $|u| = |k| = 1$. So yes, u has length 1.

Theorem 5.1.4

A vector is a unit vector if and only if $u^T u = 1$.

Unit Vector

A unit vector is a vector such that $u^T u = 1$. That is, u has length 1. If $u = (a_1, a_2, \dots, a_n)$, then

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = 1$$

$$a_1^2 + a_2^2 + \cdots + a_n^2 = 1$$

Now, how do we find k so that we can rescale a vector v so that kv has length 1? We would like $(kv)^T \cdot (kv) = 1$. This means that: $k^2 v^T v = 1$ or simply:

$$k = \frac{1}{\sqrt{v^T v}}$$

Remember that $v^T v$ is a 1×1 matrix which is simply a number in \mathbb{R} . Also, $v^T v$ is just a sum of squares so it necessarily is positive. Hence, we can take a square root.

Notationally, let $v \bullet w$ mean $v^T w$ where v and w are column vectors. We say $v \bullet w$ is the “dot product” between the vectors v and w .

Dot Product

The dot product $v \bullet w$ between two column vectors is the matrix product $v^T w$.

Using this notation,

How to Make a Unit Vector

Given a vector $v \in \mathbb{R}^n$ for some n ,

$$\frac{1}{\sqrt{v \bullet v}} v$$

is a unit vector.

Also, the length of v can be calculated as:

$$|v| = \left(\frac{1}{\sqrt{v \bullet v}} v \right) \bullet v = \frac{v \bullet v}{\sqrt{v \bullet v}} = \sqrt{v \bullet v}.$$

Length of Vector Formula

$$|v| = \sqrt{v \bullet v}$$

If $v = (a_1, a_2, \dots, a_n)$, then

$$v = \sqrt{a_1^2 + a_2^2 + \dots + a_n^2}$$

The length of a vector formula is simply a generalization of the Pythagorean Theorem in the plane.

Example 9. $|(1, 2, 3)| = \sqrt{(1, 2, 3) \bullet (1, 2, 3)} = \sqrt{1^2 + 2^2 + 3^2} = \sqrt{14}$

$\text{comp}_v w$ Formula

$$\text{comp}_v w = \frac{v}{|v|} \bullet w = \frac{v \bullet w}{\sqrt{v \bullet v}}$$

Example 10. Example of $\text{comp}_v w$. The projection length of $w = (1, 0, 1)$ along a ground vector $v = (1, 1, 1)$ is:

$$\text{comp}_v w = \frac{(1, 1, 1) \bullet (1, 0, 1)}{\sqrt{(1, 1, 1) \bullet (1, 1, 1)}} = \frac{2}{\sqrt{3}}.$$

Properties of the Dot product

The function $u \bullet : \mathbb{R}^n \rightarrow \mathbb{R}$ given by $w \mapsto u \bullet (w)$ is simply the linear transformation given by the matrix u^T . All of the properties of linear transformations apply.

- $u \bullet (v + w) = u \bullet v + u \bullet w$
- $u \bullet (kv) = ku \bullet v$

Also, direct computation yields that $w^T u = u^T w$. Therefore,

$$w \bullet u = u \bullet w.$$

5.1.5 Orthogonality

Orthogonal Vectors

Two vectors v and w are *orthogonal* to each other if $\text{comp}_v w = 0$. That is, when placed in the same plane, they appear at a right angle to each other.

If v and w are orthogonal, we write $v \perp w$.

Theorem 5.1.5 Orthogonality Condition

Two vectors v and w are *orthogonal* to each other if and only if

$$v \bullet w = 0$$

Proof. Just remember that $\text{comp}_v w$ and $\text{comp}_w v$ are computed via this dot product. □

Example 11. The vector $(1, 0, 1, 1)$ is orthogonal to $(0, 1, 1, -1)$ since

$$(1, 0, 1, 1) \bullet (0, 1, 1, -1) = 0.$$

Orthogonal Subspaces

Two subspaces V and W of a vector space are orthogonal if $v \perp w$ for all $v \in V$ and all $w \in W$. We say that V and W are orthogonal complements to each other.

Theorem 5.1.6 Orthogonality by Bases

Let V and W be two subspaces of a vector space. Let B be a basis of V and P be a basis of W . Then $V \perp W$ if and only if $b \perp p$ for all $b \in B$ and $p \in P$.

Proof. This is left as an exercise! □

Example 12. Let's find a basis for the subspace W of \mathbb{R}^3 that is orthogonal to the vector $(1, 1, 2)$. To do this

we think:

$$(1, 1, 2) \bullet (\begin{matrix} ? \\ ? \\ ? \end{matrix}) = \begin{pmatrix} 1 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} ? \\ ? \\ ? \end{pmatrix} = 0$$

So we want to determine *a basis for the kernel* of the linear transformation given by the matrix $\begin{pmatrix} 1 & 1 & 2 \end{pmatrix}$ under a column interpretation. We can use the shortcut to kernel by columns:

$$\begin{pmatrix} * & -1 & -2 \\ * & 1 & 0 \\ * & 0 & 1 \end{pmatrix}.$$

Therefore, $W = \langle (-1, 1, 0), (-2, 0, 1) \rangle$.

Orthogonal Complement

Let H be a subspace of a vector space V . Then we define its orthogonal complement to be:

$$H^\perp = \{v : v \perp h\}$$

Example 13. In the last example, $\langle (1, 1, 2) \rangle^\perp = \langle (-1, 1, 0), (-2, 0, 1) \rangle$.

There is a neat relationship between the *row* interpretation map and the *column* interpretation map for a matrix. The range of one is orthogonal to the kernel of the other. In fact, they are orthogonal complements!

Kernels are Orthogonal

Let A be a matrix that with a column interpretation describes a linear transformation f . Suppose that under a row interpretation, it represents a linear transformation g . Then:

- $\text{range}(g)^\perp = \text{row}(A)^\perp = \text{col}(A^T)^\perp = \ker(f)$
- $\text{range}(f)^\perp = \text{col}(A)^\perp = \text{row}(A^T)^\perp = \ker(g)$

Yet this is precisely what we use when we find the orthogonal complement by writing the vectors as the *rows* of a matrix and then finding the kernel!

Finding an Orthogonal Complement

To find an orthogonal complement, write the vectors as the rows of a matrix. Then, compute a basis for the kernel of that matrix thought of as a map under the column interpretation.



Example 14. Video Let's find a basis for V^\perp where $V = \langle (1, 1, 2), (0, 1, 1) \rangle$. To do this we write the vectors as a row matrix and then compute the reduced row echelon form:

$$\begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Using the fast column technique for finding a basis for the kernel under the column interpretation, we see that $(-1, -1, 1)$ is the desired basis. Therefore,

$$V^\perp = \langle (-1, -1, 1) \rangle$$

Indeed, you can verify that $(-1, -1, 1) \bullet (1, 1, 2) = 0$ and $(-1, -1, 1) \bullet (0, 1, 1) = 0$.

5.1.6 The Laplacian Symmetric Matrix (Optional)

This subsection brings up an example which is useful when studying digraphs. Suppose for instance that we have a digraph determined by the following incidence matrix:

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

Let a_{ij} be the entry in the i th row and j th column of BB^T . If we multiply BB^T using 1×1 blocks in either row or column interpretation, each entry BB^T can be thought of as $b_i \bullet b_j$ where b_i signifies the i th row of B , which corresponds to the i th vertex v_i of the digraph. Similarly, b_j represents the j th row of B which is the j th column of B^T and refers to v_j .

Degree of Vertex

The degree of a vertex in a digraph is the number of edges that touch it. If v is the vertex, then we notate the degree of v as $\deg(v)$.

Notice that

$$b_i \bullet b_j = \begin{cases} \deg(v_i) & \text{if } i \neq j \\ -(\text{the number of edges between } v_i \text{ and } v_j \text{ in either direction.}) & \text{if } i = j \end{cases}$$

This calculation confirms the idea that BB^T is symmetric: $(BB^T)^T = BB^T$. It also tells us that if we make every edge bidirectional, then subtracting the resulting “bidirectional adjacency matrix” given as:

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

from the diagonal vertex degree matrix:

$$D = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

gives us BB^T :

$$BB^T = D - A = \begin{pmatrix} 2 & -1 & 0 & -1 & 0 \\ -1 & 3 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & -2 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Laplacian Matrix

The matrix BB^T is called the Laplacian matrix of a digraph with respect to an ordering of the vertices. The matrix B is an incidence matrix with respect to that vertex ordering.

The following should be clear thinking along one row subtracting touches between individual vertices (off the

diagonal) from the diagonal entry (total number of touches):

Theorem 5.1.7

The sum of any row in the Laplacian matrix is 0.

In particular,

$$BB^T \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

That is, $(1, 1, 1, 1, 1)$ is in the column interpretation kernel of BB^T . Notice that $(1, 1, 0, 1, 0)$ is in the kernel but $(1, 1, 1, 0, 0)$ is not. A vector of 1's and 0's is in the kernel precisely when the 1's correspond to vertices that themselves form an intact subgraph without any edges leaving it—they form a *connected component*.

Connected Component

A connected component of a digraph is a connected subgraph that is disconnected from the rest of the graph.

Using these ideas we can computationally determine precisely which vertices are in each connected component. We find the kernel of BB^T by first doing row operations toward Smith normal form until the only column operations done cause the columns of the column operations matrix that correspond to the zero columns in the Smith normal form to have 0's and 1's. A basis for the kernel of BB^T is found by looking at these “kernel columns.” It should be clear at such a point what the connected components are. For instance, we could get the Smith normal form

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

having used the column operations matrix

$$\begin{pmatrix} 1 & \frac{1}{2} & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Notice that the kernel is spanned by $(0, 0, 1, 0, 0)$, $(1, 1, 0, 1, 0)$, and $(0, 0, 0, 0, 1)$. *These are the connected components!*

Exercise to the Reader

Draw out the graph given by our incidence matrix B to verify what we have found.

Key Concepts from this Section

- **A^T :** (page 461) The matrix A^T is the transpose of the matrix A .
- **transpose of a matrix:** (page 461) The transpose of a matrix A is a matrix A^T such that the list of ordered rows from top to bottom of A^T is the same as the list of ordered columns from left to right of A . Equivalently, the list of ordered rows of A from top to bottom is the same as the list of ordered columns of A^T from left to right.
- **transposes reverse the order of multiplication:** (page 462)

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

- **column interpretation convention:** (page 462) Unless otherwise indicated, we will usually assume a column interpretation as the standard notation for matrices describing linear transformations.
- **theorem 5.1.1 transposes and inverses:** (page 463) Let A be a square matrix which has an inverse. Then, $(A^{-1})^T = (A^T)^{-1}$
- **dual vectors are transposed vectors:** (page 463) Given a finite dimensional vector space V , we will naturally think of it as a space of column vectors. With a choice of basis pretending to be the standard one, we can think of V as \mathbb{R}^n for some n . If we write V^* , we will think of it as the same vector space V , but where all of the vectors are rows. These row vectors under a column interpretation are functions $\mathbb{R}^n \rightarrow \mathbb{R}$. We say V^* is the dual vector space of V . We convert from V to V^* simply by $v \mapsto v^T$.
- **v^* :** (page 463) Think of v as a column vector. We can also write v^T as v^* and all it the *dual vector* corresponding to v .
- **V^* :** (page 463) If V is a vector space of column vectors, we write V^* to denote the vector space of row vectors.
- **$\text{Hom}_{\mathbb{R}}(V, \mathbb{R})$:** (page 463) This denotes the vector space of linear transformations $V \rightarrow \mathbb{R}$. It is another way of writing V^* .
- **matrices as maps and dual maps:** (page 464) Take a matrix A which represents a function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ under a column interpretation of column vectors. Then this same matrix defines a function $f^* : \mathbb{R}^{m*} \rightarrow \mathbb{R}^{n*}$ of row vectors. That is, the function f^* is just the row interpretation map of A that takes

row vectors to row vectors *in the usual way* where we have ***not*** taken the transpose of A : just the vectors! The function f^* is called the *dual map* to f .

- **f^* :** (page 464) See the term “matrices as maps and dual maps.”
 - **symmetric matrix:** (page 464) A symmetric matrix is a matrix such that $A^T = A$. Such a matrix is necessarily a square matrix (i.e. a $n \times n$ matrix for some n).
 - **theorem 5.1.2 symmetric products:** (page 464) For any matrix A , the products AA^T and A^TA are always symmetric.
 - **comp_u(v):** (page 465) Take two vectors u and v in \mathbb{R}^n . Their span $\langle u, v \rangle$ form a plane. Draw arrows for u and v in that plane such that both of their tails are at the origin. Draw a line ℓ perpendicular to the vector u that passes through the tip of v . The distance from the origin to the intersection of ℓ and u is called the component of v along u . It is like measuring the shadow cast by v if u were the ground and light were shining straight down at a perpendicular angle to this ground. We denote this projection length $\text{comp}_u(v)$.
 - **theorem 5.1.3 projection length is a linear transformation:** (page 466) Given a vector $u \in \mathbb{R}^n$, the function $\text{comp}_u : \mathbb{R}^n \rightarrow \mathbb{R}$ is a linear transformation.
 - **orthogonal projection length:** (page 466) Suppose that $u \in \mathbb{R}^n$ is a vector of length 1. Then, the orthogonal projection length of a vector $v \in \mathbb{R}^n$ is defined as $\text{comp}_u(v)$. The function $\text{comp}_u : \mathbb{R}^n \rightarrow \mathbb{R}$ is given by the row $1 \times n$ matrix u^T if u itself describes a $n \times 1$ column vector.
 - **length of a vector:** (page 467) We define the length of a vector v to be $|\text{comp}_u(v)| = |u^T v|$ where $u = kv$ for a scalar k so that kv has length 1. That is, v has been rescaled to a unit vector u . So the length of a vector is the orthogonal projection of a vector onto a rescaled version of itself that has length 1. The length, also known as *magnitude* of the vector v is denoted as $|v|$.
 - **theorem 5.1.4 :** (page 467) A vector is a unit vector if and only if $u^T u = 1$.
 - **unit vector:** (page 467) A unit vector is a vector such that $u^T u = 1$. That is, u has length 1. If $u = (a_1, a_2, \dots, a_n)$, then
- $$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = 1$$
- $$a_1^2 + a_2^2 + \cdots + a_n^2 = 1$$
- **$v \bullet w$:** (page 468) We write $v \bullet w$ to mean $v^T w$ where v and w are column vectors.
 - **dot product:** (page 468) The dot product $v \bullet w$ between two column vectors is the matrix product $v^T w$.

- **how to make a unit vector:** (page 468) Given a vector $v \in \mathbb{R}^n$ for some n ,

$$\frac{1}{\sqrt{v \bullet v}} v$$

is a unit vector.

- **length of vector formula:** (page 468)

$$|v| = \sqrt{v \bullet v}$$

If $v = (a_1, a_2, \dots, a_n)$, then

$$v = \sqrt{a_1^2 + a_2^2 + \dots + a_n^2}$$

- **comp_vw formula:** (page 469)

$$\text{comp}_v w = \frac{v}{|v|} \bullet w = \frac{v \bullet w}{\sqrt{v \bullet v}}$$

- **properties of the dot product:** (page 469) The function $u \bullet : \mathbb{R}^n \rightarrow \mathbb{R}$ given by $w \mapsto u \bullet (w)$ is simply the linear transformation given by the matrix u^T . All of the properties of linear transformations apply.

- $u \bullet (v + w) = u \bullet v + u \bullet w$
- $u \bullet (kv) = ku \bullet v$

Also, direct computation yields that $w^T u = u^T w$. Therefore,

$$w \bullet u = u \bullet w.$$

- **orthogonal vectors:** (page 470) Two vectors v and w are *orthogonal* to each other if $\text{comp}_v w = 0$. That is, when placed in the same plane, they appear at a right angle to each other.

- **$v \perp w$:** (page 470) We write $v \perp w$ to signify that v and w are orthogonal to each other.

- **theorem 5.1.5 orthogonality condition:** (page 470) Two vectors v and w are *orthogonal* to each other if and only if

$$v \bullet w = 0$$

- **orthogonal subspaces:** (page 470) Two subspaces V and W of a vector space are orthogonal if $v \perp w$ for all $v \in V$ and all $w \in W$. We say that V and W are orthogonal complements to each other.

- **theorem 5.1.6 orthogonality by bases:** (page 470) Let V and W be two subspaces of a vector space. Let B be a basis of V and P be a basis of W . Then $V \perp W$ if and only if $b \perp p$ for all $b \in B$ and $p \in P$.

- **orthogonal complement:** (page 471) Let H be a subspace of a vector space V . Then we define its orthogonal complement to be:

$$H^\perp = \{v : v \perp h\}$$

- **kernels are orthogonal:** (page 471) Let A be a matrix that with a column interpretation describes a linear transformation f . Suppose that under a row interpretation, it represents a linear transformation g . Then:
 - $\text{range}(g)^\perp = \text{row}(A)^\perp = \text{col}(A^T)^\perp = \ker(f)$
 - $\text{range}(f)^\perp = \text{col}(A)^\perp = \text{row}(A^T)^\perp = \ker(g)$

- **finding an orthogonal complement:** (page 472) To find an orthogonal complement, write the vectors as the rows of a matrix. Then, compute a basis for the kernel of that matrix thought of as a map under the column interpretation.
- **degree of vertex:** (page 472) The degree of a vertex in a digraph is the number of edges that touch it. If v is the vertex, then we notate the degree of v as $\deg(v)$.
- **laplacian matrix:** (page 473) The matrix BB^T is called the Laplacian matrix of a digraph with respect to an ordering of the vertices. The matrix B is an incidence matrix with respect to that vertex ordering.
- **theorem 5.1.7 :** (page 474) The sum of any row in the Laplacian matrix is 0.
- **connected component:** (page 474) A connected component of a digraph is a connected subgraph that is disconnected from the rest of the graph.

5.1.7 Exercises

Dual Maps (Transposes)

For each of the following, let f denote column interpretation map of the matrix. Then, find the matrix for which its column interpretation describes the map f^* . Remember that f^* denotes the row interpretation function of the matrix given for f .

$$1. f : \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 2 & 2 & 1 \end{pmatrix}$$

$$2. f : \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$3. f : \begin{pmatrix} 2 & 1 \\ 0 & 0 \\ -2 & 0 \end{pmatrix}$$

$$4. f : \begin{pmatrix} 2 & -2 & 1 \\ 0 & -1 & 2 \\ 0 & -1 & 2 \end{pmatrix}$$

$$5. f : \begin{pmatrix} 0 & 0 \\ 1 & -2 \end{pmatrix}$$

$$6. f : \begin{pmatrix} -1 & 1 \\ -2 & -1 \end{pmatrix}$$

$$7. f : \begin{pmatrix} 2 & -1 \\ -1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$8. f : \begin{pmatrix} 0 & 0 \\ -1 & -1 \end{pmatrix}$$

$$9. f : \begin{pmatrix} -2 \\ 0 \end{pmatrix}$$

$$10. f : \begin{pmatrix} 0 & -2 & -2 \\ -2 & 0 & 0 \\ -2 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Vector Computation Practice

Compute the length of the following vectors.

$$11. (2, -1, 2, 2)$$

$$12. (0, -1, 0, -2)$$

13. $(-2, -2, -1, 2)$

14. $(1, 1)$

15. $(1, -2)$

16. $(-1, -1)$

17. $(1, -1, 0)$

18. $(0, 2, 1)$

Compute $\text{comp}_u(v)$ for the following.

19. $u = (1, 2, -1) \quad v = (-1, 0, -1)$

20. $u = (-2, 1, 2, 2) \quad v = (0, 1, -1, -2)$

21. $u = (-1, -2, 1, 2) \quad v = (0, 0, -1, -1)$

22. $u = (2, 0, -1, 1) \quad v = (-1, 0, 1, -2)$

23. $u = (0, -2, 1) \quad v = (-1, -2, -2)$

24. $u = (-1, 0, 1, -2) \quad v = (-2, -1, 2, 0)$

25. $u = (0, -1, -2, -2) \quad v = (-1, -2, 0, -1)$

26. $u = (-1, -2, 1, 0) \quad v = (0, -1, 2, -1)$

Orthogonal Complements

Find a basis for the orthogonal complement V^\perp for the vector space V given. This technique allows you to find the vectors that are in the plane orthogonal to a line or find the line that is orthogonal to a plane, etc.

27. $V = \langle (1, 0, 2), (0, 1, -2) \rangle$

28. $V = \langle (1, 2, 0, 2), (0, 0, 1, -2) \rangle$

29. $V = \langle (1, 0, 0), (0, 1, 0) \rangle$

30. $V = \langle (1, 0, 1, -1, 2), (0, 1, 2, 2, 2) \rangle$

31. $V = \langle (1, -2, 0, -1, 0, -2), (0, 0, 1, 1, 0, 1), (0, 0, 0, 0, 1, 1) \rangle$

32. $V = \langle (1, 0, 0, 1, 0, -1), (0, 0, 1, 3, 0, 2), (0, 0, 0, 0, 1, 3) \rangle$

33. $V = \langle (1, 4, 0, 3), (0, 0, 1, -4) \rangle$

34. $V = \langle (1, 0, 2, -2, 4), (0, 1, 0, 0, 0) \rangle$

35. $V = \langle (1, 1, 0, 0, 0, -3), (0, 0, 1, 1, 0, 3), (0, 0, 0, 0, 1, 4) \rangle$

36. $V = \langle (1, 5, 0, 2), (0, 0, 1, -6) \rangle$

Proof Practice

37. Prove that the following are symmetric matrices for any matrices A and B for which the following multiplications are well-defined:

(a) $A(BB^T)^{-1}A^T$

(b) $(ABA^T)(AB^TA^T)$

(c) $(A^TBB^TA)^{-1}$

38. Suppose that we have two linear transformations $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ and $g : \mathbb{R}^m \rightarrow \mathbb{R}^k$. Prove that we have the following equality:

$$f^* \circ g^* = (g \circ f)^*$$

39. Let V and W be two subspaces of a vector space. Let B be a basis of V and P be a basis of W . Then prove that $V \perp W$ if and only if $b \perp p$ for all $b \in B$ and $p \in P$.

The Laplacian Matrix

40. Apply the ideas in the section about the Laplacian matrix to find the connected components of the graphs determined by the following:

(a) Incidence Matrix:
$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

(b) Adjacency matrix:

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

5.1.8 Solutions

$$\mathbf{1.} \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 2 \\ -1 & -1 & 1 \end{pmatrix}$$

$$\mathbf{2.} \begin{pmatrix} 0 & 0 & 0 \end{pmatrix}$$

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

$$\mathbf{4.} \begin{pmatrix} 2 & 0 & 0 \\ -2 & -1 & -1 \\ 1 & 2 & 2 \end{pmatrix}$$

$$\mathbf{5.} \begin{pmatrix} 0 & 1 \\ 0 & -2 \end{pmatrix}$$

$$\mathbf{6.} \begin{pmatrix} -1 & -2 \\ 1 & -1 \end{pmatrix}$$

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

$$\mathbf{8.} \begin{pmatrix} 0 & -1 \\ 0 & -1 \end{pmatrix}$$

$$\mathbf{9.} \begin{pmatrix} -2 & 0 \end{pmatrix}$$

$$\mathbf{10.} \begin{pmatrix} 0 & -2 & -2 & 0 \\ -2 & 0 & 1 & 0 \\ -2 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathbf{11.} \sqrt{13}$$

$$\mathbf{12.} \sqrt{5}$$

$$\mathbf{13.} \sqrt{13}$$

$$\mathbf{14.} \sqrt{2}$$

$$\mathbf{15.} \sqrt{5}$$

$$\mathbf{16.} \sqrt{2}$$

$$\mathbf{17.} \sqrt{2}$$

$$\mathbf{18.} \sqrt{5}$$

$$\mathbf{19.} 0$$

$$\mathbf{20.} -\frac{5}{13}\sqrt{13}$$

21. $-\frac{3}{10}\sqrt{10}$

22. $-\frac{5}{6}\sqrt{6}$

23. $\frac{2}{5}\sqrt{5}$

24. $\frac{2}{3}\sqrt{6}$

25. $\frac{4}{3}$

26. $\frac{2}{3}\sqrt{6}$

27. $\langle(-2, 2, 1)\rangle$

28. $\langle(-2, 1, 0, 0),$
 $(-2, 0, 2, 1)\rangle$

29. $\langle(0, 0, 1)\rangle$

30. $\langle(-1, -2, 1, 0, 0),$
 $(1, -2, 0, 1, 0),$
 $(-2, -2, 0, 0, 1)\rangle$

31. $\langle(2, 1, 0, 0, 0, 0),$
 $(1, 0, -1, 1, 0, 0),$
 $(2, 0, -1, 0, -1, 1)\rangle$

32. $\langle(0, 1, 0, 0, 0, 0),$
 $(-1, 0, -3, 1, 0, 0),$
 $(1, 0, -2, 0, -3, 1)\rangle$

33. $\langle(-4, 1, 0, 0),$
 $(-3, 0, 4, 1)\rangle$

34. $\langle(-2, 0, 1, 0, 0),$
 $(2, 0, 0, 1, 0),$
 $(-4, 0, 0, 0, 1)\rangle$

35. $\langle(-1, 1, 0, 0, 0, 0),$
 $(0, 0, -1, 1, 0, 0),$
 $(3, 0, -3, 0, -4, 1)\rangle$

36. $\langle(-5, 1, 0, 0),$
 $(-2, 0, 6, 1)\rangle$

37. In each case, just take the transpose of the expression. Using properties of the transpose and how the transpose interacts with inverses, verify that each expression is equal to its transpose.

38. This is really just understanding notation. Let A be the matrix for f and B the matrix for g both under the column interpretation. Then $(g \circ f)^*$ means the *row* interpretation function for the matrix $\underbrace{B}_{g} \underbrace{A}_{f}$. But if we

think of BA with row interpretation maps, the row interpretation map g^* of B comes first. The result of this is plugged into the row interpretation map f^* of A reading from left to right for row interpretation composition. We have just showed that the row interpretation map for BA is the following composition of row interpretation maps: $f^* \circ g^*$. Of course, realize that we have written the composition as if it were in a column interpretation (right to left). This is because f^* and g^* are the row interpretation maps *written* with matrices in a column interpretation!

39. If $V \perp W$, then it is trivial that the bases will be orthogonal to each other just by the definition of what it means for $V \perp W$. What is more nontrivial is the other direction: if the bases themselves are orthogonal to each other, does this guarantee that the two subspaces will be as well? That is, any vector in V will be orthogonal to any vector in W . Well, let's take an arbitrary vector $v \in V$. It can be written uniquely as a linear combination of the basis elements in B . Say

$$v = a_1 b_1 + \cdots + a_n b_n$$

where $B = \{b_1, \dots, b_n\}$. Similarly, let's take $w \in W$ and write it in terms of the basis $P = \{p_1, \dots, p_m\}$ so that

$$w = k_1 p_1 + \cdots + k_m p_m$$

Now, we know that two vectors are orthogonal to each other if and only if their dot product is 0. Let's take a dot product of v and w :

$$(a_1 b_1 + \cdots + a_n b_n) \bullet (k_1 p_1 + \cdots + k_m p_m)$$

Since the dot product is linear in each component, it splits (distributes) across the addition and the scalars come out. We are left with a linear combination of products $b_i \bullet p_j$. All these products are 0 by our orthogonality assumption. This means that the whole linear combination of products is 0. That is, $v \bullet w = 0$ so that $v \perp w$. Since v and w were arbitrary, $V \perp W$.

40. Solutions/hints by part:

(a) First find the Laplacian matrix $B \cdot B^T$ as:

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

Then, compute its Smith Normal Form

$$\left(\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

keeping track of the column operations. Apply these column operations on the 8×8 identity matrix. One way of applying the column operations will yield:

$$\left(\begin{array}{ccccccc} 0 & -1 & 0 & -2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{array} \right)$$

Notice that there are 4 connected components. We can read these in order from this column operations matrix starting in the fifth column: $\{v_8\}$, $\{v_3, v_6, v_7\}$, $\{v_5\}$, $\{v_1, v_2, v_4\}$.

- (b) We can get the Laplacian matrix directly from the adjacency matrix by replacing what is in the diagonal by whatever we need so that each row adds to 0:

$$\left(\begin{array}{ccccc} -1 & 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 \end{array} \right)$$

We can already see the connected components. But let's work through the details just to check that we

can think through them effectively. We find the Smith Normal Form of this matrix:

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

keeping track of the column operations. The column operations matrix could be:

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

Reading off the 3 connected components starting in the third column, we have: $\{v_1, v_2\}$, $\{v_4\}$, $\{v_3, v_5\}$.

Projections via Right and Left

5.2

Inverses

5.2.1 Decomposing the Domain of a Surjective Linear Transformation	488
5.2.2 Making a Left/Right Inverse Pair for Projections	493
5.2.3 Orthogonal Projections	500
5.2.4 Exercises	507
5.2.5 Solutions	512

Questions to Guide Your Study:

- *How does having a right inverse help to decompose the domain into two distinct parts?*
- *How can we create a linear transformation that projects onto a line at different angles?*
- *What are two methods for finding orthogonal projections?*

5.2.1 Decomposing the Domain of a Surjective Linear Transformation

Given a surjective linear transformation $f : D \rightarrow C$, it has a right inverse g . This right inverse g itself is injective. *Let's think why!* The linear transformation g itself has a *left* inverse. What is that left inverse? The function f . These ideas are found in the equation:

$$f \circ g = \text{id}_C$$

So we know that g is injective. What does that mean? This tells us that g injects the *range* of f back into D . That is, it just transfers the range of f isomorphically back into the domain D . Let's call this injected image in the domain simply $g(C)$ where $C = f(D) = \text{range}(f)$ since f is surjective. This image $g(C)$ is a subspace of D . There is another subspace associated with f inside of the domain D . It is the kernel of f .

Think: $f(\ker(f)) = 0_C$ and $g(0_C) = 0_D$. What does this mean? It means that the kernel is only represented in $g(C)$ right at 0_D . Do you remember that the kernel of f consists of all vectors v such that $f(v) = 0_C$? Also

note that $(f \circ g)(C) = \text{id}_C(C)$. The only way that $(f \circ g)(v) = \text{id}_C(v) = 0_C$ is for $v = 0_C$ so that the only element of $g(C)$ that can possibly be sent to 0_C via f is $g(0_C) = 0_D$. Indeed:

$$\ker(f) \cap g(C) = 0_D.$$

This automatically tells us that there are *no dependencies* from vectors in $g(C)$ to vectors in $\ker(f)$. What does this mean? Suppose that we have a basis for $\ker(f)$ as w_1 and w_2 and a basis for $g(C)$ as v_1 and v_2 . Let's consider linear independence/dependence between these vectors. Take a linear combination

$$a_1w_1 + a_2w_2 + b_1v_1 + b_2v_2 = 0_D.$$

This means that:

$$a_1w_1 + a_2w_2 = b_1v_1 + b_2v_2 \in \ker(f) \cap g(C) = 0_D.$$

Yet, since $\{w_1, w_2\}$ and $\{v_1, v_2\}$ are both linearly independent collections of vectors, then we must have that $a_1 = a_2 = b_1 = b_2 = 0$. This forces $S = \{w_1, w_2, v_1, v_2\}$ to be a linearly independent set of vectors. Not only is it linearly independent, but the dimension of the kernel plus the dimension of the range is equal to the number of columns in a Smith normal form. This is equal to the dimension of the domain. Consequently, S is a basis for D .

We use the notation “ $D = \ker(f) \oplus g(C)$ ” to signify that a basis for D comes from taking a basis from $\ker(f)$ and a basis from $g(C)$ and disjointly putting them together. It means that together $\ker(f)$ and $g(C)$ span D in a linearly independent way. We say D is a “**direct sum** of $\ker(f)$ and $g(C)$.”

⊕ Direct Sum

Let V and W be subspaces of a vector space M . Then we write

$$M = V \bigoplus W$$

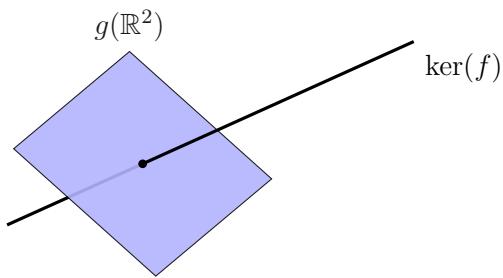
and read “ M is a direct sum of V and W .” This means that a basis for V adjoined with a basis for W is a basis for M . That is, V and W span M in a linearly independent way (to each other).

Theorem 5.2.1 Domain Direct Sum

Let $f : D \rightarrow C$ be a surjective linear transformation and let $g : C \rightarrow D$ be a right inverse. Then,

$$D = g(C) \bigoplus \ker(f).$$

Example 1. Suppose that $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ is a surjective linear transformation and that $g : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ is a right inverse to f . Since f is surjective, $f(\mathbb{R}^3) = \mathbb{R}^2$. Then, g takes \mathbb{R}^2 isomorphically back into \mathbb{R}^3 as a plane $g(\mathbb{R}^2)$ through the origin. The kernel of f and this plane $g(\mathbb{R}^2)$ must span all of \mathbb{R}^3 in a linear independent way. This necessitates that $\ker(f)$ is just a straight line through the origin as depicted:



Example 2. Suppose that $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ is given by

$$\begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

We can arrive at the Smith normal form

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

by *only* doing column operations since every row is a “pivot row” and this is “reduced column echelon form.” One possible column operations matrix is given by:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 & 0 & -2 \\ -1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{\text{Column Operations}}$$

The left two columns of the column operations matrix give a right inverse $g : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ given by:

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

The far right column gives a basis for the $\ker(f)$. In fact, all three columns give a basis for the domain of f which is \mathbb{R}^3 and can be separated as follows:

Column Operations Matrix:

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

$g(\mathbb{R}^2) \oplus \ker(f)$

So really, we are just using the column outputs of the column operations matrix as the basis for the domain of f when we think of this decomposition.

Example 3. Let's use the f and g from the last example. Suppose that have a vector $v \in \mathbb{R}^3$. Then

$$v \in \mathbb{R}^3 = g(\mathbb{R}^2) \bigoplus \ker(f).$$

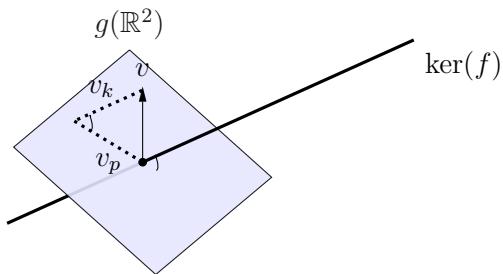
So if c_1, c_2, c_3 are *the columns* of the column operations matrix thought of as vectors, then

$$v = \underbrace{a_1 c_1 + a_2 c_2}_{\in g(\mathbb{R}^2)} + \underbrace{a_3 c_3}_{\in \ker(f)}$$

for unique scalars $a_1, a_2, a_3 \in \mathbb{R}$. Or more simply:

$$v = \underbrace{v_p}_{\in g(\mathbb{R}^2)} + \underbrace{v_k}_{\in \ker(f)}$$

for a unique v_p and v_k . The vector v_p is the unique projection of v onto the plane $g(\mathbb{R}^2)$ such that $v - v_p \in \ker(f)$ —that is, $v_k = v - v_p$ is a vector parallel to the line given by $\ker(f)$. This has a great visualization:



Notice that v_k is depicted parallel to $\ker(f)$. The process of projecting v to v_p is *a projection at the angle* made by $\ker(f)$ and the plane $g(\mathbb{R}^2)$.

Now, notice that

$$f(v - g(f(v))) = f(v) - (f \circ g)(f(v)) = f(v) - \text{id}_C(f(v)) = f(v) - f(v) = 0_C$$

so that $v - (g \circ f)(v) \in \ker(f)$. Remember that v_p is the *unique* projection onto the plane $g(\mathbb{R}^2)$ such that $v - v_p \in \ker(f)$. This uniqueness tells us:

$$v_p = (g \circ f)(v)$$

Then since $v = v_p + v_k$, we know that $v_k = v - v_p$. Let's try this out. Take $v = (1, 0, -1)$ and find

$$\begin{aligned} v_p &= (g \circ f)(v) = \begin{pmatrix} 1 & 0 \\ -1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \end{aligned}$$

So, we know that:

$$\underbrace{(1, 0, -1)}_v = \underbrace{(-1, 1, 0)}_{v_p} + v_k$$

Hence:

$$\underbrace{(1, 0, -1)}_v = \underbrace{(-1, 1, 0)}_{v_p} + \underbrace{(2, -1, -1)}_{v_k}$$

Notice something: $(2, -1, -1)$ is a multiple of the basis vector $(-2, 1, 1)$ we found for the kernel in the last example! This should be expected since v_k should be in the kernel of f which is 1-dimensional.

Theorem 5.2.2 Vector Decomposition

Suppose that $f : D \rightarrow C$ is a surjective linear transformation and that $g : C \rightarrow D$ is a right inverse.

Then given any $v \in D$,

$$v = \underbrace{v_p}_{\in g(C)} + \underbrace{v_k}_{\in \ker(f)}$$

where $v_p = (g \circ f)(v)$ (writing the *right* inverse on the *left*) and $v_k = v - v_p$. This decomposition is unique (which is implied by the fact $D = g(C) \oplus \ker(f)$).

The most important idea of this section can be expressed as follows:

Shadow Vector Function

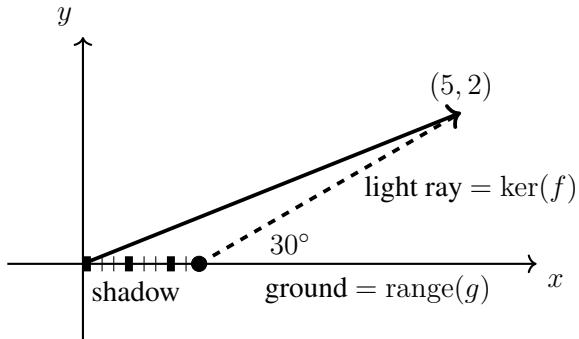
If $g : C \rightarrow D$ is a right inverse to $f : D \rightarrow C$, then *if we think of g on the left instead of the right, we get*

$$\underbrace{g \circ f}_{\text{Shadow Vector Function}}$$

- Input v
- Output the **shadow vector** of v on $\text{range}(g)$ made by light rays parallel to $\ker(f)$.

5.2.2 Making a Left/Right Inverse Pair for Projections

Let's consider projections to the x -axis (this will be $g(C)$) in $D = \mathbb{R}^2$ which are made at 30° .



Let's build $f : D \rightarrow C$ and $g : C \rightarrow D$. Remember:

- $f \circ g = \text{id}_C$
- $g \circ f = (\text{the projection function})$

First, let's focus on the column operations matrix that we would like to have for f if we were putting f into Smith normal form with *only column operations*. Since $\dim(D) = 2$, the column operations matrix for $f : D \rightarrow C$ will be a 2×2 matrix. With our current specifications we could come up with the following column operations matrix. Let's explain how.

Column Operations Matrix That Takes f to Smith Normal Form:

$$\begin{pmatrix} 1 & \sqrt{3} \\ 0 & 1 \end{pmatrix}$$

$g(C) \oplus \ker(f)$

We would like the kernel line to be at 30° . Hence, we could choose $\left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right)$ as a basis vector for the kernel

since it marks 30° on the unit circle. Yet, we can rescale this basis vector to $(\sqrt{3}, 1)$. We choose the basis for $g(C)$ to be $(1, 0)$ since we decided that $g(C)$ should be the x -axis line and $(1, 0)$ is a nice basis for it.

Now, we would like f to be a left inverse to g . The linear transformation g is therefore injective. Since its range $g(C)$ has dimension 1, its domain which is C must also have dimension 1. Hence, $C = \mathbb{R}^1$.

The dimension of the range of an injective linear transformation is equal to the dimension of its domain.

Notice that the codomain of g which is D is \mathbb{R}^2 because the outputs are expressed as vectors in \mathbb{R}^2 . Hence, $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ and $g : \mathbb{R} \rightarrow \mathbb{R}^2$. The matrix for g can simply be taken as the basis for $g(C)$ put into a column matrix:

$$g : \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

The linear transformation f should be represented by a 1×2 matrix such that:

- $\ker(f) = \langle(\sqrt{3}, 1)\rangle$
- $f \circ g = \text{id}_C$ where $C = \mathbb{R}^1$. The matrix for $\text{id}_C = f \circ g$ is therefore $\begin{pmatrix} 1 \end{pmatrix}$.

There are multiple ways of finding the matrix for f .

Method 1: We could think of having the 1×2 matrix for f in reduced row echelon form. This would look like:

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

for some $a \in \mathbb{R}$. Now, the one pivot column is the single entry a . If we want to use our column trick from the reduced row echelon form to find the kernel, we go through the following steps:

$$\begin{pmatrix} 1 & a \end{pmatrix} \rightarrow \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -a \\ 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1+1 & -a \\ 0+1 & 0 \end{pmatrix}; \rightarrow \begin{pmatrix} -a \\ 1 \end{pmatrix}$$

We see that the kernel of f has $(-a, 1)$ as a basis. We already know we want $(\sqrt{3}, 1)$ as a basis so that:

$$\langle(-a, 1)\rangle = (\sqrt{3}, 1)$$

This tells us that $a = -\sqrt{3}$. Hence, if we choose

$$\begin{pmatrix} 1 & a \end{pmatrix} = \begin{pmatrix} 1 & -\sqrt{3} \end{pmatrix}$$

for f , we would have the right kernel.

Alternatively, we could have just observed or guessed that $\begin{pmatrix} 1 & -\sqrt{3} \end{pmatrix}$ would give the right kernel.

Now to make sure $f \circ g$ has $\begin{pmatrix} 1 \end{pmatrix}$ as its matrix, we replace f by $k \cdot \begin{pmatrix} 1 & -\sqrt{3} \end{pmatrix}$ for some constant $k \in \mathbb{R}$ and compute:

$$\begin{pmatrix} 1 \end{pmatrix} = \underbrace{k \cdot \begin{pmatrix} 1 & -\sqrt{3} \end{pmatrix}}_f \cdot \underbrace{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}_g = k$$

and see that $k = 1$. Therefore, the matrix for f is:

$$f : \begin{pmatrix} 1 & -\sqrt{3} \end{pmatrix}$$

Method 2: Simply perform *row* operations to the column operations matrix we found above for putting f into Smith normal form:

Column Operations Matrix:

$$\begin{pmatrix} 1 & \sqrt{3} \\ 0 & 1 \end{pmatrix} \\ g(C) \oplus \ker(f)$$

$$\begin{pmatrix} 1 & \sqrt{3} \\ (-\sqrt{3} \cdot 0) & 0 \\ 0 & (-\sqrt{3} \cdot 1) \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and apply these same steps to the identity matrix on \mathbb{R}^2 :

$$\begin{pmatrix} 1 & 0 \\ (-\sqrt{3} \cdot 0) & 0 \\ 0 & (-\sqrt{3} \cdot 1) \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -\sqrt{3} \\ 0 & 1 \end{pmatrix}$$

Take the top row:

$$\begin{pmatrix} 1 & -\sqrt{3} \\ 0 & 1 \end{pmatrix}$$

This is a good matrix for f :

$$f : \begin{pmatrix} 1 & -\sqrt{3} \end{pmatrix}$$

This is because multiplying by it on the left picks out the top row of the identity matrix:

$$\begin{pmatrix} 1 & -\sqrt{3} \\ f & \in \ker(f) \end{pmatrix} \cdot \begin{pmatrix} 1 & \sqrt{3} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ f \circ g & f(\sqrt{3}, 1) \end{pmatrix}$$

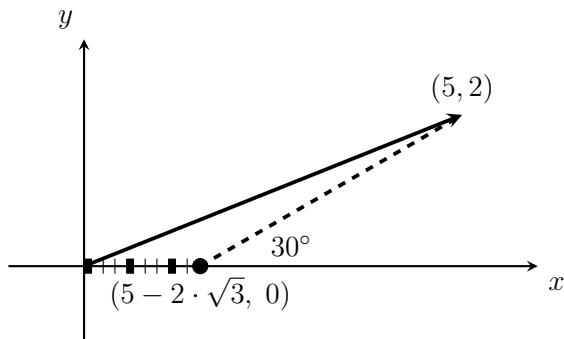
The matrix for f can be taken as the top row of B^{-1} where B is the column operations matrix that takes f to Smith normal form. So if we know B , we can find f .

So what have we accomplished? We have found a left/right inverse pair of matrices f and g such that $(g \circ f)$ (*putting the right inverse g on the left*) tells us how to project onto the x -axis at 30° .

$$(g \circ f) : \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -\sqrt{3} \end{pmatrix} = \begin{pmatrix} 1 & -\sqrt{3} \\ 0 & 0 \end{pmatrix}$$

We can apply this to *any vector* in \mathbb{R}^2 . For instance, to project $(5, 2)$, we obtain:

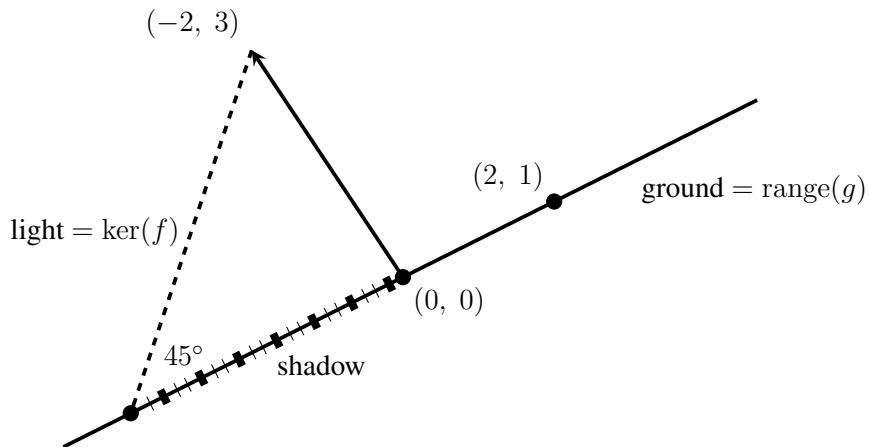
$$\begin{pmatrix} 1 & -\sqrt{3} \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} 5 - 2\sqrt{3} \\ 0 \end{pmatrix}$$



This methodology could potentially be used in graphics to find the coordinate position at which a line exits a desired view window: and even a skewed view window!



Example 4. In the spirit and notation of the last example, Let's find a 45° projection of $(-2, 3)$ onto the line $\langle(2, 1)\rangle$.



This means that we want the range of g to be $\langle(2, 1)\rangle$ and the kernel of f to be $\langle(a, b)\rangle$ where (a, b) is a 45° counterclockwise rotation from $(2, 1)$.

Let's find (a, b) . Counterclockwise rotation can be represented in a column interpretation as:

$$+45^\circ : \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

Therefore, we can take

$$\begin{pmatrix} a \\ b \end{pmatrix} = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

But, for simplicity, note that we can rescale this basis element of the kernel to simply $(1, 3)$. Hence, our column operations matrix might look like:

$$\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \\ g(C) \oplus \ker(f)$$

We are looking for $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ and $g : \mathbb{R} \rightarrow \mathbb{R}^2$. We can let g be given by the matrix $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$. We let f be such that $(f \circ g)$ is given by the matrix $\begin{pmatrix} 1 \end{pmatrix}$ and so that $f(1, 3) = 0$.

Method 1: First, we think:

$$\underbrace{\begin{pmatrix} ? & ? \end{pmatrix}}_f \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

We notice that $\begin{pmatrix} 3 & -1 \end{pmatrix}$ works for $f(1, 3) = 0$. That is, we found something that gives the right kernel by inspection. Yet, we can also again use the fast column kernel technique! We try to find a reduced row echelon form that has $(1, 3)$ in its kernel:

- The vector $\begin{pmatrix} 1 \\ 3 \end{pmatrix}$ came from a *nonpivot* column. Rescale the vector to $\begin{pmatrix} \frac{1}{3} \\ 1 \end{pmatrix}$ and realize that the $+1$ at the bottom came from adding 1 's down the diagonal.
- The top entry $\frac{1}{3}$ was found by negating $-\frac{1}{3}$.
- So the original reduced row echelon form could be $\begin{pmatrix} 1 & -\frac{1}{3} \end{pmatrix}$. This is just a rescaling of what we found by inspection: $\begin{pmatrix} 3 & -1 \end{pmatrix}$.

We have the kernel right. Now we need the matrix for $f \circ g$ to be $\begin{pmatrix} 1 \end{pmatrix}$. So, we rescale $\begin{pmatrix} 3 & -1 \end{pmatrix}$ by multiplying by a scalar k so that

$$k \cdot \begin{pmatrix} 3 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \end{pmatrix}$$

Note that this is: $k \cdot (3 \cdot 2 - 1 \cdot 1) = 1$ so that $k = \frac{1}{5}$. Hence:

$$f : \begin{pmatrix} \frac{3}{5} & -\frac{1}{5} \end{pmatrix} \quad g : \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

Method 2: To find f , we could have found the inverse of the column operations matrix by *only using row operations*:

$$\begin{array}{ccc} \left(\begin{array}{cc} 2 & 1 \\ 1 & 3 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & 3 \\ -2 \cdot 1 & -2 \cdot 3 \\ 2 & 1 \end{array} \right) \\ \left(\begin{array}{cc} 1 & 3 \\ \frac{1}{5} \cdot 0 & \frac{1}{5} \cdot -5 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & 3 \\ -3 \cdot 0 & -3 \cdot 1 \\ 0 & 1 \end{array} \right) \\ \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) & & \end{array}$$

Now we apply these same row operations to the identity matrix:

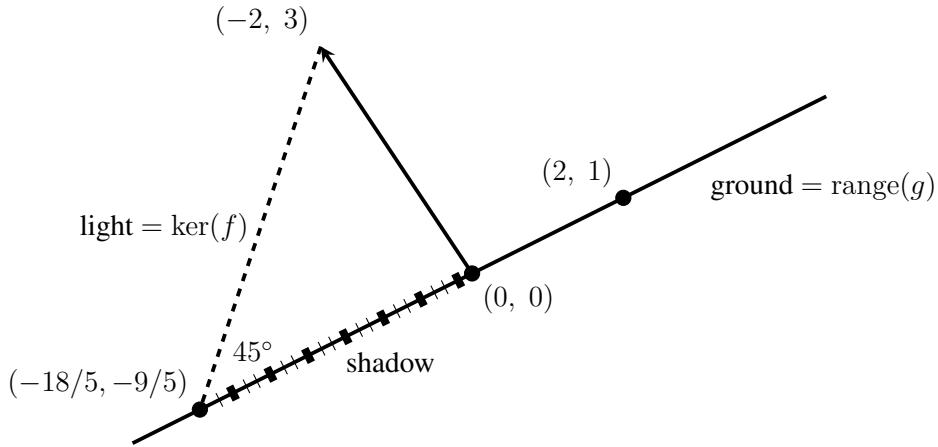
$$\begin{array}{ccc} \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 0 & 1 \\ -2 \cdot 0 & -2 \cdot 1 \\ 1 & 0 \end{array} \right) \\ \left(\begin{array}{cc} 0 & 1 \\ \frac{1}{5} \cdot 1 & \frac{1}{5} \cdot -2 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 0 & 1 \\ -3 \cdot \left(-\frac{1}{5}\right) & -3 \cdot \left(\frac{2}{5}\right) \\ -\frac{1}{5} & \frac{2}{5} \end{array} \right) \\ \left(\begin{array}{cc} \frac{3}{5} & -\frac{1}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{array} \right) & & \end{array}$$

Taking the top line of this matrix, we again see:

$$f : \begin{pmatrix} \frac{3}{5} & -\frac{1}{5} \end{pmatrix}$$

Now, to find our desired projection, we compute:

$$(g \circ f)(-2, 3) = \underbrace{\begin{pmatrix} 2 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{3}{5} & -\frac{1}{5} \end{pmatrix}}_{g \circ f} \cdot \begin{pmatrix} -2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} -\frac{9}{5} \\ -\frac{9}{5} \end{pmatrix} = \begin{pmatrix} -\frac{18}{5} \\ -\frac{9}{5} \end{pmatrix}.$$



Angled Projections in \mathbb{R}^2

To find a function that projects a vector onto a line $\langle(a, b)\rangle$ via lines parallel to $\langle(c, d)\rangle$, we compute:

$$\underbrace{\begin{pmatrix} a \\ b \end{pmatrix}}_g \cdot \underbrace{\begin{pmatrix} t & w \end{pmatrix}}_f$$

where

$$\underbrace{\begin{pmatrix} t & w \end{pmatrix}}_f \cdot \begin{pmatrix} c \\ d \end{pmatrix} = 0$$

and $f \circ g$ is given by the matrix $\begin{pmatrix} 1 \end{pmatrix}$. To find f :

- Method 1: Either use inspection to make sure $\underbrace{\begin{pmatrix} t & w \end{pmatrix}}_f \cdot \begin{pmatrix} c \\ d \end{pmatrix} = 0$ or think of the fast column technique for finding a basis vector for the kernel of $\underbrace{\begin{pmatrix} t & w \end{pmatrix}}_f$. Then rescale to make sure that f is a left inverse to g .
- Method 2: Let f be the top row of the inverse matrix:

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1}$$

5.2.3 Orthogonal Projections

The angled projections we have seen thus far are skewed—but projections that work at right angles, called *orthogonal* projections, take on a very nice form. Let's look at an example. What if we want to just project to the x -axis and we wanted the y -axis itself to have no projection at all to it? That is, we would like the y -axis which appears at a right angle to be the kernel of f . We could set up our column operations matrix as

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad g(C) \oplus \ker(f)$$

In this case g is given by $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and f is given by $\begin{pmatrix} 1 & 0 \end{pmatrix}$. That is, f and g represent the same vector $(1, 0)$ (they are just transposes of each other)! The projection function onto the x -axis is given by

$$g \circ f : \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

a symmetric matrix!.

Let's try this in another situation. What if we want to project to the line $\langle(1, 2)\rangle$ letting f and g again be the same vector. So let g be $k \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ for some scalar k . We do this because all we know so far is that we want the range of g to be $\langle(1, 2)\rangle$ but we want to strategically choose f and g so they are the same. Hence, we simply know at first that the one column of g is a multiple of $(1, 2)$. We would like f to be this same vector: $k \cdot \begin{pmatrix} 1 & 2 \end{pmatrix}$. We need that $(f \circ g) = \text{id}_{\mathbb{R}}$ which is given by the 1×1 matrix $\begin{pmatrix} 1 \end{pmatrix}$. We solve for k :

$$k \cdot \begin{pmatrix} 1 & 2 \end{pmatrix} \cdot k \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \end{pmatrix}$$

$$5k^2 = 1 \implies k = \frac{1}{\sqrt{5}}.$$

So this means that the projection function is

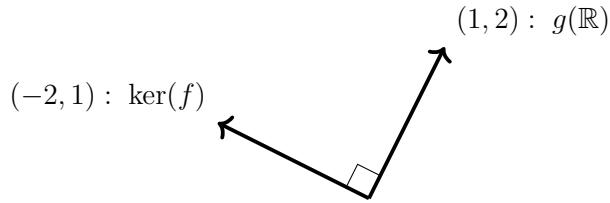
$$\underbrace{\frac{1}{\sqrt{5}} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix}}_g \cdot \underbrace{\frac{1}{\sqrt{5}} \cdot \begin{pmatrix} 1 & 2 \end{pmatrix}}_f = \frac{1}{5} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$$

again a symmetric matrix!

Notice that $\ker(f)$ found by the fast column technique or inspection on $\frac{1}{\sqrt{5}} \cdot \begin{pmatrix} 1 & 2 \end{pmatrix}$ is $\langle(-2, 1)\rangle$ upon

rescaling. An illustration of the column technique for finding a kernel basis is as follows:

$$\begin{pmatrix} 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -2 \\ 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1+1 & -2 \\ 0 & +1 \end{pmatrix} \rightarrow (-2, 1)$$



Notice that $\ker(f)$ appears at a right angle.

Note that $\begin{pmatrix} 1 & 2 \end{pmatrix} \cdot \underbrace{w}_{\text{column}} = (1, 2) \bullet w = 0$ is the same as saying that w is orthogonal to $(1, 2)$ and this is the same as saying that w is in the kernel of the matrix function $\begin{pmatrix} 1 & 2 \end{pmatrix}$ under the column interpretation. That is, the kernel of the matrix function $\begin{pmatrix} 1 & 2 \end{pmatrix}$ is orthogonal to $(1, 2)$.

So really, if f and g represent the same vector, we really do get a right-angled projection. Let's look at this a little further. We had in this last example a vector $v = \frac{1}{\sqrt{5}} \cdot (1, 2)$ where g is given by the *column* vector v and f is given by the *row* vector v^T . Note that v is a unit vector. Yet this *has to be true if* $f \circ g = \text{id}_{\mathbb{R}}$ which means that $v^T v = 1$ or simply $v^T v = v \bullet v = |v|^2 = 1$. When we compute the projection of w onto v , we compute

$$(g \circ f)(w) = v \cdot v^T \cdot w = v \cdot (v \bullet w)$$

In general, if v is not given as unit vector, we need to rescale it to a unit vector kv because f and g need to be a left/right inverse pair: $f \circ g = \text{id}_{\mathbb{R}}$ which is the same as saying $(kv)^T \cdot kv = 1$. We use $k = \frac{1}{\sqrt{v \bullet v}}$ and then calculate the projection of w on the vector v as:

$$\frac{1}{\sqrt{v \bullet v}} v \cdot \left(\frac{1}{\sqrt{v \bullet v}} v \bullet w \right) = \underbrace{\left(\frac{v \bullet w}{v \bullet v} \right)}_{\text{comp}_v w} \cdot v$$

That is, this projection is v rescaled to the amount that equals the orthogonal projection length of w on v .

We call this the *orthogonal projection* of w on v :

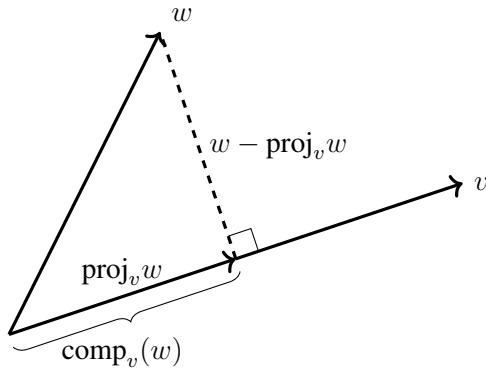
proj_vw via Dot Product

The orthogonal projection of w on v is given as:

$$\text{proj}_v w = \left(\frac{v \bullet w}{v \bullet v} \right) v = \underbrace{\frac{v}{|v|}}_{\text{comp}_v w} \bullet w \underbrace{\frac{v}{|v|}}_{\text{comp}_v w}$$

and represents the unit vector $\frac{v}{|v|}$ rescaled by comp_vw.

The difference between comp_vw and proj_vw is that comp_vw is a scalar “projection length” and proj_vw is a vector: $\frac{v}{|v|}$ rescaled by comp_vw.



From the picture, $(w - \text{proj}_v w)$ and v are orthogonal to each other. Indeed, computationally:

$$(w - \text{proj}_v w) \bullet v = \left(w - \left(\frac{v \bullet w}{v \bullet v} \right) v \right) \bullet v = w \bullet v - \frac{v \bullet w}{v \bullet v} \cdot (v \bullet v) = 0$$

Remember that projecting a vector $w \in \mathbb{R}^2$ onto the subspace $\langle v \rangle$ orthogonally is a linear transformation $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ with range $\langle v \rangle$. The matrix which describes this linear transformation is of the form $g \circ f$ discussed above. Turn v into a unit vector by replacing v with:

$$\frac{1}{\sqrt{v \bullet v}} v = \frac{1}{\sqrt{v^T v}} v$$

Then, g is given by $\frac{1}{\sqrt{v^T v}} v$ thought of as a column and f is given by the same vector thought of as a row. So the matrix for f will be the transpose of what it is for g . Under a column interpretation, the matrix for $g \circ f$ is given by:

$$g \circ f : \underbrace{\frac{1}{\sqrt{v^T v}} v}_{g} \cdot \underbrace{\left(\frac{1}{\sqrt{v^T v}} v \right)^T}_{f} = \frac{vv^T}{v^T v}$$

Matrix for Orthogonal Projection proj_v

The matrix function that describes the orthogonal projection onto $\langle v \rangle$ is given in a column interpretation by the matrix:

$$\frac{vv^T}{v^Tv}$$

Remember that v^Tv can be thought of as a scalar—that is why we can just write it like this in a denominator. We are just dividing the matrix vv^T by the scalar v^Tv . *This formulation looks cool!* Since this matrix itself is symmetric, it also gives projection via a *row* projection.



Example 5. Suppose that we would like to find the orthogonal projection of $w = (2, 3)$ onto $v = (-1, 4)$.

Using Dot Product:

$$\frac{v \bullet w}{v \bullet v} v = \frac{2 \cdot (-1) + 3 \cdot 4}{(-1)^2 + 4^2} v = \frac{10}{17} v$$

Using the matrix for proj_v : Remember that $v^Tv = v \bullet v = 17$

$$\frac{vv^T}{v^Tv} w = \frac{\begin{pmatrix} -1 \\ 4 \end{pmatrix} \cdot \begin{pmatrix} -1 & 4 \end{pmatrix}}{17} w = \frac{1}{17} \begin{pmatrix} 1 & -4 \\ -4 & 16 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 2 \\ 3 \end{pmatrix}}_w = \frac{1}{17} \begin{pmatrix} -10 \\ 40 \end{pmatrix} = \frac{10}{17} \cdot \underbrace{\begin{pmatrix} -1 \\ 4 \end{pmatrix}}_v$$

Using the matrix for proj_v multiplied by a row is the same:

$$w^T \frac{vv^T}{v^Tv} = \underbrace{\begin{pmatrix} 2 & 3 \end{pmatrix}}_{w^T} \cdot \begin{pmatrix} 1 & -4 \\ -4 & 16 \end{pmatrix} \cdot \frac{1}{17} = \frac{1}{17} \begin{pmatrix} -10 \\ 40 \end{pmatrix} = \frac{10}{17} \cdot \underbrace{\begin{pmatrix} -1 \\ 4 \end{pmatrix}}_v$$

Comparison Between Orthogonal Methods

If we will be changing which vector w to project to v often, then we can think about the two methods with a box for what will be varying:

$$\frac{v \bullet \square}{v \bullet v} v = \frac{vv^T}{v^T v} \square$$

The second formulation has the advantage that \square is just the input of a matrix function. The output of this matrix function is everything that we want. The first formulation has \square inside of a dot product. The components of v are then multiplied by the fraction of two dot products. The advantage of this technique is that one only has to consider *dot products* instead of multiplication of a matrix and a column vector.

You can always find a projection matrix by just knowing the destinations of e_1, e_2 , etc. *This section has given us some alternate techniques! These techniques will be useful as we look at the Gram Schmidt process in the next section.*

Key Concepts from this Section

- **direct sum:** (page 489) A direct sum of two vector spaces V and W is a vector space M where a basis for V adjoined with a basis for W is a basis for M . That is, V and W span M in a linearly independent way (to each other).
- **\oplus direct sum:** (page 489) Let V and W be subspaces of a vector space M . Then we write

$$M = V \bigoplus W$$

and read “ M is a direct sum of V and W .” This means that a basis for V adjoined with a basis for W is a basis for M . That is, V and W span M in a linearly independent way (to each other).

- **theorem 5.2.1 domain direct sum:** (page 489) Let $f : D \rightarrow C$ be a surjective linear transformation and let $g : C \rightarrow D$ be a right inverse. Then,

$$D = g(C) \bigoplus \ker(f).$$

- **theorem 5.2.2 vector decomposition:** (page 492) Suppose that $f : D \rightarrow C$ is a surjective linear transformation and that $g : C \rightarrow D$ is a right inverse. Then given any $v \in D$,

$$v = \underbrace{v_p}_{\in g(C)} + \underbrace{v_k}_{\in \ker(f)}$$

where $v_p = (g \circ f)(v)$ (writing the *right* inverse on the *left*) and $v_k = v - v_p$. This decomposition is unique (which is implied by the fact $D = g(C) \oplus \ker(f)$).

- **shadow vector function:** (page 492) If $g : C \rightarrow D$ is a right inverse to $f : D \rightarrow C$, then *if we think of g on the left instead of the right*, we get

$$\underbrace{g \circ f}_{\text{Shadow Vector Function}}$$

- **Input v**
- **Output the shadow vector of v on range(g) made by light rays parallel to $\ker(f)$.**

- **angled projections in \mathbb{R}^2 :** (page 499) To find a function that projects a vector onto a line $\langle(a, b)\rangle$ via lines parallel to $\langle(c, d)\rangle$, we compute:

$$\underbrace{\begin{pmatrix} a \\ b \end{pmatrix}}_g \cdot \underbrace{\begin{pmatrix} t & w \end{pmatrix}}_f$$

where

$$\underbrace{\begin{pmatrix} t & w \end{pmatrix}}_f \cdot \begin{pmatrix} c \\ d \end{pmatrix} = 0$$

and $f \circ g$ is given by the matrix $\begin{pmatrix} 1 \end{pmatrix}$. To find f :

- Method 1: Either use inspection to make sure $\underbrace{\begin{pmatrix} t & w \end{pmatrix}}_f \cdot \begin{pmatrix} c \\ d \end{pmatrix} = 0$ or think of the fast column technique for finding a basis vector for the kernel of $\underbrace{\begin{pmatrix} t & w \end{pmatrix}}_f$. Then rescale to make sure that f is a left inverse to g .
- Method 2: Let f be the top row of the inverse matrix:

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1}$$

- **orthogonal projection:** (page 501) The orthogonal projection of w on v represents the unit vector $\frac{v}{|v|}$ rescaled by $\text{comp}_v w$.
- **$\text{proj}_v w$ via dot product:** (page 501) The orthogonal projection of w on v is given as:

$$\text{proj}_v w = \left(\frac{v \bullet w}{v \bullet v} \right) v = \underbrace{\frac{v}{|v|}}_{\text{comp}_v w} \bullet w \frac{v}{|v|}$$

and represents the unit vector $\frac{v}{\|v\|}$ rescaled by $\text{comp}_v w$.

- **matrix for orthogonal projection proj_v :** (page 502) The matrix function that describes the orthogonal projection onto $\langle v \rangle$ is given in a column interpretation by the matrix:

$$\frac{vv^T}{v^Tv}$$

Remember that v^Tv can be thought of as a scalar—that is why we can just write it like this in a denominator. We are just dividing the matrix vv^T by the scalar v^Tv . *This formulation looks cool!* Since this matrix itself is symmetric, it also gives projection via a *row* projection.

- **comparison between orthogonal methods:** (page 503) If we will be changing which vector w to project to v often, then we can think about the two methods with a box for what will be varying:

$$\frac{v \bullet \square}{v \bullet v} v = \frac{vv^T}{v^Tv} \square$$

The second formulation has the advantage that \square is just the input of a matrix function. The output of this matrix function is everything that we want. The first formulation has \square inside of a dot product. The components of v are then multiplied by the fraction of two dot products. The advantage of this technique is that one only has to consider *dot products* instead of multiplication of a matrix and a column vector.

5.2.4 Exercises

Projecting a Vector onto $\text{range}(g)$ via $\ker(f)$

In the following exercises, f is a left inverse to g and g is a right inverse to f . Find the unique decomposition of v as $v = \underbrace{v_p}_{\in \text{range}(g)} + \underbrace{v_k}_{\in \ker(f)}$.

1. $v = (-1, -2, 0)$

$$f : \begin{pmatrix} -1 & -1 & -2 \\ 0 & -2 & -2 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{1}{2} & \frac{3}{8} \\ \frac{1}{2} & -\frac{5}{8} \\ -\frac{1}{2} & \frac{1}{8} \end{pmatrix}$$

2. $v = (0, 1, 0)$

$$f : \begin{pmatrix} 0 & -2 & 2 \\ 1 & 0 & 0 \end{pmatrix}$$

$$g : \begin{pmatrix} 0 & 1 \\ -\frac{1}{6} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

3. $v = (2, -2, 1)$

$$f : \begin{pmatrix} 1 & 2 & -1 \\ -1 & 2 & 1 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{4} & \frac{1}{4} \\ -1 & 0 \end{pmatrix}$$

4. $v = (0, 2, 2)$

$$f : \begin{pmatrix} -2 & 0 & -1 \\ -1 & 2 & -1 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{2}{5} & \frac{1}{5} \\ -\frac{3}{10} & \frac{2}{5} \\ -\frac{1}{5} & -\frac{2}{5} \end{pmatrix}$$

5. $v = (0, 0, 0)$

$$f : \begin{pmatrix} -2 & 2 & -2 \\ -2 & 2 & 2 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{1}{4} & -\frac{1}{12} \\ 0 & \frac{1}{6} \\ -\frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

6. $v = (0, 0, 1)$

$$f : \begin{pmatrix} 2 & 1 & 1 \\ -1 & 2 & -1 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{1}{2} & 1 \\ \frac{1}{2} & 0 \\ \frac{3}{2} & -2 \end{pmatrix}$$

7. $v = (0, 0, -1)$

$$f : \begin{pmatrix} -1 & -1 & -1 \\ -1 & 2 & 2 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{2}{3} & -\frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \\ -\frac{2}{3} & -\frac{1}{3} \end{pmatrix}$$

8. $v = (-1, -1, -2)$

$$f : \begin{pmatrix} 2 & 2 & 1 \\ 0 & 2 & -1 \end{pmatrix}$$

$$g : \begin{pmatrix} \frac{3}{14} & -\frac{1}{14} \\ \frac{1}{7} & \frac{2}{7} \\ \frac{2}{7} & -\frac{3}{7} \end{pmatrix}$$

9. $v = (-2, 0, -1)$

$$f : \begin{pmatrix} 2 & -1 & 1 \\ -1 & -1 & 0 \end{pmatrix}$$

$$g : \begin{pmatrix} \frac{2}{3} & 0 \\ -\frac{2}{3} & -1 \\ -1 & -1 \end{pmatrix}$$

10. $v = (2, 1, 2)$

$$f : \begin{pmatrix} -2 & -2 & 2 \\ 1 & 2 & 1 \end{pmatrix}$$

$$g : \begin{pmatrix} 0 & \frac{1}{2} \\ -\frac{1}{6} & 0 \\ \frac{1}{3} & \frac{1}{2} \end{pmatrix}$$

11. $v = (-1, 0, 2)$

$$f : \begin{pmatrix} 0 & -1 & 1 \\ -1 & 0 & -2 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{2}{3} & -\frac{1}{3} \\ -\frac{2}{3} & -\frac{1}{3} \\ \frac{1}{3} & -\frac{1}{3} \end{pmatrix}$$

12. $v = (-1, -1, 0)$

$$f : \begin{pmatrix} 2 & 0 & 0 \\ -1 & 2 & 0 \end{pmatrix}$$

$$g : \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{1}{4} & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$$

13. $v = (-1, 2, -2)$

$$f : \begin{pmatrix} -1 & 0 & 0 \\ 2 & -2 & 2 \end{pmatrix}$$

$$g : \begin{pmatrix} -1 & 0 \\ -\frac{3}{4} & -\frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

14. $v = (0, 2, -2)$

$$f : \begin{pmatrix} 1 & -2 & 2 \\ -1 & 0 & 1 \end{pmatrix}$$

$$g : \begin{pmatrix} \frac{1}{3} & 0 \\ 0 & 1 \\ \frac{1}{3} & 1 \end{pmatrix}$$

15. $v = (-1, 1, 0)$

$$f : \begin{pmatrix} -2 & -2 & 2 \\ -2 & -1 & 2 \end{pmatrix}$$

$$g : \begin{pmatrix} \frac{3}{2} & -2 \\ -1 & 1 \\ 1 & -1 \end{pmatrix}$$

16. $v = (-2, -1, 0)$

$$f : \begin{pmatrix} -1 & 2 & 0 \\ -2 & 0 & -1 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{1}{7} & -\frac{2}{7} \\ \frac{3}{7} & -\frac{1}{7} \\ \frac{2}{7} & -\frac{3}{7} \end{pmatrix}$$

17. $v = (-1, 1, -2)$

$$f : \begin{pmatrix} -2 & -2 & -2 \\ 1 & -2 & 2 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{1}{7} & -\frac{3}{7} \\ -\frac{3}{14} & -\frac{1}{7} \\ -\frac{1}{7} & \frac{4}{7} \end{pmatrix}$$

18. $v = (-2, -1, 2)$

$$f : \begin{pmatrix} -1 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{3}{10} & \frac{2}{5} \\ \frac{1}{10} & \frac{1}{5} \\ \frac{1}{2} & 0 \end{pmatrix}$$

19. $v = (-2, 2, 0)$

$$f : \begin{pmatrix} -1 & 0 & -1 \\ 2 & 0 & -1 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{1}{3} & \frac{1}{3} \\ -\frac{1}{3} & \frac{1}{3} \\ -\frac{2}{3} & -\frac{1}{3} \end{pmatrix}$$

20. $v = (0, 1, 2)$

$$f : \begin{pmatrix} 1 & -2 & -1 \\ 0 & 2 & -2 \end{pmatrix}$$

$$g : \begin{pmatrix} \frac{1}{7} & -\frac{2}{7} \\ -\frac{2}{7} & \frac{1}{14} \\ -\frac{2}{7} & -\frac{3}{7} \end{pmatrix}$$

Angled and Orthogonal Projections

For the following, find the unique matrix function (in a column interpretation) that tells how to project a vector in \mathbb{R}^2 onto the subspace $\langle v \rangle \subset \mathbb{R}^2$ given via “light rays” that are an angle θ counterclockwise rotation from v . That is, we are looking for the matrix describing $g \circ f$ where g is a *right* inverse to f , $\text{range}(g) = \langle v \rangle$, and $\ker(f)$ describes the direction of the “light rays.” This matrix function outputs the **shadow vector on the ground** $\langle v \rangle$.

21. Subspace = $\langle(0, 1)\rangle$

Angle: 45°

22. Subspace = $\langle(1, 0)\rangle$

Angle: 60°

23. Subspace = $\langle(0, 1)\rangle$

Angle: 60°

24. Subspace = $\langle(1, 0)\rangle$

Angle: 30°

25. Subspace = $\langle(-2, 2)\rangle$

Angle: 45°

26. Subspace = $\langle(2, -2)\rangle$

Angle: 45°

27. Subspace = $\langle(2, -1)\rangle$

Angle: 45°

28. Subspace = $\langle(1, -1)\rangle$

Angle: 45°

29. Subspace = $\langle(-1, -1)\rangle$

Angle: 45°

30. Subspace = $\langle(-2, -2)\rangle$

Angle: 90°

31. Subspace = $\langle(1, 1)\rangle$

Angle: 90°

32. Subspace = $\langle(2, -1)\rangle$

Angle: 90°

33. Subspace = $\langle(-2, -1)\rangle$

Angle: 90°

34. Subspace = $\langle(-1, -1)\rangle$

Angle: 90°

Orthogonal Projections

For each of the following, find the orthogonal projection vector $\text{proj}_v w$ of w onto the line $\langle v \rangle$.

35. $v = (2, -1)$

$$w = (-2, 1)$$

36. $v = (-3, -3)$

$$w = (-2, 2)$$

37. $v = (-1, 1)$

$$w = (2, -2)$$

38. $v = (-1, -1)$

$$w = (1, -1)$$

39. $v = (1, 3)$

$$w = (1, -1)$$

40. $v = (3, -2)$

$$w = (2, -2)$$

41. $v = (1, -2)$

$$w = (-3, 2)$$

42. $v = (-3, 3)$

$$w = (1, -2)$$

43. $v = (2, -1)$

$$w = (-3, -3)$$

44. $v = (-2, -2)$

$$w = (1, -3)$$

45. $v = (-3, -1)$

$$w = (3, -2)$$

46. $v = (-1, 2)$

$$w = (-2, 3)$$

$$\mathbf{47.} \quad v = (-3, 3)$$

$$w = (-2, 2)$$

$$\mathbf{48.} \quad v = (-3, -1)$$

$$w = (1, -1)$$

$$\mathbf{49.} \quad v = (-2, -1)$$

$$w = (-3, -3)$$

$$\mathbf{50.} \quad v = (3, -3)$$

$$w = (-2, -2)$$

$$\mathbf{51.} \quad v = (-1, 2)$$

$$w = (1, 3)$$

$$\mathbf{52.} \quad v = (1, 1)$$

$$w = (1, 3)$$

$$\mathbf{53.} \quad v = (1, -2)$$

$$w = (-3, -1)$$

$$\mathbf{54.} \quad v = (-3, -2)$$

$$w = (3, -3)$$

5.2.5 Solutions

1. $(0, -1, -1) + (-1, -1, 1)$

2. $(0, \frac{1}{3}, -\frac{2}{3}) + (0, \frac{2}{3}, \frac{2}{3})$

3. $(4, -2, 3) + (-2, 0, -2)$

4. $(\frac{6}{5}, \frac{7}{5}, -\frac{2}{5}) + (-\frac{6}{5}, \frac{3}{5}, \frac{12}{5})$

5. $(0, 0, 0) + (0, 0, 0)$

6. $(-\frac{3}{2}, \frac{1}{2}, \frac{7}{2}) + (\frac{3}{2}, -\frac{1}{2}, -\frac{5}{2})$

7. $(0, -1, 0) + (0, 1, -1)$

8. $(-\frac{9}{7}, -\frac{6}{7}, -\frac{12}{7}) + (\frac{2}{7}, -\frac{1}{7}, -\frac{2}{7})$

9. $(-\frac{10}{3}, \frac{4}{3}, 3) + (\frac{4}{3}, -\frac{4}{3}, -4)$

10. $(3, \frac{1}{3}, \frac{7}{3}) + (-1, \frac{2}{3}, -\frac{1}{3})$

11. $(-\frac{1}{3}, -\frac{1}{3}, \frac{5}{3}) + (-\frac{2}{3}, \frac{1}{3}, \frac{1}{3})$

12. $(-1, -1, -2) + (0, 0, 2)$

13. $(-1, \frac{7}{4}, -\frac{9}{4}) + (0, \frac{1}{4}, \frac{1}{4})$

14. $(-\frac{8}{3}, -2, -\frac{14}{3}) + (\frac{8}{3}, 4, \frac{8}{3})$

15. $(-2, 1, -1) + (1, 0, 1)$

16. $(-\frac{8}{7}, -\frac{4}{7}, -\frac{12}{7}) + (-\frac{6}{7}, -\frac{3}{7}, \frac{12}{7})$

17. $(\frac{17}{7}, \frac{1}{7}, -\frac{32}{7}) + (-\frac{24}{7}, \frac{6}{7}, \frac{18}{7})$

18. $(-\frac{9}{5}, -\frac{2}{5}, 1) + (-\frac{1}{5}, -\frac{3}{5}, 1)$

19. $(-2, -2, 0) + (0, 4, 0)$

20. $(0, 1, 2) + (0, 0, 0)$

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

22. $\begin{pmatrix} 1 & -\frac{1}{3}\sqrt{3} \\ 0 & 0 \end{pmatrix}$

23. $\begin{pmatrix} 0 & 0 \\ \frac{1}{3}\sqrt{3} & 1 \end{pmatrix}$

24. $\begin{pmatrix} 1 & -\sqrt{3} \\ 0 & 0 \end{pmatrix}$

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

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

27. $\begin{pmatrix} \frac{2}{5} & -\frac{6}{5} \\ -\frac{1}{5} & \frac{3}{5} \end{pmatrix}$

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

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

30. $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

31. $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

32. $\begin{pmatrix} \frac{4}{5} & -\frac{2}{5} \\ -\frac{2}{5} & \frac{1}{5} \end{pmatrix}$

33. $\begin{pmatrix} \frac{4}{5} & \frac{2}{5} \\ \frac{2}{5} & \frac{1}{5} \end{pmatrix}$

34. $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

35. $(-2, 1)$

36. $(0, 0)$

37. $(2, -2)$

38. $(0, 0)$

39. $(-\frac{1}{5}, -\frac{3}{5})$

40. $(\frac{30}{13}, -\frac{20}{13})$

41. $(-\frac{7}{5}, \frac{14}{5})$

42. $(\frac{3}{2}, -\frac{3}{2})$

43. $(-\frac{6}{5}, \frac{3}{5})$

44. $(-1, -1)$

45. $(\frac{21}{10}, \frac{7}{10})$

46. $(-\frac{8}{5}, \frac{16}{5})$

47. $(-2, 2)$

48. $(\frac{3}{5}, \frac{1}{5})$

49. $(-\frac{18}{5}, -\frac{9}{5})$

50. $(0, 0)$

$$\mathbf{51.} (-1, 2)$$

$$\mathbf{52.} (2, 2)$$

$$\mathbf{53.} \left(-\frac{1}{5}, \frac{2}{5}\right)$$

$$\mathbf{54.} \left(\frac{9}{13}, \frac{6}{13}\right)$$

Gram-Schmidt Orthogonalization

5.3

5.3.1 Orthogonal Right Inverses	515
5.3.2 Iterative Procedure using Matrices	518
5.3.3 Iterative Procedure Using Dot Product	523
5.3.4 Orthonormal Bases	525
5.3.5 QR Decomposition	526
5.3.6 LQ Decomposition	533
5.3.7 Exercises	538
5.3.8 Solutions	541

Questions to Guide Your Study:

- *What is an orthogonal right inverse?*
- *What is the Gram Schmidt process and how does it help us?*
- *How do we go through the Gram Schmidt process with matrices?*
- *How do we go through the Gram Schmidt process with dot products?*
- *What is an orthogonal versus an orthonormal basis?*
- *What is QR decomposition and how does it work?*

5.3.1 Orthogonal Right Inverses

We are going to discuss how we can create a left/right inverse pair f and g that gives an orthogonal projection when f has more than one row! This is essential to what will follow. We want to develop a technique that will turn a whole collection of linearly independent vectors into a collection where each vector is orthogonal to every other in that collection. This process *will not change the span of the vectors!*

So, in order to discuss just how to come up with a good right inverse g that will do the trick if f has many rows (which are pairwise orthogonal), we need to build up a few ideas.

Row Space

The row space $\text{row}(A)$ of a matrix A can be equivalently described in any of the following ways:

- the span of the rows
- the range of A under a *row interpretation*
- the range of A^T under a *column interpretation*

Theorem 5.3.1 Kernel Orthogonal to Row Space

Suppose that A is a matrix describing a linear transformation f under a column interpretation. Then $\ker(f) \perp \text{row}(A)$.

Proof. Let v_1, v_2, \dots, v_n be vectors representing the rows of A (but thought of as column vectors since by default we naturally assume a vector is a column). Then, the rows of A are given by the *row vectors* $v_1^T, v_2^T, \dots, v_n^T$. Let's use a (total) row partition of A in a block multiplication of $A \cdot w$ to see:

$$A \cdot w = \begin{pmatrix} v_1^T \\ v_2^T \\ \vdots \\ v_n^T \end{pmatrix} \cdot w = \begin{pmatrix} v_1^T \bullet w \\ v_2^T \bullet w \\ \vdots \\ v_n^T \bullet w \end{pmatrix} = \begin{pmatrix} v_1 \bullet w \\ v_2 \bullet w \\ \vdots \\ v_n \bullet w \end{pmatrix}$$

The vector w will be in $\ker(f)$ if and only if $A \cdot w$ is equal the zero vector in the codomain. This happens if and only if $v_k \bullet w = 0$ for all $k \in \{1, 2, \dots, n\}$. Since a spanning set for $\text{row}(A)$ is orthogonal to $\ker(f)$, we must have that $\text{row}(A) \perp \ker(f)$. \square

Let's see how we can find a right inverse for a matrix if we know that its rows are orthogonal to each other.

Suppose that we have two vectors $v_1 = (1, 0, 1)$ and $v_2 = (1, 1, -1)$ which are orthogonal to each other (since $v_1 \bullet v_2 = 0$). Let $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ be the linear transformation described by the matrix $A = \begin{pmatrix} v_1^T \\ v_2^T \end{pmatrix} =$

$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & -1 \end{pmatrix}$ under a column interpretation. Then, notice that

$$AA^T = \left(\frac{v_1^T}{v_2^T} \right) \cdot \left(\begin{array}{c|c} v_1 & v_2 \end{array} \right) = \left(\begin{array}{c|c} v_1^T v_1 & v_1^T v_2 \\ \hline v_2^T v_1 & v_2^T v_2 \end{array} \right)$$

Since $v_1 \bullet v_2 = 0$, we have:

$$= \left(\begin{array}{c|c} v_1 \bullet v_1 & v_1 \bullet v_2 \\ \hline v_2 \bullet v_1 & v_2 \bullet v_2 \end{array} \right) = \left(\begin{array}{c|c} |v_1|^2 & 0 \\ \hline 0 & |v_2|^2 \end{array} \right)$$

Since v_1 and v_2 are not the zero vector, $|v_1| \neq 0$ and $|v_2| \neq 0$. Hence, AA^T has the identity as its Smith normal form. *It is an isomorphism and has an inverse.* In fact, we can check by diagonal block multiplication that the inverse is simply:

$$(AA^T)^{-1} = \begin{pmatrix} \frac{1}{|v_1|^2} & 0 \\ 0 & \frac{1}{|v_2|^2} \end{pmatrix}$$

This actually gives a way to build a right inverse for f . Notice that

$$AA^T(AA^T)^{-1} = \text{id}_{\mathbb{R}^2}$$

So by introducing parentheses, we see a right inverse g :

$$\underbrace{A}_f \underbrace{(A^T(AA^T)^{-1})}_g = \text{id}_{\mathbb{R}^2}$$

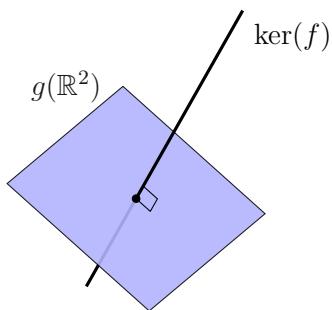
We consider how g is built and what its range is. We think of the matrices in the product for g starting from the right and working to the left. This is the direction of function composition in a column interpretation.

- First run an isomorphism $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by $(AA^T)^{-1}$.
- Note that all elements of \mathbb{R}^2 are images of $(AA^T)^{-1}$.
- All of the elements in \mathbb{R}^2 make it to the function given by A^T so that all of the range of A^T is possible.
- The range of g which is $g(\mathbb{R}^2)$ is the same as the range of A^T which is $\text{row}(A)$. So $g(\mathbb{R}^2) = \text{range}(A^T) = \text{row}(A)$.

Yet we know that since A represents f that $\text{row}(A) \perp \ker(f)$. In other words:

$$g(\mathbb{R}^2) \perp \ker(f)$$

So, the plane that describes $g(\mathbb{R}^2)$ is perpendicular to the line $\ker(f)$: *we get an orthogonal decomposition $g(\mathbb{R}^2) \oplus \ker(f)$* :



We call a right inverse g that produces such a decomposition an ***orthogonal right inverse***. This example can be generalized to the following theorem:

Theorem 5.3.2 Orthogonal Right Inverse

If A has pairwise orthogonal rows representing a linear transformation f , then $A^T(AA^T)^{-1}$ is a right inverse g such that $\text{range}(g) \perp \ker(f)$.

5.3.2 Iterative Procedure using Matrices

Pairwise Orthogonal

The vectors in a collection C are called pairwise orthogonal if whenever $a, b \in C$ and $a \neq b$, then $a \bullet b = 0$.

Theorem 5.3.3 Gram-Schmidt Iteration by Right Inverse

Suppose...

- the vectors v_1, v_2, \dots, v_n are pairwise orthogonal to each other
- and $w \notin \langle v_1, v_2, \dots, v_n \rangle$

Let...

- f_n be the linear transformation described by the matrix $A_n = \begin{pmatrix} v_1^T \\ v_2^T \\ \vdots \\ v_n^T \end{pmatrix}$

- g_n be the right inverse of f_n described by the matrix $A_n^T (A_n A_n^T)^{-1}$.
- v_{n+1} be the vector $w - g_n \circ f_n(w)$.

Then, v_1, v_2, \dots, v_{n+1} are all pairwise orthogonal and

$$\langle v_1, v_2, \dots, v_{n+1} \rangle = \langle v_1, v_2, \dots, w \rangle.$$

Proof. The linear transformation g_n is an orthogonal right inverse to f_n . Since g_n is a right inverse, $v_{n+1} = w - g_n \circ f_n(w) \in \ker(f_n)$. Since $\ker(f_n) \perp g(C)$, then $v_{n+1} \perp \text{range}(g_n) = \langle v_1, v_2, \dots, v_n \rangle$ (since g_n ends with the map A_n^T where A_n is the matrix for f_n). This tells us that v_1, v_2, \dots, v_{n+1} are all pairwise orthogonal.

Also,

$$v_{n+1} = w - \underbrace{g_n \circ f_n(w)}_{\substack{\text{Output is in range}(A_n^T) \\ \text{which is} \\ \langle v_1, v_2, \dots, v_n \rangle}}$$

tells us that $v_{n+1} \in \langle v_1, v_2, \dots, v_n, w \rangle$. Hence,

$$w = v_{n+1} + \underbrace{g_n \circ f_n(w)}_{\substack{\text{Output is in range}(A_n^T) \\ \text{which is} \\ \langle v_1, v_2, \dots, v_n \rangle}}$$

tells us that $w \in \langle v_1, v_2, \dots, v_{n+1} \rangle$. □

We can use this theorem repeatedly to turn a collection of linearly independent vectors w_1, w_2, \dots, w_n into a collection of pairwise orthogonal vectors v_1, v_2, \dots, v_n that have *the same span* as the original collection. This takes a basis and turns it into a pairwise orthogonal basis for *the same vector space*.

Let's try it!

Suppose that we have three vectors w_1, w_2, w_3 . Let $v_1 = w_1$. Then set $A_1 = v_1^T$ so that $g_1 \circ f_1$ is given by:

$$\underbrace{A_1^T (A_1 A_1^T)^{-1}}_{g_1} \cdot \underbrace{A_1}_{f_1}$$

Let's call this matrix B_1 and using $A_1 = v_1^T$, we compute:

$$B_1 = v_1 \left(\underbrace{v_1^T v_1}_{\text{1} \times 1 \text{ so a}} \right)^{-1} v_1^T = v_1 \frac{1}{v_1^T v_1} v_1^T = \frac{v_1 v_1^T}{v_1^T v_1}$$

scalar.

Applying the theorem, $v_2 = w_2 - g_1 \circ f_1(w_2)$ will be orthogonal to v_1 . We write: $v_2 = w_2 - B_1 \cdot w_2$ since B_1 represents the function $g_1 \circ f_1$. To find v_3 , we compute $v_3 = w_3 - g_2 \circ f_2(w_3)$. Let's figure out what the matrix B_2 for $g_2 \circ f_2$ will look like:

$$\begin{aligned} & \underbrace{A_2^T (A_2 A_2^T)^{-1}}_{g_2} \cdot \underbrace{A_2}_{f_2} \\ &= \underbrace{\left(\begin{array}{c|c} v_1 & v_2 \\ \hline A_2^T & \end{array} \right)}_{\text{A } 2 \times 2 \text{ matrix}} \cdot \left(\underbrace{\left(\begin{array}{c|c} v_1 & v_2 \\ \hline A_2^T & \end{array} \right)}_{\text{A } 2 \times 2 \text{ matrix}}^{-1} \right) \cdot \underbrace{\left(\begin{array}{c} v_1^T \\ v_2^T \end{array} \right)}_{A_2} \\ &= \underbrace{\left(\begin{array}{c|c} v_1 & v_2 \\ \hline A_2^T & \end{array} \right)}_{\text{A } 2 \times 2 \text{ matrix}} \cdot \underbrace{\left(\begin{array}{cc|cc} v_1^T v_1 & v_1^T v_2 & & \\ v_2^T v_1 & v_2^T v_2 & & \\ \hline v_1 \bullet v_1 & v_1 \bullet v_2 & & \\ v_2 \bullet v_1 & v_2 \bullet v_2 & & \end{array} \right)^{-1}}_{\text{A } 4 \times 4 \text{ matrix}} \cdot \underbrace{\left(\begin{array}{c} v_1^T \\ v_2^T \end{array} \right)}_{A_2} \end{aligned}$$

Since $v_1 \bullet v_2 = 0$, and using the fact that $v \bullet v = |v|^2$, we have that this middle matrix is

$$\begin{pmatrix} |v_1|^2 & 0 \\ 0 & |v_2|^2 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{|v_1|^2} & 0 \\ 0 & \frac{1}{|v_2|^2} \end{pmatrix}$$

Multiplying this middle matrix with A_2 yields:

$$\begin{pmatrix} \frac{1}{|v_1|^2} & 0 \\ 0 & \frac{1}{|v_2|^2} \end{pmatrix} \cdot \underbrace{\begin{pmatrix} v_1^T \\ v_2^T \end{pmatrix}}_{A_2} = \begin{pmatrix} \frac{v_1^T}{|v_1|^2} \\ -\frac{v_2^T}{|v_2|^2} \end{pmatrix}$$

Hence,

$$B_2 = \underbrace{\begin{pmatrix} v_1 & |v_2 \rangle \end{pmatrix}}_{A_2^T} \cdot \begin{pmatrix} \frac{v_1^T}{|v_1|^2} \\ -\frac{v_2^T}{|v_2|^2} \end{pmatrix} = \frac{v_1 v_1^T}{|v_1|^2} + \frac{v_2 v_2^T}{|v_2|^2}$$

Remembering that $|v|^2 = v^T v$, we can write this also as:

$$B_2 = \frac{v_1 v_1^T}{v_1^T v_1} + \frac{v_2 v_2^T}{v_2^T v_2}$$

Theorem 5.3.4 Matrices for $g_n \circ f_n$

The matrix B_n which represents $g_n \circ f_n$ in the Gram-Schmidt process is given as:

$$B_n = \frac{v_1 v_1^T}{v_1^T v_1} + \frac{v_2 v_2^T}{v_2^T v_2} + \cdots + \frac{v_n v_n^T}{v_n^T v_n}$$

Theorem 5.3.5 Gram-Schmidt Matrix Iteration

Let B_n be the matrix described by $g_n \circ f_n$ of the last theorem. That is, define $B_1 = \frac{v_1 v_1^T}{v_1^T v_1}$ and $B_{n+1} = B_n + \frac{v_{n+1} v_{n+1}^T}{v_{n+1}^T v_{n+1}}$. Then the process $v_{n+1} = (\text{id} - B_n)w_{n+1} = w_{n+1} - B_n w_{n+1}$ with $v_1 = w_1$ turns a basis $\{w_1, w_2, \dots, w_k\}$ into a pairwise orthogonal basis $\{v_1, v_2, \dots, v_k\}$ for the same vector space.

Example 1. Let's use this process to turn the collection $w_1 = (1, 1, 1)$, $w_2 = (1, 1, 0)$ and $w_3 = (1, 0, 0)$ into

an orthogonal basis. Let $v_1 = (1, 1, 1)$. We compute

$$B_1 = \frac{v_1 v_1^T}{v_1^T v_1} = \frac{1}{v_1 \bullet v_1} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} = \frac{1}{3} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Then, we use this to calculate v_2 :

$$\begin{aligned} v_2 &= w_2 - B_1 w_2 = (\text{id}_{\mathbb{R}^3} - B_1) w_2 = \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix} \right) \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{3} \\ \frac{1}{3} \\ -\frac{2}{3} \end{pmatrix} \end{aligned}$$

If we are looking for an orthogonal basis and do not worry about how the vectors are scaled, *we could rescale* v_2 so that:

$$v_2 = (1, 1, -2).$$

Now we can compute

$$\begin{aligned} B_2 &= B_1 + \frac{v_2 v_2^T}{v_2^T v_2} = B_1 + \frac{1}{v_2 \bullet v_2} \cdot \begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & -2 \end{pmatrix} \\ &= \underbrace{\frac{1}{6} \cdot \begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix}}_{B_1 \cdot \frac{2}{2}} + \frac{1}{6} \begin{pmatrix} 1 & 1 & -2 \\ 1 & 1 & -2 \\ -2 & -2 & 4 \end{pmatrix} = \frac{1}{6} \begin{pmatrix} 3 & 3 & 0 \\ 3 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix} = \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \end{aligned}$$

So now we compute v_3 :

$$v_3 = w_3 - B_2 \cdot w_3 = (\text{id}_{\mathbb{R}^3} - B_2) \cdot w_3$$

$$= \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \right) \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ 0 \end{pmatrix}$$

Hence, upon rescaling, we have:

$$v_3 = (1, -1, 0).$$

Our new pairwise orthogonal basis is:

$$v_1 = (1, 1, 1) \quad v_2 = (1, 1, -2) \quad v_3 = (1, -1, 0)$$



[Link to run the code.](#)

```
L=[(-1, 0, 1, 0), (0, 1, 1, 1), (-1, -1, -1, 0)]
#length of the vectors:
m=len(L[0])

def B(v):
    V=matrix(4,1,v)
    return(V*v.transpose() / (V.transpose()*V)[0][0])

OrthogonalBasis=[vector(L[0])]

#Fill a square m x m matrix with 0's:
BB=matrix(m,m, (m^2)*[0])

for i in range(len(L))[1:]:
    #For the last new v in Orthogonal Basis, add vv^T to BB:
    BB+=B(OrthogonalBasis[i-1])
    OrthogonalBasis+=[vector(L[i])-vector(BB*matrix(4,1,L[i]))]

print(OrthogonalBasis)
```

5.3.3 Iterative Procedure Using Dot Product

Let's consider how we got v_3 in this last example:

$$\begin{aligned} v_3 &= w_3 - B_2 \cdot w_3 = w_3 - \left(\frac{v_1 v_1^T}{v_1^T v_1} + \frac{v_2 v_2^T}{v_2^T v_2} \right) \cdot w_3 \\ &= w_3 - \frac{v_1 v_1^T}{v_1^T v_1} w_3 - \frac{v_2 v_2^T}{v_2^T v_2} w_3 = w_3 - v_1 \frac{v_1^T w_3}{v_1^T v_1} - v_2 \frac{v_2^T w_3}{v_2^T v_2} \\ &= w_3 - \underbrace{\frac{v_1 \bullet w_3}{v_1 \bullet v_1} v_1}_{\text{proj}_{v_1} w_3} - \underbrace{\frac{v_2 \bullet w_3}{v_2 \bullet v_2} v_2}_{\text{proj}_{v_2} w_3} \end{aligned}$$

We can verify that v_3 and v_2 are orthogonal if we assume v_2 and v_1 already are by using the expansion:

$$\begin{aligned} v_3 \bullet v_2 &= \left(w_3 - \underbrace{\frac{v_1 \bullet w_3}{v_1 \bullet v_1} v_1}_{\text{proj}_{v_1} w_3} - \underbrace{\frac{v_2 \bullet w_3}{v_2 \bullet v_2} v_2}_{\text{proj}_{v_2} w_3} \right) \bullet v_2 \\ &= w_3 \bullet v_2 - \underbrace{\frac{v_1 \bullet w_3}{v_1 \bullet v_1} v_1 \bullet v_2}_0 - \underbrace{\frac{v_2 \bullet w_3}{v_2 \bullet v_2} v_2 \bullet v_2}_0 = w_3 \bullet v_2 - v_2 \bullet w_3 = 0 \end{aligned}$$

What we find is a way to view Gram Schmidt without matrices. But we compute many dot products and additions at each step instead of adding two matrices and then performing one single matrix multiplication at each step. Computationally, there is not much difference in the number of actual operations done. The reader is encouraged to discover how the matrix multiplication vv^T using a row or a column interpretation can be extremely simple.

Theorem 5.3.6 Gram-Schmidt Dot Product Iteration

The process $v_{n+1} = w_{n+1} - \text{proj}_{v_1} w_{n+1} - \text{proj}_{v_2} w_{n+1} - \cdots - \text{proj}_{v_n} w_{n+1}$ with $v_1 = w_1$ turns a basis $\{w_1, w_2, \dots, w_k\}$ into a pairwise orthogonal basis $\{v_1, v_2, \dots, v_k\}$ for the same vector space. We use the formula

$$\text{proj}_v w = \frac{v \bullet w}{v \bullet v}$$



Example 2. Let's use the Gram-Schmidt dot product technique. Let's take the collection:

$$w_1 = (0, 0, 1, 1), w_2 = (1, 0, 1, 0), w_3 = (1, 0, -1, 0)$$

which represents a basis for a 3-dimensional subspace of \mathbb{R}^4 . We will change it into a pairwise orthogonal basis for this same subspace.

- $v_1 = w_1 = (0, 0, 1, 1)$

- $v_2 = w_2 - \text{proj}_{v_1} w_2 = w_2 - \frac{v_1 \bullet w_2}{v_1 \bullet v_1} v_1$

$$= (1, 0, 1, 0) - \underbrace{\frac{(0, 0, 1, 1) \bullet (1, 0, 1, 0)}{(0, 0, 1, 1) \bullet (0, 0, 1, 1)}}_{\frac{1}{2}} (0, 0, 1, 1)$$

$$= (1, 0, 1, 0) - (0, 0, \frac{1}{2}, \frac{1}{2}) = (1, 0, \frac{1}{2}, -\frac{1}{2})$$

For simplicity, let's rescale v_2 to $(2, 0, 1, -1)$. It will still be orthogonal to v_1 .

$$v_2 = (2, 0, 1, -1)$$

$$\begin{aligned}
\bullet v_3 &= w_3 - \text{proj}_{v_1} w_3 - \text{proj}_{v_2} w_3 = w_3 - \frac{v_1 \bullet w_3}{v_1 \bullet v_1} v_1 - \frac{v_2 \bullet w_3}{v_2 \bullet v_2} v_2 \\
&= (1, 0, -1, 0) - \underbrace{\frac{(0, 0, 1, 1) \bullet (1, 0, -1, 0)}{(0, 0, 1, 1) \bullet (0, 0, 1, 1)} \cdot (0, 0, 1, 1)}_{-\frac{1}{2}} - \underbrace{\frac{(2, 0, 1, -1) \bullet (1, 0, -1, 0)}{(2, 0, 1, -1) \bullet (2, 0, 1, -1)} \cdot (2, 0, 1, -1)}_{\frac{1}{6}} \\
&= (1, 0, -1, 0) + (0, 0, \frac{1}{2}, \frac{1}{2}) + (-\frac{1}{3}, 0, -\frac{1}{6}, \frac{1}{6}) = (\frac{2}{3}, 0, -\frac{2}{3}, \frac{2}{3}) \text{ For simplicity, we can rescale } v_3 \text{ to} \\
&\quad (1, 0, -1, 1) \\
v_3 &= (1, 0, -1, 1)
\end{aligned}$$

The reader is welcome to verify that the basis

$$v_1 = (0, 0, 1, 1), v_2 = (2, 0, 1, -1), v_3 = (1, 0, -1, 1)$$

is pairwise orthogonal.

5.3.4 Orthonormal Bases

Orthogonal Basis

An orthogonal basis is one that is pairwise orthogonal

Orthonormal Basis

An orthonormal basis is an orthogonal basis such that each basis vector has length 1.

Example 3. We can change the orthogonal basis that we found in the last example into an orthonormal basis simply by dividing each vector by its length:

$$\frac{v_1}{|v_1|} = (0, 0, \frac{1}{2}, \frac{1}{2}), \frac{v_2}{|v_2|} = (\frac{1}{3}, 0, \frac{1}{6}, -\frac{1}{6}), \frac{v_3}{|v_3|} = (\frac{1}{3}, 0, -\frac{1}{3}, \frac{1}{3})$$

The next result should be clear by orthogonality and by remembering the fact that $v \bullet v = 1$ if and only if v is a unit vector:

Theorem 5.3.7

If $C = \{c_1, c_2, \dots, c_n\}$ is an orthonormal basis, then

$$c_i \bullet c_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

This very idea takes us to a very nice result:

Theorem 5.3.8

Suppose that the columns of a matrix B form an orthonormal basis for the column space of B —that is for the range of B thought of as a function under the column interpretation. Then, B^T is a left inverse for B . That is:

$$B^T \cdot B = \text{id}$$

Conversely, if $B^T \cdot B = \text{id}$, then the columns of B form an orthonormal basis for the column space of B .

Proof. Suppose first that the columns of a matrix B form an orthonormal basis for the column space of B . Let $B = (b_1 \ b_2 \ \dots \ b_n)$ where b_1, b_2, \dots, b_n are the columns of B . Then:

$$\underbrace{\begin{pmatrix} b_1^T \\ b_2^T \\ \vdots \\ b_n^T \end{pmatrix}}_{B^T} \cdot \underbrace{\left(\begin{array}{c|c|c|c} b_1 & b_2 & \cdots & b_n \end{array} \right)}_B = \begin{pmatrix} b_1^T b_1 & b_1^T b_2 & \cdots & b_1^T b_n \\ b_2^T b_1 & b_2^T b_2 & \cdots & b_2^T b_n \\ \vdots & \vdots & \ddots & \vdots \\ b_n^T b_1 & b_n^T b_2 & \cdots & b_n^T b_n \end{pmatrix}$$

$$= \begin{pmatrix} b_1 \bullet b_1 & b_1 \bullet b_2 & \cdots & b_1 \bullet b_n \\ b_2 \bullet b_1 & b_2 \bullet b_2 & \cdots & b_2 \bullet b_n \\ \vdots & \vdots & \ddots & \vdots \\ b_n \bullet b_1 & b_n \bullet b_2 & \cdots & b_n \bullet b_n \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Next suppose that $B^T \cdot B = \text{id}$. Then if we block B^T by rows and B by columns, we see that the dot product between the i th row of B^T (i.e. i th column of B) and the j th column of B (i.e. the j th column of B) is the ij th entry of $B^T \cdot B = \text{id}$. This means that the dot product between columns is always 0 if $i \neq j$ and 1 if $i = j$. This tells us that the columns all have length 1 and are orthogonal to each other. \square

5.3.5 QR Decomposition

We will use the following result in the next section on least squares where we have an exciting application of orthogonal projections:

Theorem 5.3.9

If A represents an injective linear transformation, then the matrix $A^T A$ is a square matrix which represents an isomorphism.

This subsection is devoted to the proof of this fact. We use what is called *QR decomposition* which relies

heavily on the Gram Schmidt process that turns the columns of A into an orthonormal basis. We will learn how this process proves this result and then we will practice actually finding QR decompositions.

So, let's begin by thinking about the process. Suppose that A is a $m \times n$ matrix. Let the columns of A be represented as follows:

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

Further suppose that the columns are linearly independent so that we may apply Gram Schmidt. This is equivalent to the Smith normal form of A having 1 in each column—so that there are no zero columns. That is, A is injective.

Let's run the Gram Schmidt process iteratively on these column vectors $a_1, \dots, a_n \in \mathbb{R}^m$ to find vectors $q_1, \dots, q_n \in \mathbb{R}^m$. Think about the dot product iterative procedure. Essentially, we have that q_1 is a_1 , q_2 is a linear combination of a_2 and q_1 , q_3 is a linear combination of a_3 , q_1 , and q_2 , q_4 is a linear combination of a_3 , q_1 , q_2 , and q_3 , etc. where the scalar coefficients are just fractions of dot products. We will name these coefficients with subscripts:

<ul style="list-style-type: none"> • $q_1 = a_1$ • $q_2 = a_2 - t_{12}q_1$ • $q_3 = a_3 - t_{13}q_1 - t_{23}q_2$ • $q_4 = a_4 - t_{14}q_1 - t_{24}q_2 - t_{34}q_3$ ⋮ • $q_n = a_n - t_{1n}q_1 - \cdots - t_{nn}q_{n-1}$ 	<p>Solve for a_1, a_2, a_3, etc.</p>  <ul style="list-style-type: none"> • $a_1 = q_1$ • $a_2 = t_{12}q_1 + q_2$ • $a_3 = t_{13}q_1 + t_{23}q_2 + q_3$ • $a_4 = t_{14}q_1 + t_{24}q_2 + t_{34}q_3 + q_4$ ⋮ • $a_n = t_{1n}q_1 + t_{2n}q_2 + \cdots + q_n$
--	--

These equations give us a way to break up the paths that the matrix A gives:

$$\begin{aligned} e_1 &\longmapsto a_1 \\ e_2 &\longmapsto a_2 \\ &\vdots \\ e_n &\longmapsto a_n \end{aligned}$$

They do this as follows:

$$\begin{array}{c}
 \xrightarrow{\quad r : \mathbb{R}^n \rightarrow \mathbb{R}^n \quad} \\
 \bullet e_1 \mapsto e_1 \\
 \bullet e_2 \mapsto t_{12}e_1 + e_2 \\
 \bullet e_3 \mapsto t_{13}e_1 + t_{23}e_2 + e_3 \\
 \bullet e_4 \mapsto t_{14}e_1 + t_{24}e_2 + t_{34}e_3 + e_4 \\
 \vdots \\
 \bullet e_n \mapsto t_{1n}e_1 + t_{2n}e_2 + \cdots + e_n
 \end{array}
 \qquad
 \begin{array}{c}
 \xrightarrow{\quad q : \mathbb{R}^n \rightarrow \mathbb{R}^m \quad} \\
 e_1 \mapsto q_1 \\
 e_2 \mapsto q_2 \\
 \vdots \\
 e_n \mapsto q_n
 \end{array}
 \qquad
 \begin{array}{l}
 \bullet q_1 = a_1 \\
 \bullet t_{12}q_1 + q_2 = a_2 \\
 \bullet t_{13}q_1 + t_{23}q_2 + q_3 = a_3 \\
 \bullet t_{14}q_1 + t_{24}q_2 + t_{34}q_3 + q_4 = a_4 \\
 \vdots \\
 \bullet t_{1n}q_1 + t_{2n}q_2 + \cdots + q_n = a_n
 \end{array}$$

Notice that $q \circ r(e_1) = a_1$, $q \circ r(e_2) = a_2$, etc. That is, the matrix for $q \circ r$ under a column interpretation is A itself *because* it sends e_i to a_i which is the i th column of A .

As a matrix multiplication which is equal to A , $q \circ r$ is (under a column interpretation) as follows:

$$A = \underbrace{\begin{pmatrix} q_1 & q_2 & \cdots & q_n \end{pmatrix}}_q \cdot \underbrace{\begin{pmatrix} 1 & t_{12} & t_{13} & \cdots & t_{1n} \\ 0 & 1 & t_{23} & \cdots & t_{2n} \\ 0 & 0 & 1 & \cdots & t_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}}_r$$

Into the middle of this multiplication, let's insert a product that is the $n \times n$ identity matrix:

$$\underbrace{\begin{pmatrix} q_1 & q_2 & \cdots & q_n \end{pmatrix}}_q \cdot \underbrace{\begin{pmatrix} \frac{1}{|q_1|} & 0 & 0 & 0 & \cdots \\ 0 & \frac{1}{|q_2|} & 0 & 0 & \cdots \\ 0 & 0 & \frac{1}{|q_3|} & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ 0 & 0 & 0 & \cdots & \frac{1}{|q_n|} \end{pmatrix}}_{\text{id}} \cdot \underbrace{\begin{pmatrix} |q_1| & 0 & 0 & 0 & \cdots \\ 0 & |q_2| & 0 & 0 & \cdots \\ 0 & 0 & |q_3| & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ 0 & 0 & 0 & \cdots & |q_n| \end{pmatrix}}_{\text{id}} \cdot \underbrace{\begin{pmatrix} 1 & t_{12} & t_{13} & \cdots & t_{1n} \\ 0 & 1 & t_{23} & \cdots & t_{2n} \\ 0 & 0 & 1 & \cdots & t_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}}_r$$

We define matrices Q and R as follows:

$$Q = \underbrace{\begin{pmatrix} q_1 & q_2 & \cdots & q_n \end{pmatrix}}_q \cdot \begin{pmatrix} \frac{1}{|q_1|} & 0 & 0 & 0 & \cdots \\ 0 & \frac{1}{|q_2|} & 0 & 0 & \cdots \\ 0 & 0 & \frac{1}{|q_3|} & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ 0 & 0 & 0 & \cdots & \frac{1}{|q_n|} \end{pmatrix} = \begin{pmatrix} \frac{q_1}{|q_1|} & \frac{q_2}{|q_2|} & \cdots & \frac{q_n}{|q_n|} \end{pmatrix}$$

$$R = \underbrace{\begin{pmatrix} |q_1| & 0 & 0 & 0 & \cdots \\ 0 & |q_2| & 0 & 0 & \cdots \\ 0 & 0 & |q_3| & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ 0 & 0 & 0 & \cdots & |q_n| \end{pmatrix}}_r \cdot \underbrace{\begin{pmatrix} 1 & t_{12} & t_{13} & \cdots & t_{1n} \\ 0 & 1 & t_{23} & \cdots & t_{2n} \\ 0 & 0 & 1 & \cdots & t_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}}_{\text{id}} = \begin{pmatrix} |q_1| & |q_1|t_{12} & |q_1|t_{13} & \cdots & |q_1|t_{1n} \\ 0 & |q_2| & |q_2|t_{23} & \cdots & |q_2|t_{2n} \\ 0 & 0 & |q_3| & \cdots & |q_3|t_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & |q_n| \end{pmatrix}$$

Then we have that $A = QR$. In particular, the columns of Q make up an orthonormal basis so that $Q^T Q$ is equal to an $n \times n$ identity matrix by [Theorem 5.3.8](#). This means that

$$A^T A = (QR)^T (QR) = R^T Q^T Q R = R^T R$$

The reader can verify that column operations can easily bring R to the identity matrix. This means that both R and R^T are isomorphisms. Therefore, $A^T A$ is an isomorphism as desired.

Upper triangular matrix

A *square* matrix is said to be upper triangular, if below the diagonal from top left to bottom right, there are only 0's.

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

Example 4. The following are upper triangular matrices:

$$\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 4 & 5 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -20 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

QR Decomposition

A QR decomposition for a matrix A is writing the matrix A as the product QR where the columns of Q form an orthonormal basis for the span of the columns of A and R is an upper triangular matrix.

Example 5. Let's find the QR decomposition of

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & -1 \\ 1 & 0 & 0 \\ w_1 & w_2 & w_3 \end{pmatrix}$$

Notice that the columns are the same vectors that we applied Gram-Schmidt to in [example 2](#). In this Gram Schmidt process, we rescaled our results v_2 and v_3 so that they looked nice. Unfortunately, this ruins things a little bit for QR decomposition. We redo the Gram-Schmidt process. This time, we do not rescale at any step.

- $v_1 = w_1 = (0, 0, 1, 1)$
- $v_2 = w_2 - \text{proj}_{v_1} w_2 = w_2 - \frac{v_1 \bullet w_2}{v_1 \bullet v_1} v_1$
 $= (1, 0, 1, 0) - \underbrace{\frac{(0, 0, 1, 1) \bullet (1, 0, 1, 0)}{(0, 0, 1, 1) \bullet (0, 0, 1, 1)}}_{\frac{1}{2}} (0, 0, 1, 1)$
 $= (1, 0, 1, 0) - (0, 0, \frac{1}{2}, \frac{1}{2}) = (1, 0, \frac{1}{2}, -\frac{1}{2}).$
- $v_3 = w_3 - \text{proj}_{v_1} w_3 - \text{proj}_{v_2} w_3 = w_3 - \frac{v_1 \bullet w_3}{v_1 \bullet v_1} v_1 - \frac{v_2 \bullet w_3}{v_2 \bullet v_2} v_2$
 $= (1, 0, -1, 0) - \underbrace{\frac{(0, 0, 1, 1) \bullet (1, 0, -1, 0)}{(0, 0, 1, 1) \bullet (0, 0, 1, 1)}}_{-\frac{1}{2}} (0, 0, 1, 1) - \underbrace{\frac{(1, 0, \frac{1}{2}, -\frac{1}{2}) \bullet (1, 0, -1, 0)}{(1, 0, \frac{1}{2}, -\frac{1}{2}) \bullet (1, 0, \frac{1}{2}, -\frac{1}{2})}}_{\frac{1}{3}} (1, 0, \frac{1}{2}, -\frac{1}{2})$

$$= (1, 0, -1, 0) + (0, 0, \frac{1}{2}, \frac{1}{2}) + (-\frac{1}{3}, 0, -\frac{1}{6}, \frac{1}{6}) = (\frac{2}{3}, 0, -\frac{2}{3}, \frac{2}{3})$$

$$v_3 = (\frac{2}{3}, 0, -\frac{2}{3}, \frac{2}{3})$$

We have that:

- $w_1 = v_1$
- $w_2 = \frac{1}{2}v_1 + v_2$
- $w_3 = -\frac{1}{2}v_1 + \frac{1}{3}v_2 + v_3$

Now, we proceed as follows to come up with Q and R where we use $|v_1| = \sqrt{2}$, $|v_2| = \sqrt{\frac{3}{2}}$, and $|v_3| = \frac{2}{\sqrt{3}}$

$$Q = \begin{pmatrix} 0 & 1 & \frac{2}{3} \\ 0 & 0 & 0 \\ \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 0 \\ \frac{1}{2} \\ -\frac{1}{2} \end{pmatrix} & \sqrt{\frac{2}{3}} \cdot \begin{pmatrix} 0 \\ \frac{1}{2} \\ -\frac{1}{2} \\ \frac{2}{3} \end{pmatrix} & \frac{\sqrt{3}}{2} \cdot \begin{pmatrix} 0 \\ -\frac{2}{3} \\ \frac{2}{3} \\ 0 \end{pmatrix} \\ \frac{v_1}{|v_1|} & \frac{v_2}{|v_2|} & \frac{v_3}{|v_3|} \end{pmatrix} = \begin{pmatrix} 0 & \sqrt{\frac{2}{3}} & \frac{1}{3}\sqrt{3} \\ 0 & 0 & 0 \\ \frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{\frac{2}{3}} & -\frac{1}{3}\sqrt{3} \\ \frac{1}{2}\sqrt{2} & -\frac{1}{2}\sqrt{\frac{2}{3}} & \frac{1}{3}\sqrt{3} \end{pmatrix}$$

$$R = \begin{pmatrix} \sqrt{2} \cdot \begin{pmatrix} 1 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \\ \sqrt{\frac{3}{2}} \cdot \begin{pmatrix} 0 & 1 & \frac{1}{3} \end{pmatrix} \\ \frac{2}{\sqrt{3}} \cdot \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 2\sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} & -\sqrt{\frac{1}{2}} \\ 0 & \frac{3}{2}\sqrt{\frac{2}{3}} & \frac{1}{2}\sqrt{\frac{2}{3}} \\ 0 & 0 & \frac{2}{3}\sqrt{3} \end{pmatrix}$$

$w_1 = v_1$
 $w_2 = \frac{1}{2}v_1 + v_2$
 $w_3 = -\frac{1}{2}v_1 + \frac{1}{3}v_2 + v_3$

You can verify the following equality $A = QR$:

$$\underbrace{\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & -1 \\ 1 & 0 & 0 \end{pmatrix}}_A = \underbrace{\begin{pmatrix} 0 & \sqrt{\frac{2}{3}} & \frac{1}{3}\sqrt{3} \\ 0 & 0 & 0 \\ \frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{\frac{2}{3}} & -\frac{1}{3}\sqrt{3} \\ \frac{1}{2}\sqrt{2} & -\frac{1}{2}\sqrt{\frac{2}{3}} & \frac{1}{3}\sqrt{3} \end{pmatrix}}_Q \cdot \underbrace{\begin{pmatrix} 2\sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} & -\sqrt{\frac{1}{2}} \\ 0 & \frac{3}{2}\sqrt{\frac{2}{3}} & \frac{1}{2}\sqrt{\frac{2}{3}} \\ 0 & 0 & \frac{2}{3}\sqrt{3} \end{pmatrix}}_R$$

The matrices Q and R that give a QR decomposition are unique! They are only ones that actually accomplish the desired task. Before proving this, we mention a couple preliminary facts:

Lemma 5.3.10

The inverse of an upper triangular matrix which represents an isomorphism is upper triangular.

Proof. If there is a zero in the diagonal from top left to bottom right of an upper triangular matrix, then the number of pivots in getting reduced row echelon form is less than n . This implies that the Smith normal form is not the identity matrix. This contradicts the fact that the matrix is assumed to be an isomorphism. Hence, by rescaling rows and airdropping *upward only* one can make the upper triangular matrix into an identity. These same operations applied to an identity matrix produce the inverse matrix. Yet notice that the *upward* airdrops and rescaling on an identity matrix produce an *upper* triangular matrix. \square

Lemma 5.3.11

The product of two upper triangular square $n \times n$ matrices is upper triangular.

Proof. Suppose that the two matrices are A and B . Notice that under a row interpretation of multiplication, the first row of AB is a linear combination of all the rows of B . The second row of AB is a linear combination of all but the first row of B because the second row of A has a 0 in its first entry. This means that first entry of the second row of AB is 0 since the first entry of all the rows of B after the first row is 0. Similarly, the k th row of AB is a linear combination of the last $n - (k - 1)$ rows of B . The first $k - 1$ entries of all of these rows in B is 0. Hence, the first $k - 1$ entries of the k th row of AB are all zeros. This tells us that AB is upper triangular. \square

Theorem 5.3.12

The QR decomposition of a matrix is unique.

Proof. Suppose that the matrix A has two different QR decompositions so that $A = Q_1 R_1 = Q_2 R_2$. Note that R_1 and R_2 both have the same size as matrices. Suppose that they are both $n \times n$ matrices. Then, multiply by Q_2^T on the left and R_1^{-1} on the right:

$$Q_2^T (Q_1 R_1) R_1^{-1} = Q_2^T (Q_2 R_2) R_1^{-1}$$

Notice that because the columns of Q_2 are orthonormal and there are n of them, $Q_2^T Q_2 = \text{id}_{n \times n}$. So we have:

$$Q_2^T Q_1 \underbrace{R_1 R_1^{-1}}_{\text{id}_{n \times n}} = \underbrace{Q_2^T Q_2}_{\text{id}_{n \times n}} R_2 R_1^{-1}$$

$$Q_2^T Q_1 = R_2 R_1^{-1}$$

Notice that

$$\begin{aligned} (Q_2^T Q_1)^T (Q_2^T Q_1) &= Q_1^T \underbrace{Q_2 Q_2^T}_{\text{id } n \times n} Q_1 \\ &= Q_1^T Q_1 = \text{id}_{n \times n} \end{aligned}$$

This tells us that the columns of the product $(Q_2^T Q_1)$ must be orthonormal. By our results on inverses and products of upper triangular matrices, $R_2 R_1^{-1}$ is upper triangular. Since $R_2 R_1^{-1}$ and $(Q_2^T Q_1)$ are the exact same matrix, we can say that this matrix has orthonormal columns and is upper triangular. The reader is invited to show by induction that this means that each column starting from the first to the last are all standard basis vectors. That is, $Q_2^T Q_1 = R_2 R_1^{-1} = \text{id}_{n \times n}$. See the exercises! This means that $Q_2^T = Q_1^{-1}$. Yet we know by orthonormality that $Q_1^{-1} = Q_1^T$ so that $Q_2^T = Q_1^T$ so that $Q_2 = Q_1$. We also have that $R_2 = R_1$. Therefore, the two QR decompositions are the same. \square

What is so good about having a QR decomposition? One nice thing is that our matrix Q has orthonormal columns.

Theorem 5.3.13

If Q is a matrix with orthonormal columns and that v is a column vector that we have an equality of vector lengths: $|Qv| = |v|$.

Proof. See the exercises! \square

This in particular shows that such a matrix Q describes a linear transformation that preserves all lengths! You should note that Q must be a injective function in order to have orthonormal columns. Therefore, Q injects vectors from one vector space into a potentially much larger one all the while preserving their lengths.

Yet also, R is upper triangular which has its own uses. There are many algorithms that rely on this decomposition. Since this decomposition is a common use of the Gram Schmidt process, it is included in this text.

5.3.6 LQ Decomposition

A LQ Decomposition is just the transpose of a QR decomposition for A^T where A represents a surjective function under a column interpretation. Now remember that if A is surjective in its column interpretation, then A^T is injective in its column interpretation. Therefore, we can find a QR decomposition for A^T and write it as $A^T = QR$. Now, take transposes:

$$(A^T)^T = (QR)^T \quad \rightarrow \quad A = \underbrace{R^T}_L \cdot \underbrace{Q^T}_{\text{new "Q"}}$$

Lower triangular matrix

A *square* matrix is said to be lower triangular if above the diagonal from top left to bottom right, there are only 0's.

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

Example 6. The following are lower triangular matrices:

$$\begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} \quad \begin{pmatrix} 4 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 \\ 0 & 0 & -20 & 0 \\ 0 & 1 & 1 & -1 \end{pmatrix}$$

LQ Decomposition

A LQ decomposition for a matrix A is writing the matrix A as the product LQ where the rows of Q form an orthonormal basis for the span of the rows of Q and L is an lower triangular matrix.

Example 7. We consider the transpose of the matrix in [example 5](#) and find the LQ decomposition of it:

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

This matrix represents a surjective function under the column interpretation. We simply take the transpose of the decomposition that we found in [example 5](#):

$$\underbrace{\begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \end{pmatrix}}_{B=A^T} = \underbrace{\begin{pmatrix} 2\sqrt{\frac{1}{2}} & 0 & 0 \\ \sqrt{\frac{1}{2}} & \frac{3}{2}\sqrt{\frac{2}{3}} & 0 \\ -\sqrt{\frac{1}{2}} & \frac{1}{2}\sqrt{\frac{2}{3}} & \frac{2}{3}\sqrt{3} \end{pmatrix}}_{L=R^T} \cdot \underbrace{\begin{pmatrix} 0 & 0 & \frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \\ \sqrt{\frac{2}{3}} & 0 & \frac{1}{2}\sqrt{\frac{2}{3}} & -\frac{1}{2}\sqrt{\frac{2}{3}} \\ \frac{1}{3}\sqrt{3} & 0 & -\frac{1}{3}\sqrt{3} & \frac{1}{3}\sqrt{3} \end{pmatrix}}_{“Q”=Q^T}$$

Key Concepts from this Section

- **row space:** (page 515) The row space $\text{row}(A)$ of a matrix A can be equivalently described in any of the following ways:
 - the span of the rows
 - the range of A under a *row interpretation*
 - the range of A^T under a *column interpretation*
- **theorem 5.3.1 kernel orthogonal to row space:** (page 516) Suppose that A is a matrix describing a linear transformation f under a column interpretation. Then $\ker(f) \perp \text{row}(A)$.
- **orthogonal right inverse:** (page 518) Suppose that the linear transformation is a right inverse to $f : D \rightarrow C$. Then, we say that g is an orthogonal right inverse if $g(C) \perp \ker(f)$.
- **theorem 5.3.2 orthogonal right inverse:** (page 518) If A has pairwise orthogonal rows representing a linear transformation f , then $A^T(AA^T)^{-1}$ is a right inverse g such that $\text{range}(g) \perp \ker(f)$.
- **pairwise orthogonal:** (page 518) The vectors in a collection C are called pairwise orthogonal if whenever $a, b \in C$ and $a \neq b$, then $a \bullet b = 0$.
- **theorem 5.3.3 gram-schmidt iteration by right inverse:** (page 518) Suppose...
 - the vectors v_1, v_2, \dots, v_n are pairwise orthogonal to each other
 - and $w \notin \langle v_1, v_2, \dots, v_n \rangle$

Let...

- f_n be the linear transformation described by the matrix $A_n = \begin{pmatrix} v_1^T \\ v_2^T \\ \vdots \\ v_n^T \end{pmatrix}$
- g_n be the right inverse of f_n described by the matrix $A_n^T(A_n A_n^T)^{-1}$.
- v_{n+1} be the vector $w - g_n \circ f_n(w)$.

Then, v_1, v_2, \dots, v_{n+1} are all pairwise orthogonal and

$$\langle v_1, v_2, \dots, v_{n+1} \rangle = \langle v_1, v_2, \dots, w \rangle.$$

- **theorem 5.3.4 matrices for $g_n \circ f_n$:** (page 521) The matrix B_n which represents $g_n \circ f_n$ in the Gram-Schmidt process is given as:

$$B_n = \frac{v_1 v_1^T}{v_1^T v_1} + \frac{v_2 v_2^T}{v_2^T v_2} + \cdots + \frac{v_n v_n^T}{v_n^T v_n}$$

- **theorem 5.3.5 gram-schmidt matrix iteration:** (page 521) Let B_n be the matrix described by $g_n \circ f_n$ of the last theorem. That is, define $B_1 = \frac{v_1 v_1^T}{v_1^T v_1}$ and $B_{n+1} = B_n + \frac{v_{n+1} v_{n+1}^T}{v_{n+1}^T v_{n+1}}$. Then the process $v_{n+1} = (\text{id} - B_n)v_{n+1} = w_{n+1} - B_n w_{n+1}$ with $v_1 = w_1$ turns a basis $\{w_1, w_2, \dots, w_k\}$ into a pairwise orthogonal basis $\{v_1, v_2, \dots, v_k\}$ for the same vector space.
- **theorem 5.3.6 gram-schmidt dot product iteration:** (page 524) The process $v_{n+1} = w_{n+1} - \text{proj}_{v_1} w_{n+1} - \text{proj}_{v_2} w_{n+1} - \dots - \text{proj}_{v_n} w_{n+1}$ with $v_1 = w_1$ turns a basis $\{w_1, w_2, \dots, w_k\}$ into a pairwise orthogonal basis $\{v_1, v_2, \dots, v_k\}$ for the same vector space. We use the formula

$$\text{proj}_v w = \frac{v \bullet w}{v \bullet v} v$$

- **orthogonal basis:** (page 525) An orthogonal basis is one that is pairwise orthogonal
- **orthonormal basis:** (page 525) An orthonormal basis is an orthogonal basis such that each basis vector has length 1.
- **theorem 5.3.7 :** (page 525) If $C = \{c_1, c_2, \dots, c_n\}$ is an orthonormal basis, then

$$c_i \bullet c_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

- **theorem 5.3.8 :** (page 526) Suppose that the columns of a matrix B form an orthonormal basis for the column space of B —that is for the range of B thought of as a function under the column interpretation. Then, B^T is a left inverse for B . That is:

$$B^T \cdot B = \text{id}$$

Conversely, if $B^T \cdot B = \text{id}$, then the columns of B form an orthonormal basis for the column space of B .

- **theorem 5.3.9 :** (page 526) If A represents an injective linear transformation, then the matrix $A^T A$ is a square matrix which represents an isomorphism.
- **upper triangular matrix:** (page 529) A *square* matrix is said to be upper triangular, if below the diagonal from top left to bottom right, there are only 0's.

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

- **qr decomposition:** (page 530) A QR decomposition for a matrix A is writing the matrix A as the product QR where the columns of Q form an orthonormal basis for the span of the columns of A and R is an upper triangular matrix.
- **lemma 5.3.10 :** (page 532) The inverse of an upper triangular matrix which represents an isomorphism is upper triangular.
- **lemma 5.3.11 :** (page 532) The product of two upper triangular square $n \times n$ matrices is upper triangular.
- **theorem 5.3.12 :** (page 532) The QR decomposition of a matrix is unique.
- **theorem 5.3.13 :** (page 533) If Q is a matrix with orthonormal columns and that v is a column vector that we have an equality of vector lengths: $|Qv| = |v|$.
- **lower triangular matrix:** (page 533) A *square* matrix is said to be lower triangular if above the diagonal from top left to bottom right, there are only 0's.

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

- **lq decomposition:** (page 534) A LQ decomposition for a matrix A is writing the matrix A as the product LQ where the rows of Q form an orthonormal basis for the span of the rows of A and L is an lower triangular matrix.

5.3.7 Exercises

Practice with Gram-Schmidt Orthogonalization

Given each of the following ordered sets of linearly independent vectors, perform the Gram-Schmidt technique to obtain an orthogonal basis for the span of the vectors.

1. $(0, 0, 0, -1)$

$(0, 1, 0, 0)$

$(1, 1, 0, -1)$

2. $(0, 1, -1, 1)$

$(-1, -1, 0, -1)$

$(0, 0, 0, -1)$

3. $(-1, 0, 0, 0)$

$(-1, 0, 0, 1)$

$(0, 1, -1, 0)$

4. $(0, -1, 0, 0)$

$(1, 0, 1, 0)$

$(0, 0, 0, -1)$

5. $(0, 1, 0, -1)$

$(-1, 0, 1, 1)$

$(0, -1, 0, 0)$

6. $(0, 0, 0, 1)$

$(-1, 0, 1, 1)$

$(0, -1, -1, 1)$

7. $(-1, -1, 0, 0)$

$(1, 1, 0, 1)$

$(0, -1, 1, -1)$

8. $(0, 1, -1, -1)$

$(0, -1, 1, 0)$

$(0, -1, 0, 0)$

9. $(0, 0, -1, 1)$

$(1, -1, -1, 0)$

$(0, 1, 0, -1)$

10. $(0, -1, -1, 1)$

$(-1, 1, -1, 0)$

$(0, 1, -1, -1)$

11. $(-1, 0, -1, 0)$

$(0, 1, 0, -1)$

$(-1, -1, -1, -1)$

12. $(1, -1, 1, -1)$

$(1, 1, 1, 0)$

$(0, 0, 1, 0)$

13. $(0, 1, 1, 0)$

$(-1, 0, 0, 0)$

$(0, 0, 1, 1)$

14. $(-1, -1, 0, -1)$

$(0, 0, 0, -1)$

$(0, -1, 1, 1)$

15. $(0, 0, 1, 0)$
 $(-1, 1, 0, -1)$
 $(0, -1, 0, 0)$

16. $(0, 0, -1, -1)$
 $(-1, 1, 0, 0)$
 $(0, 0, 1, 0)$

17. $(0, 0, 1, -1)$
 $(0, -1, 0, -1)$
 $(0, 0, -1, 0)$

18. $(1, 0, 0, -1)$
 $(-1, 0, 0, 0)$
 $(-1, 0, -1, 1)$

19. $(1, 0, 0, 0)$
 $(-1, 0, 0, -1)$
 $(0, -1, 1, 1)$

20. $(0, 1, 1, 1)$
 $(0, -1, 0, 1)$
 $(-1, -1, 0, 1)$

QR Decomposition

Perform a QR decomposition on each of the following matrices.

21.
$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

22.
$$\begin{pmatrix} -1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

23.
$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}$$

24.
$$\begin{pmatrix} -1 & -1 & -1 \\ 1 & -1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

25.
$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 1 \end{pmatrix}$$

26.
$$\begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ -1 & -1 & 0 \\ -1 & 0 & -1 \end{pmatrix}$$

27.
$$\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \\ 1 & -1 & 1 \end{pmatrix}$$

28.
$$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1 \\ -1 & -1 & 0 \end{pmatrix}$$

29.
$$\begin{pmatrix} 0 & -1 & 0 \\ -1 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

30.
$$\begin{pmatrix} -1 & -1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ -1 & -1 & 0 \end{pmatrix}$$

Proof Practice

31. Prove by induction that an upper triangular square matrix whose columns are orthonormal is an identity matrix. First change the statement to: *the first n columns of an upper triangular matrix whose columns are orthonormal are the first n standard basis vectors in order.* The base case is to show that this statement is true when $n = 1$. The inductive step is to assume that if this statement is true, then it is true for the first $n + 1$ columns as well.
32. Prove that if Q is a matrix with orthonormal columns and that v is a column vector that we have an equality of vector lengths: $|Qv| = |v|$. This in particular shows that such a matrix Q describes a linear transformation that preserves all lengths! You should note that Q must be a injective function in order to have orthonormal columns. Therefore, Q injects vectors from one vector space into a potentially much larger one all the while preserving their lengths.

5.3.8 Solutions

1. $(0, 0, 0, -1)$

$(0, 1, 0, 0)$

$(1, 0, 0, 0)$

2. $(0, 1, -1, 1)$

$(-1, -1/3, -2/3, -1/3)$

$(1/5, 2/5, -1/5, -3/5)$

3. $(-1, 0, 0, 0)$

$(0, 0, 0, 1)$

$(0, 1, -1, 0)$

4. $(0, -1, 0, 0)$

$(1, 0, 1, 0)$

$(0, 0, 0, -1)$

5. $(0, 1, 0, -1)$

$(-1, 1/2, 1, 1/2)$

$(-1/5, -2/5, 1/5, -2/5)$

6. $(0, 0, 0, 1)$

$(-1, 0, 1, 0)$

$(-1/2, -1, -1/2, 0)$

7. $(-1, -1, 0, 0)$

$(0, 0, 0, 1)$

$(1/2, -1/2, 1, 0)$

8. $(0, 1, -1, -1)$

$(0, -1/3, 1/3, -2/3)$

$(0, -1/2, -1/2, 0)$

9. $(0, 0, -1, 1)$

$(1, -1, -1/2, -1/2)$

$(1/5, 4/5, -3/5, -3/5)$

10. $(0, -1, -1, 1)$

$(-1, 1, -1, 0)$

$(2/3, 0, -2/3, -2/3)$

11. $(-1, 0, -1, 0)$

$(0, 1, 0, -1)$

$(0, -1, 0, -1)$

12. $(1, -1, 1, -1)$

$(3/4, 5/4, 3/4, 1/4)$

$(-5/11, -1/11, 6/11, 2/11)$

13. $(0, 1, 1, 0)$

$(-1, 0, 0, 0)$

$(0, -1/2, 1/2, 1)$

14. $(-1, -1, 0, -1)$

$(1/3, 1/3, 0, -2/3)$

$(1/2, -1/2, 1, 0)$

15. $(0, 0, 1, 0)$

$(-1, 1, 0, -1)$

$(-1/3, -2/3, 0, -1/3)$

16. $(0, 0, -1, -1)$

$(-1, 1, 0, 0)$

$(0, 0, 1/2, -1/2)$

17. $(0, 0, 1, -1)$
 $(0, -1, -1/2, -1/2)$
 $(0, 1/3, -1/3, -1/3)$

18. $(1, 0, 0, -1)$
 $(-1/2, 0, 0, -1/2)$
 $(0, 0, -1, 0)$

19. $(1, 0, 0, 0)$
 $(0, 0, 0, -1)$
 $(0, -1, 1, 0)$

20. $(0, 1, 1, 1)$
 $(0, -1, 0, 1)$
 $(-1, 0, 0, 0)$

21. $Q = \begin{pmatrix} -\frac{1}{2}\sqrt{2} & -\sqrt{\frac{1}{2}} & 0 \\ 0 & 0 & -1 \\ -\frac{1}{2}\sqrt{2} & \sqrt{\frac{1}{2}} & 0 \\ 0 & 0 & 0 \end{pmatrix}$
 $R = \begin{pmatrix} \sqrt{2} & -\frac{1}{2}\sqrt{2} & 0 \\ 0 & \sqrt{\frac{1}{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$

22. $Q = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \frac{1}{2}\sqrt{2} & 0 \\ 0 & 0 & 1 \\ 0 & \frac{1}{2}\sqrt{2} & 0 \end{pmatrix}$
 $R = \begin{pmatrix} 1 & 0 & 1 \\ 0 & \sqrt{2} & -\sqrt{2} \\ 0 & 0 & 1 \end{pmatrix}$

23. $Q = \begin{pmatrix} 0 & 0 & \frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & -\sqrt{\frac{1}{2}} & 0 \\ 0 & 0 & -\frac{1}{2}\sqrt{2} \\ -\frac{1}{2}\sqrt{2} & -\sqrt{\frac{1}{2}} & 0 \end{pmatrix}$
 $R = \begin{pmatrix} \sqrt{2} & -\frac{1}{2}\sqrt{2} & 0 \\ 0 & \sqrt{\frac{1}{2}} & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix}$

24. $Q = \begin{pmatrix} -\frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{3} & \frac{1}{2}\sqrt{\frac{2}{3}} \\ \frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{3} & \frac{1}{2}\sqrt{\frac{2}{3}} \\ 0 & \frac{1}{3}\sqrt{3} & \sqrt{\frac{2}{3}} \\ 0 & 0 & 0 \end{pmatrix}$
 $R = \begin{pmatrix} \sqrt{2} & 0 & \sqrt{2} \\ 0 & \sqrt{3} & \frac{1}{3}\sqrt{3} \\ 0 & 0 & \sqrt{\frac{2}{3}} \end{pmatrix}$

25. $Q = \begin{pmatrix} \frac{1}{2} & \frac{1}{2}\sqrt{2} & \frac{1}{6}\sqrt{3} \\ -\frac{1}{2} & 0 & -\frac{1}{6}\sqrt{3} \\ -\frac{1}{2} & 0 & \frac{1}{2}\sqrt{3} \\ \frac{1}{2} & -\frac{1}{2}\sqrt{2} & \frac{1}{6}\sqrt{3} \end{pmatrix}$
 $R = \begin{pmatrix} 2 & 0 & 1 \\ 0 & \sqrt{2} & 0 \\ 0 & 0 & \sqrt{3} \end{pmatrix}$

26. $Q = \begin{pmatrix} 0 & -\frac{3}{5}\sqrt{\frac{5}{3}} & -\frac{1}{3}\sqrt{\frac{3}{5}} \\ -\frac{1}{3}\sqrt{3} & \frac{1}{5}\sqrt{\frac{5}{3}} & \frac{2}{3}\sqrt{\frac{3}{5}} \\ -\frac{1}{3}\sqrt{3} & -\frac{2}{5}\sqrt{\frac{5}{3}} & \frac{1}{3}\sqrt{\frac{3}{5}} \\ -\frac{1}{3}\sqrt{3} & \frac{1}{5}\sqrt{\frac{5}{3}} & -\sqrt{\frac{3}{5}} \end{pmatrix}$
 $R = \begin{pmatrix} \sqrt{3} & \frac{1}{3}\sqrt{3} & \frac{1}{3}\sqrt{3} \\ 0 & \sqrt{\frac{5}{3}} & -\frac{1}{5}\sqrt{\frac{5}{3}} \\ 0 & 0 & \sqrt{\frac{3}{5}} \end{pmatrix}$

$$27. Q = \begin{pmatrix} 0 & 0 & \frac{1}{2}\sqrt{2} \\ -\frac{1}{2}\sqrt{2} & -\sqrt{\frac{1}{2}} & 0 \\ 0 & 0 & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & -\sqrt{\frac{1}{2}} & 0 \end{pmatrix}$$

$$R = \begin{pmatrix} \sqrt{2} & -\frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} \\ 0 & \sqrt{\frac{1}{2}} & -\sqrt{\frac{1}{2}} \\ 0 & 0 & \sqrt{2} \end{pmatrix}$$

$$28. Q = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & \frac{1}{2}\sqrt{2} \\ 0 & 0 & -\frac{1}{2}\sqrt{2} \\ -1 & 0 & 0 \end{pmatrix}$$

$$R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix}$$

$$29. Q = \begin{pmatrix} 0 & -\frac{2}{5}\sqrt{\frac{5}{2}} & -\frac{2}{3}\sqrt{\frac{3}{5}} \\ -\frac{1}{2}\sqrt{2} & -\frac{1}{5}\sqrt{\frac{5}{2}} & -\frac{1}{3}\sqrt{\frac{3}{5}} \\ -\frac{1}{2}\sqrt{2} & \frac{1}{5}\sqrt{\frac{5}{2}} & \frac{1}{3}\sqrt{\frac{3}{5}} \\ 0 & \frac{2}{5}\sqrt{\frac{5}{2}} & -\sqrt{\frac{3}{5}} \end{pmatrix}$$

$$R = \begin{pmatrix} \sqrt{2} & \frac{1}{2}\sqrt{2} & 0 \\ 0 & \sqrt{\frac{5}{2}} & -\frac{2}{5}\sqrt{\frac{5}{2}} \\ 0 & 0 & \sqrt{\frac{3}{5}} \end{pmatrix}$$

$$30. Q = \begin{pmatrix} -\frac{1}{2}\sqrt{2} & 0 & -\sqrt{\frac{1}{2}} \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ -\frac{1}{2}\sqrt{2} & 0 & \sqrt{\frac{1}{2}} \end{pmatrix}$$

$$R = \begin{pmatrix} \sqrt{2} & \sqrt{2} & \frac{1}{2}\sqrt{2} \\ 0 & 1 & 1 \\ 0 & 0 & \sqrt{\frac{1}{2}} \end{pmatrix}$$

31. For the base case, the first column is of the form $c_1 = (a, 0, 0, \dots, 0)$. Clearly, $c_1 \bullet c_1 = a^2$ so that $|c_1| = a$. Yet since we assume orthonormality, $a = 1$ so that $c_1 = e_1$. Next, assume that the statement is true for n . Then the $n + 1$ st column, $c_{n+1} \bullet \underbrace{c_j}_{e_j} = 0$ for $j \in \{1, \dots, n\}$. This says that c_{n+1} is 0 in each component except for its $(n + 1)$ st entry. This one nonzero entry must be 1 to ensure that the length of c_{n+1} is 1. Therefore, $c_{n+1} = e_{n+1}$. This completes the inductive step.

32. This is the same as proving we have an equality of $Qv \bullet Qv = v \bullet v$. We can rewrite $Qv \bullet Qv$ as $(Qv)^T Qv = v^T \underbrace{Q^T Q}_{\text{id}} v = v^T v = v \bullet v$ which proves the result.

Least Squares

5.4

5.4.1 Orthogonal Right Inverse gives Closest Solution	544
5.4.2 Two Examples	546
5.4.3 Intuition For Best Fit Line	549
5.4.4 Fitting to other Curves	550
5.4.5 Using Calculus to Prove Minimality (Optional)	553
5.4.6 Exercises	556
5.4.7 Solutions	558

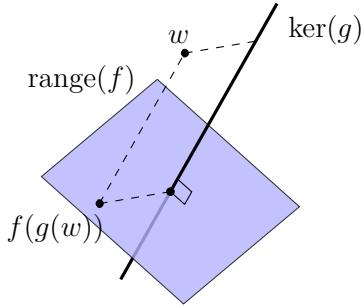
Questions to Guide Your Study:

- *How can you use an orthogonal right inverse to minimize a distance?*
- *How can you use this idea to find a straight line of best fit among a series of points?*
- *How is this orthogonal right inverse idea equivalent to minimizing a sum of squares?*
- *How can calculus prove that our right inverse idea is a minimum?*

5.4.1 Orthogonal Right Inverse gives Closest Solution



Suppose that we want to figure out a vector x such that $f(x)$ is the closest it can be to w for a linear transformation $f : D \rightarrow C$. If w is outside of the range of f and if f is injective, then the closest we can get $f(x)$ to w is by drawing a line orthogonal to $\text{range}(f)$ so that it hits w . The way to do this is by a left-right inverse pair (f, g) so that f itself is an orthogonal right inverse to $g : C \rightarrow D$. Then, $(f \circ g)(w)$ is the orthogonal projection of w onto $\text{range}(f)$. This tells us that $x = g(w)$ is the desired vector as we can see illustrated below:



So our task is to determine how to construct g if we know the matrix for f so that f will be an orthogonal right inverse. If we assume that f is injective and represented by a matrix A , then we proved in the last section using a QR decomposition that $A^T A$ is an isomorphism and so has an inverse. Notice the following:

$$(A^T A)^{-1} (A^T) A = \text{id} \quad \longrightarrow \quad \underbrace{\left((A^T A)^{-1} A^T \right)}_{g = \text{left Inverse of } f} \cdot \underbrace{A}_{f} = \text{id}$$

We have just found a left inverse of f which we call g . Notice that f is a right inverse of g and so decomposes the domain C of g as we have seen before as

$$\text{range}(f) \bigoplus \ker(g)$$

We are decomposing the codomain of f because it is the domain of g and g is the function that has a right inverse.

Suppose that $k \in \ker(g)$. Then:

$$0_D = g(k) = (A^T A)^{-1} A^T \cdot k$$

Multiply both sides of this equation on the left by $(A^T A)$:

$$\underbrace{(A^T A) \cdot 0_D}_{0_D} = g(k) = \underbrace{(A^T A) \cdot (A^T A)^{-1} A^T \cdot k}_{\text{id}}$$

$$0_D = A^T \cdot k$$

This means that $k \in \ker(A^T)$. That is,

$$\ker(g) \subset \ker(A^T)$$

We know that

$$\ker(A^T) \perp \text{range}(A) \implies \ker(g) \perp \text{range}(f)$$

We see that f is an *orthogonal right inverse* to g . Simply using the function g given by $(A^T A)^{-1} A^T$ can solve a lot of minimization problems! We will examine one type of these in this section.

5.4.2 Two Examples

Example 1. Let's find the line $y = mt + b$ that best fits the points $(0, -1)$, $(2, -1)$, and $(1, 0)$. To do this, we think:

$$\begin{array}{rcl} y & = & m \cdot t + b \\ (-1) & = & m \cdot (0) + b \\ (-1) & = & m \cdot (2) + b \\ (0) & = & m \cdot (1) + b \end{array} \implies \begin{array}{rcl} t \cdot m + 1 \cdot b & = & y \\ (0) \cdot m + 1 \cdot b & = & (-1) \\ (2) \cdot m + 1 \cdot b & = & (-1) \\ (1) \cdot m + 1 \cdot b & = & (0) \end{array}$$

That is,

$$\underbrace{\begin{pmatrix} 0 & 1 \\ 2 & 1 \\ 1 & 1 \end{pmatrix}}_{f : A} \cdot \underbrace{\begin{pmatrix} m \\ b \end{pmatrix}}_x \stackrel{\text{get close}}{\approx} \underbrace{\begin{pmatrix} -1 \\ -1 \\ 0 \end{pmatrix}}_w$$

We are trying to find the input $x = (m, b)$ of f that gets us closest to $w = (-1, -1, 0)$. We found above that $x = g(w)$ does this where g is given by $(A^T A)^{-1} A^T$.

We find:

$$A^T A = \underbrace{\begin{pmatrix} 0 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}}_{A^T} \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ 2 & 1 \\ 1 & 1 \end{pmatrix}}_A = \begin{pmatrix} 5 & 3 \\ 3 & 3 \end{pmatrix}$$

Now we compute $(A^T A)^{-1}$ by only using row operations. First, we find the row operations that take the matrix to the identity:

$$\begin{array}{ccc} \begin{pmatrix} 5 & 3 \\ 3 & 3 \end{pmatrix} & \xrightarrow{\quad} & \begin{pmatrix} 5 & 3 \\ 1 & 1 \end{pmatrix} \\ \left(\begin{array}{cc} \cancel{\frac{1}{3} \cdot 3} & \cancel{\frac{1}{3} \cdot 3} \\ 1 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & \frac{3}{5} \\ 1 & 1 \end{array} \right) \\ \left(\begin{array}{cc} 1 & \frac{3}{5} \\ -1 \cdot 1 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & \frac{3}{5} \\ 0 & \frac{2}{5} \end{array} \right) \\ \left(\begin{array}{cc} 1 & \frac{3}{5} \\ -\frac{3}{5} \cdot 0 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \end{array}$$

Now, we apply those same row operations to the identity and we will have $(A^T A)^{-1}$:

$$\begin{array}{ccc} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \xrightarrow{\quad} & \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{3} \end{pmatrix} \\ \left(\begin{array}{cc} \cancel{\frac{1}{3} \cdot 0} & \cancel{\frac{1}{3} \cdot 1} \\ 1 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & 0 \\ 0 & \frac{1}{3} \end{array} \right) \end{array}$$

$$\begin{array}{ccc}
 \left(\begin{array}{cc} \frac{1}{5} & 0 \\ 0 & \frac{1}{3} \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} \frac{1}{5} & 0 \\ -\frac{1}{5} & \frac{1}{3} \end{array} \right) \\
 \left(\begin{array}{cc} \frac{1}{5} & 0 \\ -\frac{3}{5} \cdot \frac{-1}{2} & \frac{5}{6} \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{5}{6} \end{array} \right)
 \end{array}$$

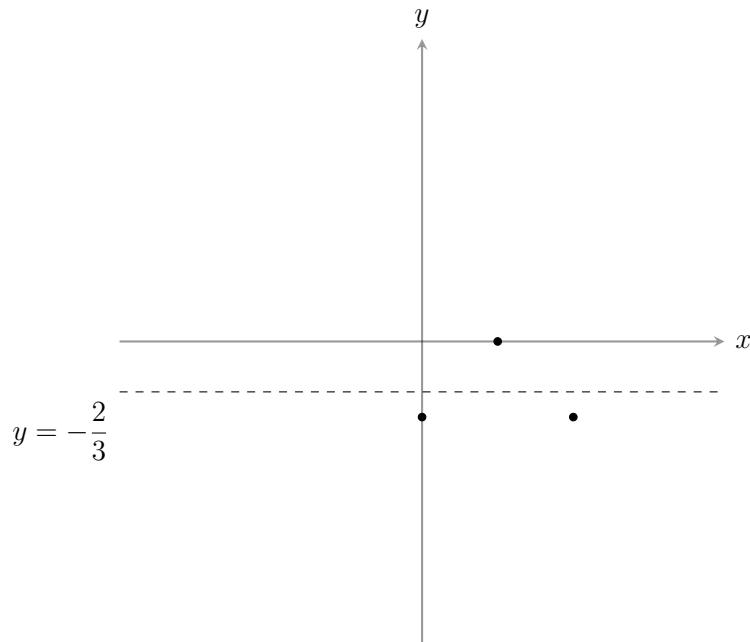
Therefore we have:

$$g(w) = \underbrace{\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{5}{6} \end{pmatrix}}_{(A^T A)^{-1}} \cdot \underbrace{\begin{pmatrix} 0 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}}_{A^T} \cdot \underbrace{\begin{pmatrix} -1 \\ -1 \\ 0 \end{pmatrix}}_w$$

For a faster calculation, first compute $A^T w = \begin{pmatrix} -2 \\ -2 \end{pmatrix}$ so that

$$g(w) = \underbrace{\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{5}{6} \end{pmatrix}}_{(A^T A)^{-1}} \cdot \underbrace{\begin{pmatrix} -2 \\ -2 \end{pmatrix}}_{A^T w} = \begin{pmatrix} 0 \\ -\frac{2}{3} \end{pmatrix} = b$$

Therefore, the line of best fit is $y = 0 \cdot x - \frac{2}{3}$ which is simply the horizontal line $y = -\frac{2}{3}$:





Example 2. Let's change one of the points in the last example and then find the line of best fit between them. Consider the points:

$$(0, -1) \quad (-1, -1) \quad (1, 0)$$

Following the same setup from the last example, we have that

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

and that w is again $(-1, -1, 0)$ since we only changed the point $(2, -1)$ to $(-1, -1)$. We compute $g(w) = (A^T A)^{-1} A^T \cdot w$:

$$A^T A = \underbrace{\begin{pmatrix} 0 & -1 & 1 \\ 1 & 1 & 1 \end{pmatrix}}_{A^T} \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 1 \\ 1 & 1 \end{pmatrix}}_A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$$

Therefore,

$$(A^T A)^{-1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$$

Compute $A^T \cdot w$:

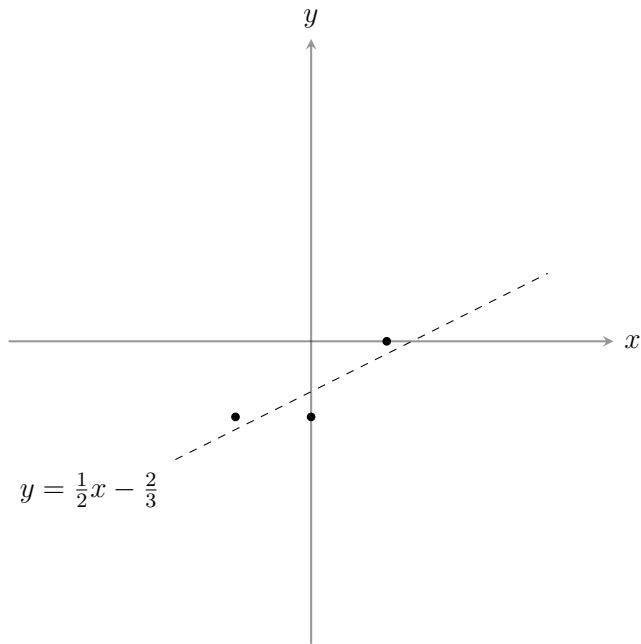
$$\underbrace{\begin{pmatrix} 0 & -1 & 1 \\ 1 & 1 & 1 \end{pmatrix}}_{A^T} \cdot \underbrace{\begin{pmatrix} -1 \\ -1 \\ 0 \end{pmatrix}}_w = \begin{pmatrix} 1 \\ -2 \end{pmatrix}$$

Now compute $(A^T A)^{-1} A^T \cdot w$:

$$\underbrace{\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}}_{(A^T A)^{-1}} \cdot \underbrace{\begin{pmatrix} 1 \\ -2 \end{pmatrix}}_{A^T \cdot w} = \begin{pmatrix} \frac{1}{2} \\ -\frac{2}{3} \end{pmatrix} = \begin{pmatrix} m \\ b \end{pmatrix}$$

Therefore, the line of best fit is:

$$y = \frac{1}{2}x - \frac{2}{3}$$



Least Squares

The technique discussed in this section for finding a line of best fit given a list of points.

Why is it called “least squares?” This next little subsection helps with that.

5.4.3 Intuition For Best Fit Line

Consider example 2 above. We were trying to find a vector $x = (m, b)$ so that the distance from $f(x)$ to w was a minimum. This is the same as saying that the length of the vector $w - f(x)$ which runs between $f(x)$ and w has minimal length. That is, we were trying to find x so that $|w - f(x)| = \sqrt{(w - f(x)) \bullet (w - f(x))}$ reached a minimum. This is the same as trying to get $(w - f(x)) \bullet (w - f(x))$ to be minimal. Let’s try to understand what this means. Let $h(t) = mt + b$ be the line we are searching for and label our points as:

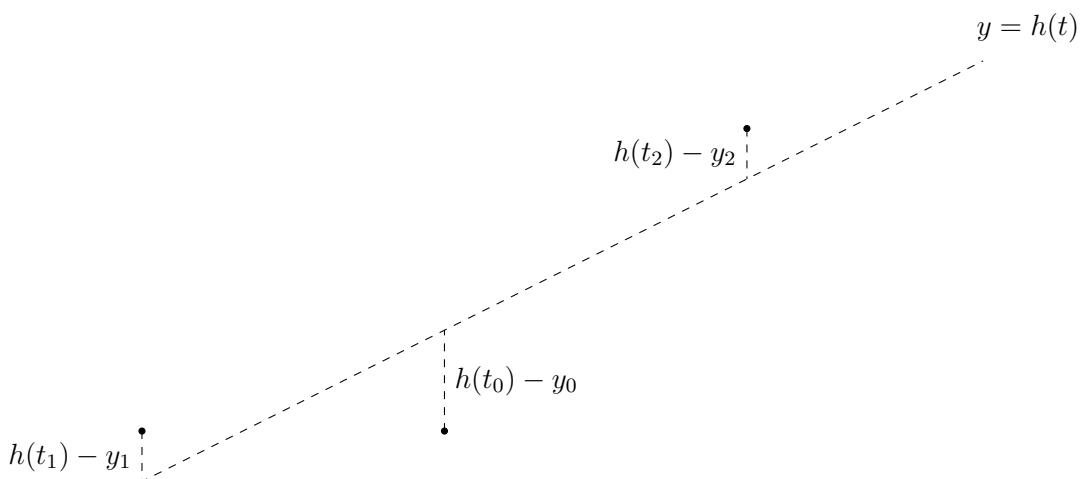
$$(t_0, y_0) = (0, -1) \quad (t_1, y_1) = (-1, -1) \quad (t_2, y_2) = (1, 0)$$

Note that $w = (-1, -1, 0) = (y_0, y_1, y_2)$. Consider:

$$f(x) = \underbrace{\begin{pmatrix} t_0 & 1 \\ t_1 & 1 \\ t_2 & 1 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} m \\ b \end{pmatrix}}_x = \begin{pmatrix} m \cdot t_0 + 1 \cdot b \\ m \cdot t_1 + 1 \cdot b \\ m \cdot t_2 + 1 \cdot b \end{pmatrix} = h(t_0) = h(t_1) = h(t_2)$$

$$w - f(x) = \underbrace{\begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}}_w - \underbrace{\begin{pmatrix} h(t_0) \\ h(t_1) \\ h(t_2) \end{pmatrix}}_{f(x)} = \begin{pmatrix} y_0 - h(t_0) \\ y_1 - h(t_1) \\ y_2 - h(t_2) \end{pmatrix}$$

We can visualize the components of the vector $w - f(x)$ whose length we want to minimize:



To minimize the length of the vector $|w - f(x)|$ we minimize

$$\begin{aligned} (w - f(x)) \bullet (w - f(x)) &= \begin{pmatrix} h(t_0) - y_0 & h(t_1) - y_1 & h(t_2) - y_2 \end{pmatrix} \cdot \begin{pmatrix} h(t_0) - y_0 \\ h(t_1) - y_1 \\ h(t_2) - y_2 \end{pmatrix} \\ &= (h(t_0) - y_0)^2 + (h(t_1) - y_1)^2 + (h(t_2) - y_2)^2 \end{aligned}$$

We are trying to minimize the sum of the squares of the distances between the y -values of the points and the corresponding y -values on the desired line.

5.4.4 Fitting to other Curves

We can use the very same method that we have just used to find a best fit curve of many other types than just straight lines.

Example 3. Suppose that we want to find the best fitting parabola of the form $y = ax^2 + bx + c$ to the following points:

$$(1, 0), (2, 1), (0, -2), (1, -2)$$

We think:

$$\begin{aligned}(1, 0) : \quad a \cdot (1)^2 + b \cdot (1) + c &= 0 \\ ((2, 1) : \quad a \cdot (2)^2 + b \cdot (2) + c &= 1 \\ (0, -2) : \quad a \cdot (0)^2 + b \cdot (0) + c &= -2 \\ (1, -2) : \quad a \cdot (1)^2 + b \cdot (1) + c &= -2\end{aligned}$$

Then, we rewrite these equations as a single matrix equation:

$$\underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}}_A \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ -2 \\ -2 \end{pmatrix}$$

Now, we compute:

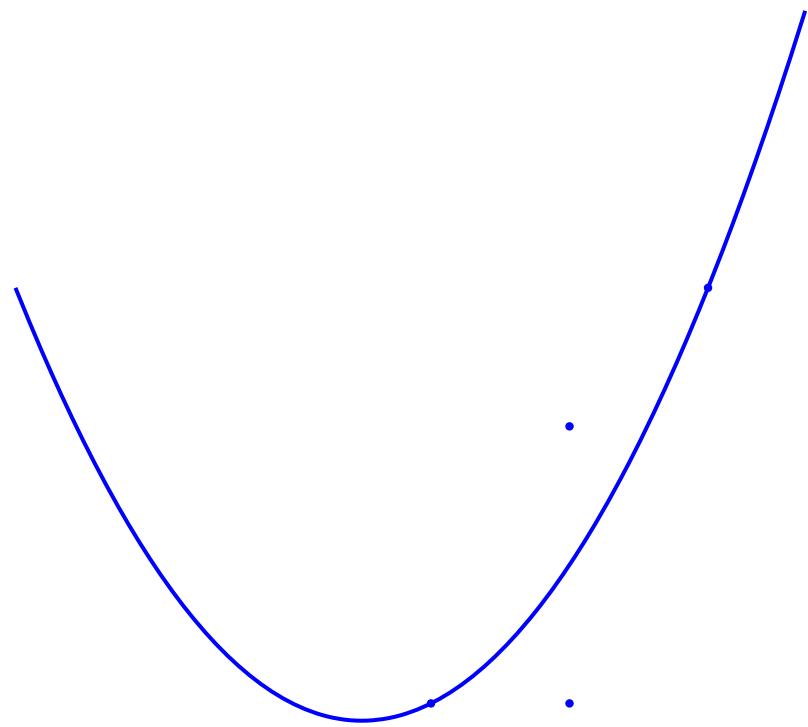
$$\left(\underbrace{\begin{pmatrix} 1 & 4 & 0 & 1 \\ 1 & 2 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}}_{A^T} \cdot \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}}_A \right)^{-1} = \begin{pmatrix} 1 & -2 & \frac{1}{2} \\ -2 & \frac{9}{2} & -\frac{3}{2} \\ \frac{1}{2} & -\frac{3}{2} & 1 \end{pmatrix}$$

Therefore, we set:

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & -2 & \frac{1}{2} \\ -2 & \frac{9}{2} & -\frac{3}{2} \\ \frac{1}{2} & -\frac{3}{2} & 1 \end{pmatrix}}_{(A^T A)^{-1}} \cdot \underbrace{\begin{pmatrix} 1 & 4 & 0 & 1 \\ 1 & 2 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}}_{A^T} \cdot \begin{pmatrix} 0 \\ 1 \\ -2 \\ -2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ -2 \end{pmatrix}$$

The best fitting parabola is:

$$\frac{1}{2}x^2 + \frac{1}{2}x - 2$$



Example 4. Let's find a best fit curve of the form $y = a \cdot \ln(x) + b$ for the points:

$$(2, 1), (4, 2), (3, 4)$$

Using the same method as we did in the previous example we are looking for a close solution to:

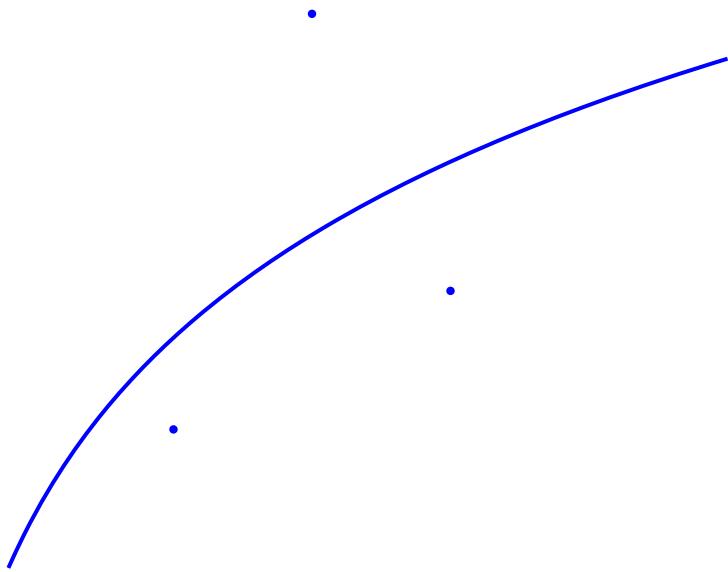
$$\underbrace{\begin{pmatrix} 0.693147180559945 & 1.000000000000000 \\ 1.38629436111989 & 1.000000000000000 \\ 1.09861228866811 & 1.000000000000000 \end{pmatrix}}_A \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix}$$

We calculate:

$$(A^T A)^{-1} A^T \cdot \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 1.83362991631818 \\ 0.390875140334802 \end{pmatrix}$$

so that our best fit curve is:

$$y = 1.83362991631818 \ln(x) + 0.390875140334802$$



5.4.5 Using Calculus to Prove Minimality (Optional)

We want to find out when

$$(w - \underbrace{A \cdot x}_{f(x)}) \bullet (w - \underbrace{A \cdot x}_{f(x)})$$

achieves a minimum. We compute:

$$(w - A \cdot x) \bullet (w - A \cdot x) = (w - A \cdot x)^T (w - A \cdot x) = (w^T - x^T A^T) \cdot (w - A \cdot x)$$

$$w^T w - w^T A x - x^T A^T w + x^T A^T A x$$

This matrix expression is a function of $x = (m, b)$. The vector w is a constant. We would like to determine when the derivative matrix of this expression is momentarily zero—this is the only time we could potentially have a peak or a valley if everything is smooth and unjagged. Each part of this matrix expression actually evaluates to just a number in \mathbb{R}^1 (a 1×1 matrix). We will use the following ideas:

- When we take a derivative of a linear transformation $x \mapsto Mx$ we just get M as the derivative matrix since the derivative is the approximating linear transformation itself.

- Since the function $x \mapsto x^T M^T$ component-wise is the same as $x \mapsto Mx$, they have the *same* derivative. Derivative matrices are written with respect to a *column interpretation*.
- The derivative of a constant matrix function with nothing variable is simply a zero matrix. For instance, the derivative of $f(x, y) = 0$ is $\begin{pmatrix} 0 & 0 \end{pmatrix}$. A *constant matrix is simply a shift of the zero linear transformation*.
- The product rule generalizes to a *boxing rule* thought of in the following way. Suppose that we think of our variables that occur in two different parts of the matrix expression as being *different variables even if they are not* and then compose with a function that makes them the same. That is, suppose that we split all variables that we see into two groups. The variables that occur in group 1 we add a subscript to make them different from any variable in group 2. So if both groups both have variables m and b , now we have variables m_* and b_* coming from the first group and m and b coming from the second group. Say that there are i variables in the first group and j variables in the second group. Then there are a total of $i + j$ new variables. In our current example there are $2 + 2 = 4$ variables. The function which the matrix expression describes now looks like: $(m_*, b_*, m, b) \mapsto$ matrix expression. Now, precompose this function with one that reassigns m_* and b_* as m and b . That is, this precomposed function looks like: $(m, b) \mapsto (m, b, m, b)$. The chain rule tells us the derivative of our matrix expression is the product of the derivatives of the functions we are composing:

$$\begin{pmatrix} \text{Derivative with respect to } m_* \text{ and } b_* \text{ only} & \text{Derivative with respect to } m \text{ and } b \text{ only} \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}}_{\text{Derivative of precomposed function}}$$

Through matrix block multiplication this just becomes:

$$\begin{pmatrix} \text{Derivative assuming everything out of group 1 is constant} \end{pmatrix} + \begin{pmatrix} \text{Derivative assuming everything out of group 2 is constant} \end{pmatrix}$$

Let's consider the derivative of $x \mapsto x^T A^T Ax$ where $x = (m, b)$. This is a function $\mathbb{R}^2 \rightarrow \mathbb{R}$. Think of every variable coming from x^T as being in group 1 and from x on the right as in group 2. Then, to take the derivative we proceed as follows. We first pretend that group 2 is constant and group 1 is variable. Then the function

$$x \mapsto x^T \underbrace{A^T Ax}_{\text{pretend to be constant}}$$

would have derivative $(A^T Ax)^T = x^T A^T A$. Next, we pretend that group 1 is constant and group 2 is variable.

Then the function

$$x \mapsto \underbrace{x^T A^T A}_{\text{pretend to be constant}} x$$

would have derivative $(x^T A^T A)$. Therefore, add these two derivative matrices together to get the real derivative:

$$x^T A^T A + x^T A^T A = 2x^T A^T A.$$

Using all these ideas, we obtain that the derivative of $\underbrace{w^T w}_{\text{derivative}=0} - \underbrace{w^T A x}_{\text{derivative}=w^T A} - \underbrace{x^T A^T w}_{\text{derivative}=w^T A} + \underbrace{x^T A^T A x}_{\text{derivative}=2x^T A^T A}$ is:

$$\text{first derivative: } -2w^T A + 2x^T A^T A$$

Notice that assigning $x = g(w) = (A^T A)^{-1} A^T w$ gives us:

$$-2w^T A + 2((A^T A)^{-1} A^T w)^T A^T A$$

Use the idea that the transpose of $(A^T A)^{-1}$ is itself since transposes go inside of inverses and $(A^T A)^T = A^T (A^T)^T = A^T A$:

$$-2w^T A + 2w^T A \underbrace{(A^T A)^{-1} (A^T A)}_{\text{id}} = \text{zero matrix.}$$

This tells us that our orthogonal inverse result really does tell us that the first derivative is instantaneously zero.

But does $x = g(w)$ give us a minimum? We have to check the *second* derivative. The first derivative is $-2w^T A + 2x^T A^T A$. The term $-2w^T A$ is a constant matrix and so goes away when we take its derivative. The derivative of $2x^T A^T A$ is $(2A^T A)^T = 2A^T A$. We will learn later in this textbook that any matrix of such a form turns out to be something called *positive definite* meaning that it has all positive *eigenvalues*—which we will also discuss. You can think of this as a *positive* second derivative or “concave up.” It has a minimum at this value of $x = (m, b)$! Wow! Derivative math with functions described by matrices follows a lot of the same ideas as single variable calculus!

Key Concepts from this Section

- **least squares:** (page 549) The technique discussed in this section for finding a line of best fit given a list of points.

5.4.6 Exercises

Fitting to a line $y = mx + b$

Find the line $y = mx + b$ of best fit that passes through the given points using the orthogonal left inverse technique explained in the section.

1. $(0, 2), (-2, -2), (-1, 0)$

2. $(1, -1), (-2, 2), (-1, 0)$

3. $(2, 2), (-2, -1), (-1, 1)$

4. $(0, 1), (1, 2), (-2, -1)$

5. $(0, 2), (2, 0), (-2, 2)$

6. $(1, -1), (2, 0), (-2, 2)$

7. $(0, 2), (1, -2), (-1, 1)$

8. $(0, -1), (2, 1), (-1, 2)$

9. $(1, -1), (2, -2), (-1, 1)$

10. $(0, 0), (1, -1), (2, 1)$

11. $(0, -2), (-2, -1), (-1, 2)$

12. $(1, 2), (-2, 1), (-1, -1)$

13. $(2, 1), (-2, -2), (-1, 1)$

14. $(0, 0), (1, -1), (-2, 1)$

15. $(0, 1), (2, -2), (-2, 1)$

16. $(1, 2), (2, 1), (-2, 2)$

17. $(0, 2), (1, -2), (-1, -1)$

18. $(0, 0), (2, 2), (-1, 1)$

19. $(1, 1), (2, -1), (-1, 0)$

20. $(0, 2), (1, 2), (2, -2)$

Fitting to a curve $y = a \cdot x^2 + b \cdot x + c$

Find an equation of the form $y = a \cdot x^2 + b \cdot x + c$ that best fits the given points.

21. $(1, -1), (-2, 1), (1, 2), (0, -1)$

22. $(0, -1), (-1, 0), (2, 2), (-1, 2)$

23. $(-2, 0), (-1, 2), (-2, 2), (1, 2)$

24. $(-1, 2), (1, 0), (0, -1), (-2, -2)$

25. $(-2, 1), (-1, -1), (0, 0), (1, 0)$

26. $(-2, -2), (0, -1), (-1, 2), (-1, 1)$

Fitting to a curve $y = a \cdot \ln(x) + b$

Find an equation of the form $y = a \cdot \ln(x) + b$ that best fits the given points.

27. $(4, 4), (2, 4), (1, 2)$

28. $(4, 2), (1, 2), (4, 1)$

29. $(4, 2), (3, 4), (4, 4)$

30. $(4, 3), (2, 1), (3, 4)$

31. $(3, 2), (2, 4), (3, 1)$

32. $(4, 4), (2, 4), (2, 1)$

5.4.7 Solutions

1. $y = 2x + 2$

is obtained from:

$$\begin{pmatrix} \frac{5}{6} & -\frac{1}{6} & \frac{1}{3} \\ \frac{1}{2} & -\frac{1}{2} & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -2 \\ 0 \end{pmatrix}$$

2. $y = -\frac{13}{14}x - \frac{2}{7}$

is obtained from:

$$\begin{pmatrix} \frac{4}{7} & \frac{1}{7} & \frac{2}{7} \\ \frac{5}{14} & -\frac{2}{7} & -\frac{1}{14} \end{pmatrix} \cdot \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}$$

3. $y = \frac{17}{26}x + \frac{23}{26}$

is obtained from:

$$\begin{pmatrix} \frac{11}{26} & \frac{7}{26} & \frac{4}{13} \\ \frac{7}{26} & -\frac{5}{26} & -\frac{1}{13} \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}$$

4. $y = x + 1$

is obtained from:

$$\begin{pmatrix} \frac{5}{14} & \frac{3}{7} & \frac{3}{14} \\ \frac{1}{14} & \frac{2}{7} & -\frac{5}{14} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}$$

5. $y = -\frac{1}{2}x + \frac{4}{3}$

is obtained from:

$$\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & \frac{1}{4} & -\frac{1}{4} \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 0 \\ 2 \end{pmatrix}$$

6. $y = -\frac{8}{13}x + \frac{7}{13}$

is obtained from:

$$\begin{pmatrix} \frac{4}{13} & \frac{7}{26} & \frac{11}{26} \\ \frac{1}{13} & \frac{5}{26} & -\frac{7}{26} \end{pmatrix} \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix}$$

7. $y = -\frac{3}{2}x + \frac{1}{3}$

is obtained from:

$$\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}$$

8. $y = -\frac{1}{7}x + \frac{5}{7}$

is obtained from:

$$\begin{pmatrix} \frac{5}{14} & \frac{3}{14} & \frac{3}{7} \\ -\frac{1}{14} & \frac{5}{14} & -\frac{2}{7} \end{pmatrix} \cdot \begin{pmatrix} -1 \\ 1 \\ 2 \end{pmatrix}$$

9. $y = -x$

is obtained from:

$$\begin{pmatrix} \frac{2}{7} & \frac{1}{7} & \frac{4}{7} \\ \frac{1}{14} & \frac{2}{7} & -\frac{5}{14} \end{pmatrix} \cdot \begin{pmatrix} -1 \\ -2 \\ 1 \end{pmatrix}$$

10. $y = \frac{1}{2}x - \frac{1}{2}$

is obtained from:

$$\begin{pmatrix} \frac{5}{6} & \frac{1}{3} & -\frac{1}{6} \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$$

11. $y = -\frac{1}{2}x - \frac{5}{6}$

is obtained from:

$$\begin{pmatrix} \frac{5}{6} & -\frac{1}{6} & \frac{1}{3} \\ \frac{1}{2} & -\frac{1}{2} & 0 \end{pmatrix} \cdot \begin{pmatrix} -2 \\ -1 \\ 2 \end{pmatrix}$$

12. $y = \frac{1}{2}x + 1$

is obtained from:

$$\begin{pmatrix} \frac{4}{7} & \frac{1}{7} & \frac{2}{7} \\ \frac{5}{14} & -\frac{2}{7} & -\frac{1}{14} \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix}$$

13. $y = \frac{15}{26}x + \frac{5}{26}$

is obtained from:

$$\begin{pmatrix} \frac{11}{26} & \frac{7}{26} & \frac{4}{13} \\ \frac{7}{26} & -\frac{5}{26} & -\frac{1}{13} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

14. $y = -\frac{9}{14}x - \frac{3}{14}$

is obtained from:

$$\begin{pmatrix} \frac{5}{14} & \frac{3}{7} & \frac{3}{14} \\ \frac{1}{14} & \frac{2}{7} & -\frac{5}{14} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$$

15. $y = -\frac{3}{4}x$

is obtained from:

$$\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & \frac{1}{4} & -\frac{1}{4} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

16. $y = -\frac{5}{26}x + \frac{45}{26}$

is obtained from:

$$\begin{pmatrix} \frac{4}{13} & \frac{7}{26} & \frac{11}{26} \\ \frac{1}{13} & \frac{5}{26} & -\frac{7}{26} \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}$$

17. $y = -\frac{1}{2}x - \frac{1}{3}$

is obtained from:

$$\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -2 \\ -1 \end{pmatrix}$$

18. $y = \frac{3}{7}x + \frac{6}{7}$

is obtained from:

$$\begin{pmatrix} \frac{5}{14} & \frac{3}{14} & \frac{3}{7} \\ -\frac{1}{14} & \frac{5}{14} & -\frac{2}{7} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}$$

19. $y = -\frac{3}{14}x + \frac{1}{7}$

is obtained from:

$$\begin{pmatrix} \frac{2}{7} & \frac{1}{7} & \frac{4}{7} \\ \frac{1}{14} & \frac{2}{7} & -\frac{5}{14} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$$

20. $y = -2x + \frac{8}{3}$

is obtained from:

$$\begin{pmatrix} \frac{5}{6} & \frac{1}{3} & -\frac{1}{6} \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 2 \\ -2 \end{pmatrix}$$

21. $f(x) = \frac{5}{6}x^2 + \frac{2}{3}x - 1$

22. $f(x) = \frac{7}{6}x^2 - \frac{5}{6}x - 1$

23. $f(x) = -\frac{1}{3}x^2 + \frac{7}{3}$

24. $f(x) = -\frac{3}{4}x^2 - \frac{9}{20}x + \frac{13}{20}$

25. $f(x) = \frac{1}{2}x^2 + \frac{3}{10}x - \frac{3}{5}$

26. $f(x) = -3x^2 - \frac{11}{2}x - 1$

$$\mathbf{27.} \ f(x) = 1.44269504088896 \ln(x) + 2.3$$

$$\mathbf{28.} \ f(x) = -0.360673760222241 \ln(x) + 2$$

$$\mathbf{29.} \ f(x) = -3.47605949678211 \ln(x) + 7.81884167930626$$

$$\mathbf{30.} \ f(x) = 3.18163398763897 \ln(x) - 0.703801360393752$$

$$\mathbf{31.} \ f(x) = -6.16575865594103 \ln(x) + 8.27377822837859$$

$$\mathbf{32.} \ f(x) = 2.16404256133344 \ln(x) + 1$$

Chapter 5 Selected Review Questions

Section 5.1

Can you use properties of transposes?

1. Prove that the following are symmetric matrices for any matrices A and B for which the following multiplications are well-defined:

(a) $A(BB^T)^{-1}A^T$

(b) $(ABA^T)(AB^TA^T)$

(c) $(A^TBB^TA)^{-1}$

Can you find a basis for the orthogonal complement V^\perp for the vector space V given? This technique allows you to find the vectors that are in the plane orthogonal to a line or find the line that is orthogonal to a plane, etc.

2. $V = \langle (1, 0, 2), (0, 1, -2) \rangle$

3. $V = \langle (1, 2, 0, 2), (0, 0, 1, -2) \rangle$

Section 5.2

Can you project a vector onto a $\text{range}(g)$ via $\ker(f)$? That is, can you find shadow vectors and light ray vectors?

In the following exercises, f is a left inverse to g and g is a right inverse to f . Find the unique decomposition of v as

$$v = \underbrace{v_p}_{\in \text{range}(g)} + \underbrace{v_k}_{\in \ker(f)}$$

That is, v_p is the shadow vector and v_k is the light ray.

4. $v = (-1, -2, 0)$

$$f : \begin{pmatrix} -1 & -1 & -2 \\ 0 & -2 & -2 \end{pmatrix}$$

$$g : \begin{pmatrix} -\frac{1}{2} & \frac{3}{8} \\ \frac{1}{2} & -\frac{5}{8} \\ -\frac{1}{2} & \frac{1}{8} \end{pmatrix}$$

5. $v = (0, 1, 0)$

$$f : \begin{pmatrix} 0 & -2 & 2 \\ 1 & 0 & 0 \end{pmatrix}$$

$$g : \begin{pmatrix} 0 & 1 \\ -\frac{1}{6} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

Can you find angled projections? For the following, find the unique matrix function (in a column interpretation) that tells how to project a vector in \mathbb{R}^2 onto the subspace $\langle v \rangle \subset \mathbb{R}^2$ given via “light rays” that are an angle θ counterclockwise rotation from v . That is, we are looking for the matrix describing $g \circ f$ where g is a *right* inverse to f , $\text{range}(g) = \langle v \rangle$, and $\ker(f)$ describes the direction of the “light rays.” This matrix function outputs the *shadow vector on the ground* $\langle v \rangle$.

6. Subspace = $\langle (0, 1) \rangle$

Angle: 45°

7. Subspace = $\langle (1, 0) \rangle$

Angle: 60°

Section 5.3

Can you perform the Gram Schmidt procedure? Given each of the following ordered sets of linearly independent vectors, perform the Gram-Schmidt technique to obtain an orthogonal basis for the span of the vectors.

8. $(0, 0, 0, -1)$

$$(0, 1, 0, 0)$$

$$(1, 1, 0, -1)$$

9. $(0, 1, -1, 1)$

$$(-1, -1, 0, -1)$$

$$(0, 0, 0, -1)$$

Section 5.4

Can you find the line $y = mx + b$ of best fit that passes through the given points using the orthogonal left inverse technique?

10. $(0, 2), (-2, -2), (-1, 0)$

11. $(1, -1), (-2, 2), (-1, 0)$

Solutions/Hints

1. In each case, just take the transpose of the expression. Using properties of the transpose and how the transpose interacts with inverses, verify that each expression is equal to its transpose.

2. $\langle(-2, 2, 1)\rangle$

3. $\langle(-2, 1, 0, 0), (-2, 0, 2, 1)\rangle$

4. $(0, -1, -1) + (-1, -1, 1)$

5. $(0, \frac{1}{3}, -\frac{2}{3}) + (0, \frac{2}{3}, \frac{2}{3})$

6.
$$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

7.
$$\begin{pmatrix} 1 & -\frac{1}{3}\sqrt{3} \\ 0 & 0 \end{pmatrix}$$

8. $(0, 0, 0, -1)$
 $(0, 1, 0, 0)$
 $(1, 0, 0, 0)$

9. $(0, 1, -1, 1)$
 $(-1, -1/3, -2/3, -1/3)$
 $(1/5, 2/5, -1/5, -3/5)$

10. $y = 2x + 2$

is obtained from:

$$\begin{pmatrix} \frac{5}{6} & -\frac{1}{6} & \frac{1}{3} \\ \frac{1}{2} & -\frac{1}{2} & 0 \end{pmatrix} \begin{pmatrix} 2 \\ -2 \\ 0 \end{pmatrix}$$

11. $y = -\frac{13}{14}x - \frac{2}{7}$

is obtained from:

$$\begin{pmatrix} \frac{4}{7} & \frac{1}{7} & \frac{2}{7} \\ \frac{5}{14} & -\frac{2}{7} & -\frac{1}{14} \end{pmatrix} \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}$$

Determinants 6

Permutation Arithmetic

6.1

6.1.1 Pictures of Permutations	566
6.1.2 Composition of Permutations	569
6.1.3 Even and Odd Permutations	570
6.1.4 Symmetric Groups: Half Even, Half Odd	575
6.1.5 Exercises	579
6.1.6 Solutions	581

Questions to Guide Your Study:

- *What is a permutation? What is S_n and S_A ?*
- *How can we picture composition between permutations?*
- *What are even and odd permutations?*
- *How can we determine if a permutation is even or odd?*
- *How many even and odd permutations are there in S_n ?*

Anything that deals with symmetries can be tracked back to permutations and compositions. We will be using symmetries to study something very important in linear algebra: *determinants*.

6.1.1 Pictures of Permutations

Permutation

A permutation is a *self*-bijection. That is, given a set A , a permutation f is a bijective function $f : A \rightarrow A$.

For instance, the set A could be $\{1, 2, 3, 4, 5\}$. Let's symbolically write the collection of all permutations on the set A as S_A .

S_A

The collection of all permutations (self-bijections) $A \rightarrow A$ is notated as S_A .

We will call S_A the

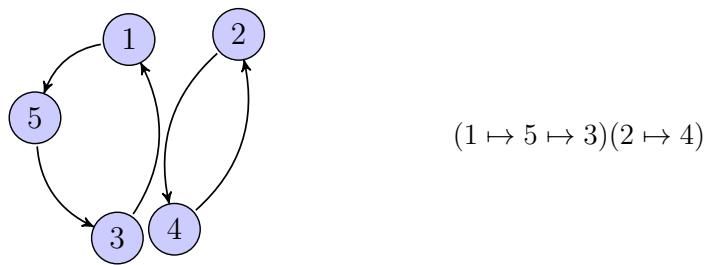
“Symmetries on A ”

We call a bijection (permutation) $A \rightarrow A$ a *symmetry* of A : we have simply relabeled A , keeping everything in A and not moving anything out or anything in.

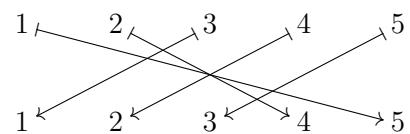
In the purest form, this is what *symmetry* means. When you reflect something about one of its lines of symmetry, you expect *no change* to what you see. Likewise, a set A stays the same after a permutation (bijection).

There are different ways of representing a permutation. All of the following depictions represent *the same* permutation:

x	$f(x)$
1	5
2	4
3	1
4	2
5	3



$$(1\ 5\ 3)(2\ 4)$$



Different pictures of the same thing help us understand different things about it. The notation $(1\ 5\ 3)(2\ 4)$ is easy to write in text. Therefore, you may see it often as we keep going. It is called *cycle notation* because it shows “assignment cycles.”

Cycle Notation

A permutation f of a finite set like $\{1, 2, 3, 4, 5, 6\}$ can be described by “assignment cycles” such as

$$(1 \mapsto 2 \mapsto 4 \mapsto 1)(3 \mapsto 5 \mapsto 3)$$

With these cycles, we know precisely how f behaves. For instance, $f(5) = 3$ and $f(2) = 4$. We also know that $f(6) = 6$ because 6 had no assignment arrow. If no assignment arrow is listed for an element, we assume that the function just sends that element to itself. The shorthand for writing out these assignment cycles is:

$$(1\ 2\ 4)(3\ 5)$$

where we understand that at the right end of the parentheses grouping, the assignment wraps around back to the front so $4 \mapsto 1$ and $5 \mapsto 3$. This shorthand notation is called *cycle notation*.

Fixed Point of a Permutation

A point is fixed in a permutation if the permutation leaves it alone; it just sends it to itself.

Disjoint cycle notation

If each assignment given in each cycle matches the function definition itself, we say that the function is written in *disjoint cycle notation*. That is, since 3 only appears in one of the cycles: (3 5), 2 only appears in (1 2 4), 1 only appears in (1 2 4), 4 only appears in (1 2 4) and 5 only appears in (3 5), the cycles are *disjoint*.

n-cycle

The cycle (1 2 4) is called a 3-cycle since it discusses 3 assignments. Likewise, (3 5) is called a 2-cycle with 2 assignments. A cycle $(a_1 a_2 \dots a_n)$ is called a *n*-cycle.

Non-disjoint cycle notation

Cycle notation that is not in disjoint notation. For instance $(1 3)(3 5 4)$ is not in disjoint cycle notation because both cycles share a 3. We think of it as a *composition* of two cycle functions: $(1 3) \circ (3 5 4)$

The permutation $(1 2 3)(3 5)$ can also be written in *non-disjoint* cycle notation:

$$\underbrace{(1 3)(1 2)(3 5)}_r = \underbrace{(1 3)}_f \circ \underbrace{(1 2)}_g \circ \underbrace{(3 5)}_h$$

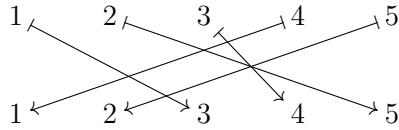
We first run h , then g , then f as we normally do with function composition. For instance, let's compute

$$r(2) = (f \circ g \circ h)(2).$$

First, notice that $h(2) = 2$ since 2 is a fixed point of the cycle (3 5). That is, the cycle (3 5) does nothing to 2 so it leaves it alone. So we have: $r(2) = (f \circ g)(2)$. Next, we put 2 into g which sends it to 1. Thus, $r(2) = f(1) = 3$ since f sends 1 to 3.

Example 1. Let's rewrite the permutation $(4 2 3)(1 2 3)(4 5)(3 2 4)$ in disjoint cycle notation. First, we write

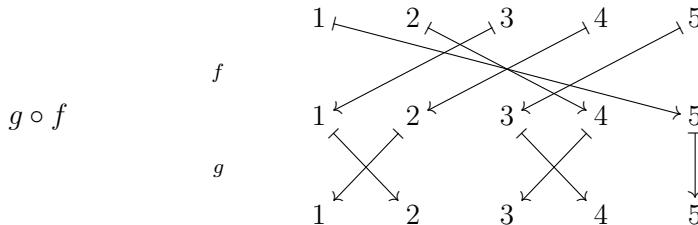
the permutation as $j = \underbrace{(4\ 2\ 3)}_f \underbrace{(1\ 2\ 3)}_g \underbrace{(4\ 5)}_h \underbrace{(3\ 2\ 4)}_r$. Now we build a function table or a diagram of assignment arrows for j . We compute $j(1) = f \circ g \circ h \circ r(1)$. Notice that r leaves 1 fixed. So this is $f \circ g \circ h(1)$. Then h also leaves 1 fixed so this is $f \circ g(1)$. Then g takes 1 to 2. So this is $f(2)$. Then f takes 2 to 3 so that the final result for $j(1)$ is 3. Therefore $1 \mapsto 3$ is an assignment arrow for j . Continuing this way, we find all assignment arrows for j and write them out:



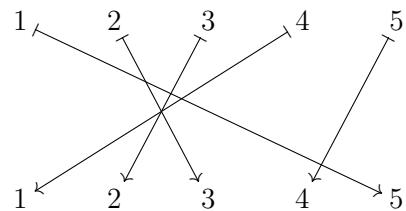
We find the following two assignment paths: $1 \mapsto 3 \mapsto 4 \mapsto 1$ and $3 \mapsto 5 \mapsto 3$. Hence, the disjoint cycle notation is: $(1\ 3\ 4)(2\ 5)$.

6.1.2 Composition of Permutations

We can run one permutation after another to create a new permutation based off of the original two. This new permutation *depends* on how we *order* the two permutations. For instance, consider two permutations f and g . Consider g after f :



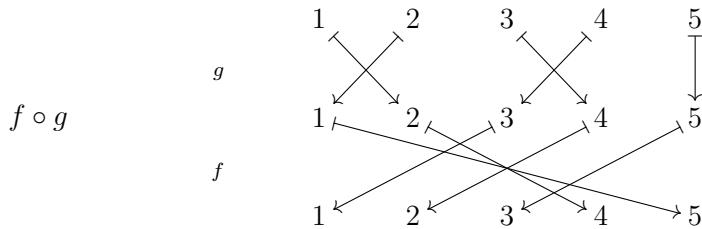
Combine paths of two arrows into one \mapsto :



Now, write the new cycle notation for $g \circ f$:

$$(1\ 5\ 4)(3\ 2)$$

Similarly, now consider f after g :



The new cycle notation for $f \circ g$ is

$$(1\ 4)(2\ 5\ 3)$$

Notice that the two new permutations $f \circ g$ and $g \circ f$ have different *disjoint* cycles completely and so therefore are completely different permutations. We see that

$$f \circ g \neq g \circ f$$

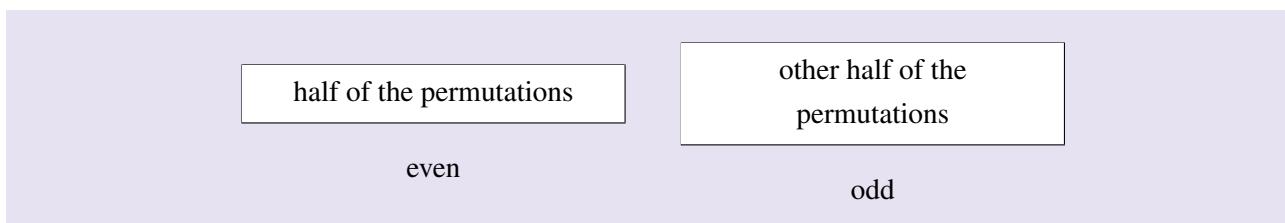
The operation \circ is *not commutative*. Many operations *are* commutative like addition $3 + 2 = 2 + 3$ or multiplication $3 \cdot 2 = 2 \cdot 3$. But composition \circ is not.

6.1.3 Even and Odd Permutations

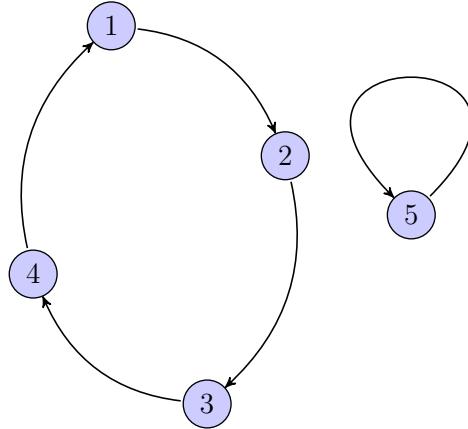
Take a set A and think of the collection S_A of permutations (symmetries) on that set. As we study symmetries (permutations among rows or columns) on a matrix, it will help us to categorize them so that there is a nice arithmetic between the categories themselves! But first, we need to form groupings—that is, *make a fiber box diagram that splits up S_A into chunks*. Any time that we make distinct groupings of things, *we are making a fiber box diagram!* We decide what the fibers of the function should be. Each fiber will represent a type of symmetry (permutation). We would like there to be two types which we will call *even permutations* and *odd permutations*. We will discuss what we mean by “odd” and “even” soon. But for now, just think of them as *names* of two different types of permutations. There will be a composition arithmetic right on these two types of symmetries given by:

\circ	even	odd
even	even	odd
odd	odd	even

That is, an even permutation composed with an even permutation should be even. An odd permutation composed with an even permutation should be odd. An odd permutation composed with an odd permutation should be even. Let $P = \{\text{even, odd}\}$ be the codomain so that our fiber box diagram for this function $f : S_A \rightarrow P$ should look like:

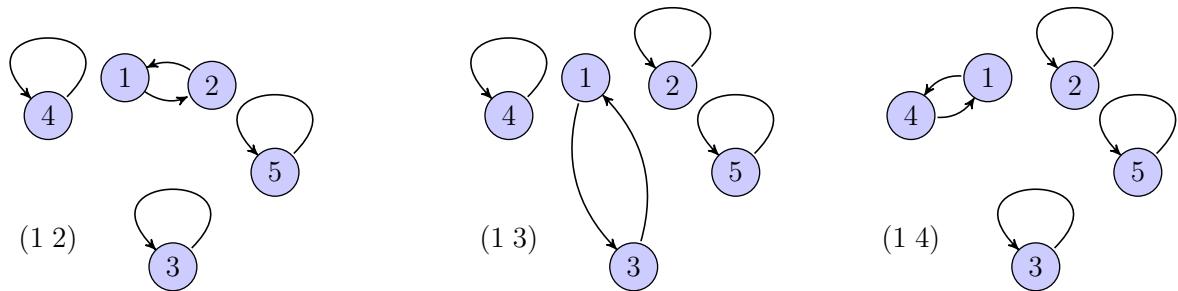


Now we will begin a discussion of how we should determine what we mean by an “even” or an “odd” type of permutation. We think about breaking up a permutation into a sequence of switches. We will write S_n to mean S_A where $A = \{1, 2, 3, \dots, n\}$. This will enable us to easily identify where our permutations come from in cycle notation. For instance,



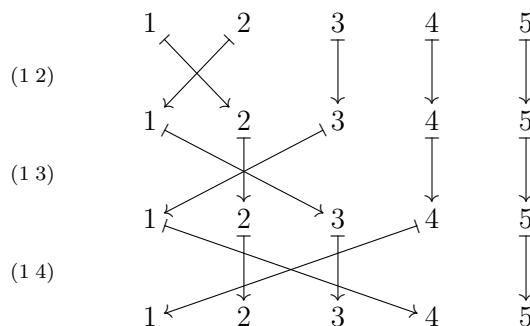
represents a permutation in S_5 . Its cycle notation can be written either as $(1 2 3 4)(5)$ or just $(1 2 3 4)$. It is customary just to omit single vertex loops. Such an omitted vertex is called a *fixed point* of the permutation.

Let’s investigate how we might represent $(1 2 3 4)$ in terms of switches. Let’s consider the three different switches shown below. Imagine following one after the other:

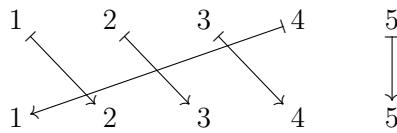


The result of taking these assignment cycles in order can be seen from stacking:

$$(1 4) \circ (1 3) \circ (1 2)$$



The composition of these three cycles is:



which in cycle notation is simply: $(1\ 2\ 3\ 4)$. Just like *this* cycle is the composition of 2-cycles (simple switches), we can decompose *any* cycle into a composition of 2-cycles. We will call these simple switch 2-cycle permutations *transpositions*.

Transpositions

A transposition is a 2-cycle like $(3\ 5)$ or $(1\ 4)$.

Thus, we say that $(1\ 2\ 3\ 4)$ can be decomposed into a composition of three transpositions: first apply $(1\ 2)$, then $(1\ 3)$ and last $(1\ 4)$. But composition order is backwards: right first and then left next:

$$(1\ 4) \circ (1\ 3) \circ (1\ 2)$$

Yet for simplicity, we often omit the composition operation \circ and just write:

$$(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$$

Similarly,

$$(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$$

This tells us that a 5-cycle (a cycle with 5 vertices) can be made up of 4 switches.

Theorem 6.1.1 Decomposing Cycles into Transpositions

The cycle $(a_1\ a_2\ \dots\ a_n)$ of length n decomposes into the following composition of $n - 1$ transpositions:

$$(a_1\ a_n) \circ (a_1\ a_{n-1}) \circ \dots \circ (a_1\ a_2)$$

Example 2. $(1\ 2\ 4\ 6)(3\ 5\ 7) = (1\ 6) \circ (1\ 4) \circ (1\ 2) \circ (3\ 7) \circ (3\ 5)$.

Just considering whether the number of transpositions that occur in such a sequencing is even or odd seems like a good way of determining whether a permutation should be “odd” or “even.” This is because composing

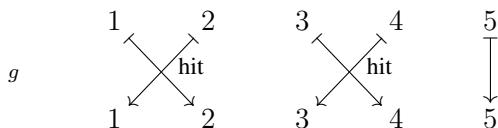
simply means running one sequence of transpositions and then the other. Effectively, *composition* then relates to *adding numbers of transpositions*. This is good because:

- odd numbers plus odd numbers are even
- even numbers plus odd numbers are odd
- even numbers plus even numbers are even

This is just what we desire! Yet one question remains:

Is there a way of decomposing the same permutation into two different sequences of transpositions so that one sequence has an odd number of transpositions and the other has an even number of transpositions?

We provide some closure to this worry and show that it will never happen. Let's take a look at a permutation g :



We see that there are two crossings or “hits” between the assignment arrows. This number of hits or crossings is well-defined for a specific permutation *that is not depicted as a stacked composition as long as we order the domain A the same way as the codomain A every time* and as long as we have a *sound definition* for crossing: *every time two arrows cross*. Let's temporarily change our method of grouping our permutations to the following two groupings:

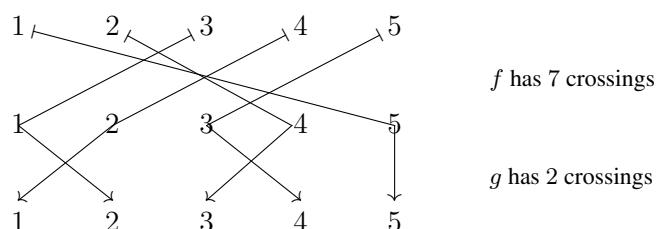
- All permutations that have an *even* number of crossings.
- All permutations that have an *odd* number of crossings.

Parity

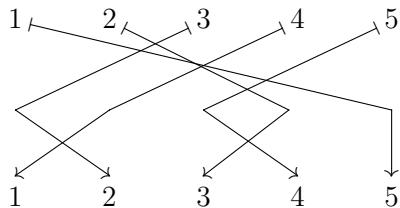
The parity of an integer is its quality of being even or odd. If an integer is even, we say it has an even parity. If it is odd, we say that it has an odd parity. The answer to the question “*what is the parity of 5?*” is “*odd*.”

Before we proceed further, let's just experiment with how composition \circ and number of crossings might interact. For instance, let's look at a composition $g \circ f$:

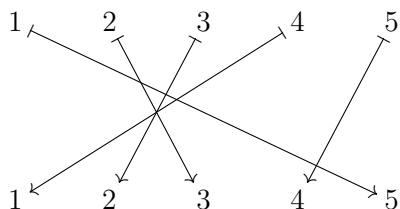
Count crossings for each function and add.
The result is 9



Drop Middles

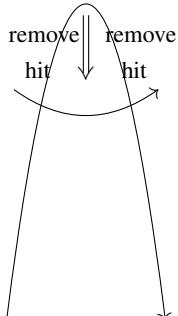


Straighten out and
recount. $g \circ f$ has 7
crossings.



Notice that the sum of the crossings of f and g is odd as in the number of crossings of $g \circ f$. The reason for this lies in the *straightening out*:

Each hump moves through another line to straighten. The number of crossings changes by 2.



Adding by 2's does not change whether a number is even or odd. In particular, every time we run one transposition we introduce exactly one crossing. This tells us that the parity of the number of crossing is the same in any stacked composition diagram of assignment arrows! This includes a sequence of transpositions! One crossing for one transposition. We can safely determine our two categories according to the number of composed transpositions. We can also be sure that the number of transpositions in all switch sequences describing the same permutation all have the same parity.

Theorem 6.1.2 Constant Parity

Given a permutation on a finite set, no matter how we write it down as a sequence of composed transpositions, the number of transpositions always will have the same parity.

We can with confidence make two well-defined definitions:

Even Permutation

A permutation that can be described as a sequence of an even number of composed transpositions.

Odd Permutation

A permutation that can be described as a sequence of an odd number of composed transpositions.

Theorem 6.1.3 Method for Determining if a Permutation is Odd or Even

Suppose that a permutation is written in cycle notation. *It does not matter* whether the notation is disjoint or nondisjoint. Then compute:

$$(\text{Sum of cycle lengths}) - (\text{number of cycles})$$

If this number is odd, the permutation is odd. If it is even, the permutation is even.

Proof. A n -cycle can be decomposed into $n - 1$ transpositions. Hence if the cycles in the permutation are written as:

$$(n_1\text{-cycle})(n_2\text{-cycle}) \cdots (n_r\text{-cycle})$$

then there are $(n_1 - 1) + (n_2 - 1) + \cdots + (n_r - 1)$ transpositions making up the permutation. This is $n_1 + n_2 + \cdots + \underbrace{n_r - 1}_{-r} - 1 - \cdots - 1 = (n_1 + n_2 + \cdots + n_r) - (r)$ transpositions. The parity of this number determines whether the permutation is even or odd. \square

Example 3. Consider the permutation $(1\ 4\ 6\ 7)(2\ 4\ 3)$. The cycle $(1\ 4\ 6\ 7)$ has length 4 which can be decomposed into 3 transpositions and the cycle $(2\ 4\ 3)$ has length 3 so that it can be decomposed into 2 transpositions. Hence, the permutation can be decomposed into $3 + 2 = 5$ transpositions. This is $(\text{sum of cycle lengths}) - (\text{number of cycles}) = 4 + 3 - 2 = 5$. Since 5 is odd, the permutation itself is odd.

6.1.4 Symmetric Groups: Half Even, Half Odd

The collection S_A with the composition operations \circ is a group. The identity element id which is just simply the “do nothing function” described by $x \mapsto x$. Nothing is changed or rearranged. Composition naturally is associative and running two permutations one after another is again a permutation so that the operation \circ is closed on S_A .

The only thing left to check is to see if has inverses. This is clear since a bijection always has a function inverse: *just reverse all of the assignment arrows*. For instance:

$$(1\ 2\ 3\ 4)^{-1} = (4\ 3\ 2\ 1) \\ (1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 1)^{-1} \quad (1 \leftarrow 2 \leftarrow 3 \leftarrow 4 \leftarrow 1)$$

Symmetric Group

The symmetric group on a set A of n objects is denoted as S_A or S_n . It is the collection of all permutations on the set A .

Because we know that S_A is a group, we can quickly see that the number of even permutations will be exactly the same as the number of odd permutations. For instance, let E be the collection of all of the even permutations and let O be the collection of all of the odd permutations. Then, choose one odd permutation $g \in O$. Notice that $x \mapsto x \circ g$ is a function $F : E \rightarrow O$ since if x is an even permutation and we compose it with the odd permutation g to make $x \circ g$, the result is an odd permutation. Thus the rule $x \mapsto x \circ g$ tells us how to go from E into O . Now, g has a permutation inverse since S_A is a group. Call it g^{-1} . Notice that a sequence of transpositions that makes g just has to be put in reverse order to get one for g^{-1} . *We have not changed the number of transpositions!* Therefore, g^{-1} is an odd permutation as well.

Now notice that $y \mapsto y \circ g^{-1}$ defines a function $G : O \rightarrow E$ since if y is an odd permutation, $y \circ g^{-1}$ (an odd permutation composed with an odd permutation) will then be an even permutation. Most importantly, realize that: $G \circ F(x) = G(x \circ g) = x \circ g \circ g^{-1} = x$ so that $G \circ F = \text{id}_E$. Similarly, $F \circ G = \text{id}_O$. This tells us that F and G are function inverses to each other which implies they are both bijections between E and O . Hence, the sizes of the two sets $|O|$ and $|E|$ are the same:

$$|O| = |E|$$

Theorem 6.1.4 Number of Permutations

There are $n!$ permutations in S_n half of which are even and half of which are odd.

Proof. The discussion above tells us that there are precisely the same number of even permutations as odd permutations. Now, why are there $n! = n \cdot (n - 1) \cdots 3 \cdot 2 \cdot 1$ permutations in S_n ? Think of a permutation on S_A where $A = \{1, 2, \dots, n\}$. For every n things f can send 1 to, there are $n - 1$ things that it can send 2 to. Now for each of the ways there are of sending 1 and 2 to something (which is $(n)(n - 1)$), there are $n - 2$ things we could send 3 to and so on. Continuing this process, we see that the number of ways of creating a bijection $f : A \rightarrow A$ is precisely $n!$. \square

Example 4. Let's list out the even and odd permutations of S_3 . The size of S_3 denoted as $|S_3|$ is $3! = 3 \cdot 2 \cdot 1 = 6$. So there should be 3 even permutations and 3 odd permutations.

- Even permutations: $(1\ 2\ 3)$, $(1\ 3\ 2)$, id
- Odd permutations: $(1\ 2)$, $(1\ 3)$, $(2\ 3)$

Key Concepts from this Section

- **permutation:** (page 566) A permutation is a *self*-bijection. That is, given a set A , a permutation f is a bijective function $f : A \rightarrow A$.
- S_A : (page 566) The collection of all permutations (self-bijections) $A \rightarrow A$ is denoted as S_A .
- **cycle notation:** (page 567) A permutation f of a finite set like $\{1, 2, 3, 4, 5, 6\}$ can be described by “assignment cycles” such as

$$(1 \mapsto 2 \mapsto 4 \mapsto 1)(3 \mapsto 5 \mapsto 3)$$

With these cycles, we know precisely how f behaves. For instance, $f(5) = 3$ and $f(2) = 4$. We also know that $f(6) = 6$ because 6 had no assignment arrow. If no assignment arrow is listed for an element, we assume that the function just sends that element to itself. The shorthand for writing out these assignment cycles is:

$$(1\ 2\ 4)(3\ 5)$$

where we understand that at the right end of the parentheses grouping, the assignment wraps around back to the front so $4 \mapsto 1$ and $5 \mapsto 3$. This shorthand notation is called *cycle notation*.

- **fixed point of a permutation:** (page 568) A point is fixed in a permutation if the permutation leaves it alone; it just sends it to itself.
- **disjoint cycle notation:** (page 568) If each assignment given in each cycle matches the function definition itself, we say that the function is written in *disjoint cycle notation*. That is, since 3 only appears in one of the cycles: $(3\ 5)$, 2 only appears in $(1\ 2\ 4)$, 1 only appears in $(1\ 2\ 4)$, 4 only appears in $(1\ 2\ 4)$ and 5 only appears in $(3\ 5)$, the cycles are *disjoint*.
- **n -cycle:** (page 568) The cycle $(1\ 2\ 4)$ is called a 3-cycle since it discusses 3 assignments. Likewise, $(3\ 5)$ is called a 2-cycle with 2 assignments. A cycle $(a_1\ a_2\ \dots\ a_n)$ is called a n -cycle.
- **non-disjoint cycle notation:** (page 568) Cycle notation that is not in disjoint notation. For instance $(1\ 3)(3\ 5\ 4)$ is not in disjoint cycle notation because both cycles share a 3. We think of it as a *composition* of two cycle functions: $(1\ 3) \circ (3\ 5\ 4)$
- **fixed point:** (page 571) A fixed point of a permutation $f : A \rightarrow A$ is an element $a \in A$ such that $f(a) = a$. That is, f fixes it. It is not a part of any assignment cycle that has another element other than a . In cycle notation, we can omit fixed points.
- **transpositions:** (page 572) A transposition is a 2-cycle like $(3\ 5)$ or $(1\ 4)$.
- **theorem 6.1.1 decomposing cycles into transpositions:** (page 572) The cycle $(a_1\ a_2\ \dots\ a_n)$ of length n decomposes into the following composition of $n - 1$ transpositions:

$$(a_1\ a_n) \circ (a_1\ a_{n-1}) \circ \dots \circ (a_1\ a_2)$$

- **parity:** (page 573) The parity of an integer is its quality of being even or odd. If an integer is even, we say it has an even parity. If it is odd, we say that it has an odd parity. The answer to the question “*what is the parity of 5?*” is “*odd*.”
- **theorem 6.1.2 constant parity:** (page 574) Given a permutation on a finite set, no matter how we write it down as a sequence of composed transpositions, the number of transpositions always will have the same parity.
- **even permutation:** (page 574) A permutation that can be described as a sequence of an even number of composed transpositions.
- **odd permutation:** (page 575) A permutation that can be described as a sequence of an odd number of composed transpositions.
- **theorem 6.1.3 method for determining if a permutation is odd or even:** (page 575) Suppose that a permutation is written in cycle notation. *It does not matter* whether the notation is disjoint or nondisjoint. Then compute:

$$(\text{Sum of cycle lengths}) - (\text{number of cycles})$$

If this number is odd, the permutation is odd. If it is even, the permutation is even.

- **symmetric group:** (page 575) The symmetric group on a set A of n objects is notated as S_A or S_n . It is the collection of all permutations on the set A .
- **theorem 6.1.4 number of permutations:** (page 576) There are $n!$ permutations in S_n half of which are even and half of which are odd.

6.1.5 Exercises

1. Rewrite the compositions below as a single permutation written in disjoint cycle notation:

- (a) $(1\ 3\ 2\ 4\ 5) \circ (2\ 5\ 3) \circ (3\ 4\ 5)$
- (b) $(1\ 5\ 3\ 4\ 2) \circ (1\ 5\ 4) \circ (1\ 5)(2\ 3\ 4)$
- (c) $(1\ 5\ 4\ 3\ 2) \circ (2\ 3\ 5) \circ (1\ 3\ 4\ 2\ 5)$
- (d) $(1\ 5) \circ (1\ 5\ 4\ 2)$
- (e) $(1\ 5\ 2) \circ (1\ 3\ 5)(2\ 4) \circ (1\ 3)(2\ 5)$
- (f) $(1\ 4)(2\ 5\ 3) \circ (1\ 4)(2\ 3) \circ (1\ 4\ 3)(2\ 5)$
- (g) $(1\ 2\ 4\ 3) \circ (1\ 4\ 3\ 2\ 5) \circ (1\ 3)(2\ 5\ 4)$
- (h) $(1\ 3\ 2\ 4\ 5) \circ (1\ 2)(3\ 4\ 5) \circ (1\ 5)(2\ 3\ 4)$
- (i) $(1\ 5\ 3)(2\ 4) \circ (1\ 5\ 2)(3\ 4) \circ (1\ 3\ 5\ 4)$
- (j) $(1\ 5\ 4) \circ (1\ 4) \circ (1\ 2)$

2. Determine if the following permutations are even or odd. Remember that one can decompose any cycle into transpositions via a procedure like $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$.

- (a) $(1\ 2\ 7\ 9\ 4\ 6\ 10\ 5)$
- (b) $(1\ 4\ 7\ 3\ 5\ 9\ 6)(2\ 8)$
- (c) $(1\ 4\ 3\ 8)(2\ 7\ 6)(5\ 9\ 10)$
- (d) $(1\ 8\ 4)(2\ 5\ 7\ 6\ 9\ 10)$
- (e) $(1\ 8\ 5)(2\ 7\ 3)(4\ 9\ 10)$
- (f) $(1\ 2\ 9\ 8\ 6\ 10)(3\ 7\ 5\ 4)$
- (g) $(1\ 10\ 9\ 8\ 6\ 5\ 2\ 3)$
- (h) $(2\ 4\ 3\ 7)(5\ 10\ 6\ 8\ 9)$
- (i) $(1\ 4)(2\ 3\ 10\ 5\ 9\ 8\ 6\ 7)$
- (j) $(1\ 6\ 10\ 7\ 8\ 5)(3\ 9)$

3. Consider the two configurations of a tile puzzle:

	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

	1	2	3
4	5	6	7
8	9	10	15
12	13	14	11

The black square denotes a blank space into which a tile can move either horizontally or vertically. Is it possible to make tile moves to change the first configuration into the second?

4. Consider the two configurations of a tile puzzle:

	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

1		2	3
4	5	6	7
9	8	10	12
11	13	15	14

The black square denotes a blank space into which a tile can move either horizontally or vertically. Is it possible to make tile moves to change the first configuration into the second?

5. Verify that:

$$(2 \ 3 \ 4) = (1 \ 2)(1 \ 4)(1 \ 3)(1 \ 2)$$

Notice that we can write $(2 \ 3 \ 4)$ completely in terms of switches with 1 which is not in the cycle $(2 \ 3 \ 4)$ at all. Let's now change the tile game of the last couple exercises. Suppose that in each move we can actually lift a tile up off the board from anywhere and put it down into the blank spot. Then is it possible to achieve *any* configuration? Why or why not? Explain and prove your answer.

6.1.6 Solutions

1. Solutions/hints by part:

(a) $(1 \ 3 \ 5 \ 4 \ 2)$

(e) $(1 \ 2 \ 5 \ 4)$

(i) $(1 \ 2 \ 5)(3 \ 4)$

(b) $(1 \ 2 \ 4)(3 \ 5)$

(f) $(1 \ 4 \ 5 \ 2 \ 3)$

(j) $(1 \ 2)(4 \ 5)$

(c) $(1 \ 4 \ 2)$

(g) $(1 \ 4 \ 5)$

(d) $(2 \ 5 \ 4)$

(h) $(1 \ 2 \ 5 \ 4 \ 3)$

2. Solutions/hints by part:

(a) odd

(e) even

(i) even

(b) odd

(f) even

(j) even

(c) odd

(g) odd

(d) odd

(h) odd

3. It takes an odd permutation to make the change. But to move the blank around the board back to its original position is an even permutation. Even and Odd permutations are in separate chunks of a partition. Therefore, there is no overlap and this cannot be.

4. The answer is the very same as for the last exercise.

5. If every permutation can be broken down into switches with just one thing, let that one thing be the blank space. So yes!

Determinants via Permutations and Sliding

6.2

6.2.1 Partitioning the Permutations with an Example	589
6.2.2 Generalizing to other Permutation Partitions	595
6.2.3 Using Cosets of Smaller Subgroups	597
6.2.4 Airdropping and Cofactor Techniques	602
6.2.5 Matrix Multiplication and Determinants	603
6.2.6 Diagonal Blocks and Determinants	607
6.2.7 Exercises	612
6.2.8 Solutions	618

Questions to Guide Your Study:

- *What is a determinant and what does it tell us about a matrix?*
- *What are some different ways of thinking about what a determinant is?*
- *What are some kitty-corner techniques for computing determinants?*
- *What are cofactors and how do they help compute determinants?*
- *How does airdropping help us compute determinants?*
- *What are some simple matrices to take determinants of?*
- *How do matrix multiplication, inverses and change of basis affect a determinant?*

How do you find the volume of an n -dimensional box? You just multiply all the side lengths together. There is a certain type of matrix which depicts an n -dimensional box:

Diagonal Matrix

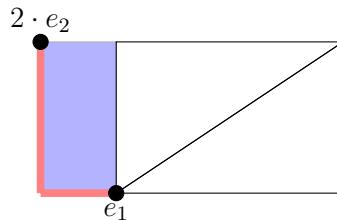
A diagonal matrix is one in which all the entries outside the diagonal from top left to bottom right are zeros:

$$\begin{pmatrix} * & & 0's \\ & \ddots & \\ 0's & & * \end{pmatrix}$$

Think about the column vectors that appear in a diagonal matrix. They are simply multiples of standard basis vectors: $a_1e_1, a_2e_2, \dots, a_ne_n$. If one corner of the box is at the origin, these column vectors then depict the sides of an n -dimensional box. To compute the volume of such a box we would just multiply the lengths together: $a_1 \cdot a_2 \cdots a_n$. This is the same as multiplying down the diagonal of a matrix. We call the volume of this box the *determinant* of the matrix. This notion of determinant will extend to matrices other than diagonal ones. In order to explore this, we want to consider the changes we can make to the sides of the box and still maintain the same volume. Let's first look at an example with 2-dimensional volume—otherwise known as *area*. Our 2-dimensional box is simply a rectangle. Suppose our matrix is

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

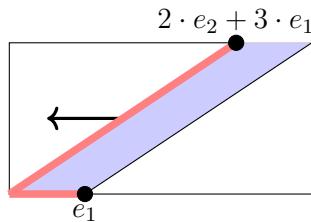
and consider the rectangle whose side lengths are given by the columns $e_1 = (1, 0)$ and $2 \cdot e_2 = (0, 2)$ where the corner of the rectangle is placed in the origin:



Consider a simple *column* airdrop:

$$\begin{pmatrix} (3 \cdot 1) & 0 \\ 1 & (3 \cdot 0) \\ 0 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$$

This operation has a very nice visualization as a *sliding*:



Visually, the shaded areas in both pictures *are identical!* We would say that the two matrices represent *the same oriented area*. We can compute this area more easily from the first picture as $2 \cdot 1$.

The columns of an $n \times n$ matrix represent sides of a n -dimensional parallelogram. We would like to create an idea that could serve as n -dimensional area or volume. This idea we will call the *determinant* of the matrix. To create this idea, we extend basic principles that we notice in 2 and 3 dimensions:

- The determinant of a diagonal matrix should just be the product of the diagonal entries. (volume of an n -dimensional box)
- Column airdropping should not change the determinant. (Column airdropping is like *sliding*)

Also, we use the idea that column airdropping is sufficient to turn a matrix into a diagonal one:

Theorem 6.2.1 Airdrop to Diagonal

Column airdropping is enough to turn any square matrix with entries in a field into a diagonal matrix.

Proof. Since the entries of the matrix are in a field, we can always multiply one nonzero entry by something that would cancel with any other entry in its same row. Start in the first row and identify an entry that is nonzero. If all entries in the first row are zero, go to the second row. Otherwise, column airdrop a multiple of this nonzero entry so that there is a nonzero entry in the first column first row position. Then, use that entry to column airdrop to every other entry in this first row to make them 0.

Next, proceed to the second row and repeat this idea except that our goal is to get a nonzero entry in the second column second row position via column airdropping. Then we use that nonzero entry to make all other entries in this row zero via more column airdrops. The only time this would not be possible is when the row is all zeros—which is fine as we progress toward our goal of having a diagonal matrix.

We perform analogous steps at each row until we end with a diagonal matrix. □

Corollary 6.2.2 Squares come from Diagonals

Every square matrix is the result of column airdrops to a diagonal matrix.

This tells us that the determinant of a $n \times n$ matrix should be defined as what we get by sliding the sides of the n -dimensional parallelogram into a rectangular box and then just multiplying the lengths of the sides

together. Yet we would like to have a description of a determinant *without airdropping* and just by thinking of computations from the matrix entries themselves.

We are going to use symmetries of the matrix to help. In particular, we look at all of the permutations of the columns. Whatever computation we choose must:

- give the determinant of a diagonal matrix as the product of the diagonal entries.
- must remain unchanged with column airdrops.
- give a 0 determinant for a matrix with repeated columns. (We should get 0 n -dimensional volume if we only have $n - 1$ sides).

Let's consider a diagonal matrix. If we permute its columns in any way that is not the identity permutation, notice that the product down the diagonal becomes 0:

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

Now suppose that we have a matrix with a repeated column. We would like the determinant to be 0. In the example below, we consider all permutations of S_3 that permute the columns:

Even $\begin{pmatrix} 1 & 2 & 1 \\ 3 & 1 & 3 \\ 2 & 4 & 2 \end{pmatrix}$ id	Even $\begin{pmatrix} 1 & 1 & 2 \\ 3 & 3 & 1 \\ 2 & 2 & 4 \end{pmatrix}$ (1 2 3)	Even $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 3 \\ 4 & 2 & 2 \end{pmatrix}$ (1 3 2)
Odd $\begin{pmatrix} 1 & 2 & 1 \\ 3 & 1 & 3 \\ 2 & 4 & 2 \end{pmatrix}$ (1 2)	Odd $\begin{pmatrix} 1 & 1 & 2 \\ 3 & 3 & 1 \\ 2 & 2 & 4 \end{pmatrix}$ (2 3)	Odd $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 3 \\ 4 & 2 & 2 \end{pmatrix}$ (1 3)

Notice that the even permutations give the same diagonals as the odd permutations. Why not take the determinant as the sum of products of the diagonals from even permutations minus the sum of products of the odd diagonals? That would guarantee that the determinant of this matrix would be 0. Further, the determinant of a diagonal matrix would still be just the product of diagonal entries because all non-identity permutations put 0's in their diagonals. *We are off to a good start!*

Permuted Diagonal Product

Given a matrix, permute its columns or its rows and then take the product of the entries that appear in the diagonal from the top left to the bottom right. This product is a permuted diagonal product.

Yet now we need to check that such an idea behaves well with column airdropping. Consider the following example:

$$\left(\begin{array}{ccc} 1 & 3 \cdot 1 & -2 \\ 3 & 3 \cdot 3 & 3 \\ 2 & 3 \cdot 2 & 1 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 1 & 3 \cdot 1 + 2 & -2 \\ 3 & 3 \cdot 3 + 1 & 3 \\ 2 & 3 \cdot 2 + 4 & 1 \end{array} \right)$$

Using the distributive property, down each permuted diagonal we get two products as illustrated:

$$+ \left(\begin{array}{ccc} 1 & 3 \cdot 1 + 2 & -2 \\ 3 & 3 \cdot 3 + 1 & 3 \\ 2 & 3 \cdot 2 + 4 & 1 \end{array} \right) + \left(\begin{array}{ccc} -2 & 1 & 3 \cdot 1 + 2 \\ 3 & 3 & 3 \cdot 3 + 1 \\ 1 & 2 & 3 \cdot 2 + 4 \end{array} \right) + \left(\begin{array}{ccc} 3 \cdot 1 + 2 & -2 & 1 \\ 3 \cdot 3 + 1 & 3 & 3 \\ 3 \cdot 2 + 4 & 1 & 2 \end{array} \right)$$

$$- \left(\begin{array}{ccc} 1 & -2 & 3 \cdot 1 + 2 \\ 3 & 3 & 3 \cdot 3 + 1 \\ 2 & 1 & 3 \cdot 2 + 4 \end{array} \right) - \left(\begin{array}{ccc} -2 & 3 \cdot 1 + 2 & 1 \\ 3 & 3 \cdot 3 + 1 & 3 \\ 1 & 3 \cdot 2 + 4 & 2 \end{array} \right) - \left(\begin{array}{ccc} 3 \cdot 1 + 2 & 1 & -2 \\ 3 \cdot 3 + 1 & 3 & 3 \\ 3 \cdot 2 + 4 & 2 & 1 \end{array} \right)$$

So, assuming that the determinant (\det) is calculated as we propose, our calculation so far amounts to:

$$\det \underbrace{\left(\begin{array}{ccc} 1 & 2 & -2 \\ 3 & 1 & 3 \\ 2 & 4 & 1 \end{array} \right)}_A + \det \underbrace{\left(\begin{array}{ccc} 1 & 3 \cdot 1 & -2 \\ 3 & 3 \cdot 3 & 3 \\ 2 & 3 \cdot 2 & 1 \end{array} \right)}_B$$

Notice that all of the permuted diagonal products of B are just 3 multiplied to the permuted diagonal products of a matrix with a repeated column:

$$\left(\begin{array}{ccc} 1 & 1 & -2 \\ 3 & 3 & 3 \\ 2 & 2 & 1 \end{array} \right)$$

This repeated column matrix has determinant 0 so that $\det B = 0$. Therefore, the determinant of the airdropped

matrix is the same as $\det A$. That is, the determinant *has not changed!* This is really good. Calculating the determinant as a sum of signed permuted diagonal products coincides perfectly with the following:

- The determinant should not change with airdrops.
- The determinant of a diagonal matrix is just the product of its one nonzero diagonal.
- The determinant of a matrix with a repeated column is 0.

In fact, such criteria uniquely define the determinant! This tells us that we have actually found an accurate formula—and it came from studying the symmetries of a matrix!

Determinant of a Matrix

Suppose that the columns of a $n \times n$ matrix A are listed as c_1, c_2, \dots, c_n . Let $\tau \in S_n$ and note the matrix given by permuting the columns according to τ by A_τ . Further, let $\text{diag } A_\tau$ be the product down the diagonal of A_τ from top left to bottom right. Then we define the determinant (\det) of A as follows:

$$\det A = \sum_{\tau \text{ even}} \text{diag } A_\tau - \sum_{\tau \text{ odd}} \text{diag } A_\tau$$

Theorem 6.2.3 Permutations of Rows or Columns

We get the exact same even and odd diagonal products if we permute the rows or if we permute the columns.

Corollary 6.2.4 Determinant of Transpose

$$\det(A^T) = \det(A)$$

Corollary 6.2.5 Column or Row Airdrops

The n -dimensional volume of the parallelogram formed by the rows is the same as the one formed by the columns. We can “slide” to a diagonal matrix by row airdrops or column airdrops or a mixture of both and obtain the same determinant.

Example 1. Consider the matrix

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

We find the determinant by doing row and column airdrops:

$$\begin{array}{ccc} \left(\begin{array}{ccc|c} 1 & 2 & 5 & \\ \hline 0 & -1 \cdot 1 & -1 \cdot 2 & -1 \cdot 5 \\ 1 & 1 & 1 & 3 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc|c} 1 & 2 & 5 & \\ \hline 0 & -2 \cdot 1 & -2 \cdot 0 & -2 \\ 0 & 0 & 1 & 0 \end{array} \right) \\ \xrightarrow{\quad} & & \left(\begin{array}{ccc|c} 1 & 0 & 0 & \\ \hline 0 & -5 \cdot 1 & -5 \cdot 0 & -5 \\ 0 & 1 & 1 & 1 \end{array} \right) \\ \xrightarrow{\quad} & & \left(\begin{array}{ccc|c} 1 & 0 & 0 & \\ \hline 0 & 0 & 0 & \\ 0 & 0 & -2 & \end{array} \right) \end{array}$$

The determinant of this matrix is clear—just the diagonal product:

$$\det(A) = 1 \cdot 1 \cdot (-2) = -2$$

At one point in this last example, we had an **upper triangular matrix** where every entry below the diagonal from upper left to lower right was 0. Column operations *easily* take us to a diagonal matrix *without changing the diagonal!* **Lower triangular matrices** work similarly.

Theorem 6.2.6 Determinants of Triangular Matrices

If a matrix is upper or lower triangular, the determinant is simply the product of the nonzero diagonal.

Example 2. The determinant of the following lower triangular matrix is $2 \cdot 5 \cdot (-1) \cdot 3 = -30$:

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

6.2.1 Partitioning the Permutations with an Example

Let's think about how many permuted diagonal products there are for square matrices. For a 2×2 there are only 2 since $|S_2| = 2! = 2$, for a 3×3 there are $6 = 3! = |S_3|$, for a 4×4 there are $24 = 4! = |S_4|$, and for a 5×5 , there are $120 = 5! = |S_5|$. *This is too many!* For computational efficiency, perhaps the fastest way to compute a determinant for large square matrices is to **slide to a diagonal** (i.e. *only* performing column or row airdrops until we have a diagonal matrix). Still, we can go even faster if we use a combination of sliding and *partitioning (or grouping) the permutations into determinants of smaller submatrices*.

Suppose that we have a 3×3 matrix. Let's choose a column of the matrix—say the first one. Each entry in this first column will be in a permuted diagonal at some point. We can split up the permutations into ones that will take certain entries to the diagonal. For instance, the permutations of S_3 can be split up according to which of them take a certain entry of this column to the diagonal. Label these collections of permutations P_1 , P_2 , and P_3 :

$P_1 :$

Permutations that send first column entry to diagonal

$P_2 :$

Permutations that send second column entry to diagonal

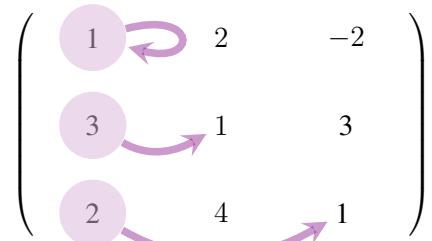
$P_3 :$

Permutations that send third column entry to diagonal

$$P_1 = \{\text{id}, (2\ 3)\}$$

$$P_2 = (1\ 2) \circ P_1 = \{(1\ 2) \circ \text{id}, (1\ 2) \circ (2\ 3)\} = \{(1\ 2), (1\ 2\ 3)\}$$

$$P_3 = (1\ 3\ 2) \circ P_1 = \{(1\ 3\ 2) \circ \text{id}, (1\ 3\ 2) \circ (2\ 3)\} = \{(1\ 3\ 2), (1\ 3)\}$$



Let's look at these subdivisions of permutations one by one.

P_1 permuted diagonals:

$$\begin{array}{c}
 + \\
 \left(\begin{array}{cc|cc}
 1 & & 2 & -2 \\
 & 3 & 1 & 3 \\
 & 2 & 4 & 1
 \end{array} \right) \\
 \text{id}
 \end{array}
 \quad
 \begin{array}{c}
 - \\
 \left(\begin{array}{cc|cc}
 1 & & -2 & 2 \\
 & 3 & 3 & 1 \\
 & 2 & 1 & 4
 \end{array} \right) \\
 (2\ 3)
 \end{array}$$

What we see are the diagonal products $+1 \cdot (1 \cdot 1)$ and $-1 \cdot (3 \cdot 4)$. Factor out the 1:

$$1 \cdot \left((1 \cdot 1) - (3 \cdot 4) \right) = 1 \cdot \det \begin{pmatrix} + & - \\ \cancel{1} & \cancel{3} \\ \cancel{4} & \cancel{1} \end{pmatrix}$$

We are multiplying the top entry “1” by the determinant which appears kitty-corner to “1” in the original matrix:

$$\left(\begin{array}{ccc|cc}
 1 & & & 2 & -2 \\
 & 3 & & & \\
 & 2 & & &
 \end{array} \right)$$

P_2 permuted diagonals:

The following are versions of our matrix when the columns have been permuted:

$$\begin{array}{c}
 - \\
 \left(\begin{array}{ccc|cc}
 2 & 1 & -2 & & \\
 \boxed{1} & \boxed{3} & 3 & & \\
 4 & 2 & 1 & &
 \end{array} \right) \\
 (1\ 2)
 \end{array}
 \quad
 \begin{array}{c}
 + \\
 \left(\begin{array}{ccc|cc}
 -2 & 1 & 2 & & \\
 3 & \boxed{3} & 1 & & \\
 1 & 2 & 4 & &
 \end{array} \right) \\
 (1\ 2\ 3)
 \end{array}$$

What we see are the diagonal products $-(2) \cdot 3 \cdot (1)$ and $(-2) \cdot 3 \cdot (4)$. Factor out the 3:

$$3 \cdot \left(-(2 \cdot 1) + (-2 \cdot 4) \right) = 3 \cdot \det \begin{pmatrix} + & - \\ \cancel{-2} & \cancel{2} \\ \cancel{1} & \cancel{4} \end{pmatrix} = 3 \cdot \left(- \det \begin{pmatrix} + & - \\ 2 & -2 \\ 4 & 1 \end{pmatrix} \right)$$

We are multiplying the middle entry “3” by the *negative* of the determinant which appears kitty-corner to “3.” In the original matrix, we can see this idea as:

$$\left(\begin{array}{ccc|cc} & & 1 & & \\ & & 3 & & \\ & & 2 & & \\ \hline & 2 & & -2 & \\ & 1 & & 3 & \\ & 4 & & 1 & \end{array} \right)$$

We can think of this *negative* as coming from the idea that the original matrix is *only one column switch away* (i.e. an *odd* permutation) from:

- having the entry 3 from the original first column moved to the diagonal
- maintaining the order of all the other columns

as is illustrated:

$$\left(\begin{array}{c|cc|cc} 1 & & & & \\ 3 & & & & \\ 2 & & & & \\ \hline & 2 & -2 & & \\ & 1 & 3 & & \\ & 4 & 1 & & \end{array} \right) \longrightarrow \left(\begin{array}{cc|c} 2 & & \\ 1 & & \\ 4 & & \\ \hline & 1 & \\ & 3 & \\ & 2 & \\ \hline & -2 & \\ & 3 & \\ & 1 & \end{array} \right)$$

P_3 permuted diagonals:

$$+ \left(\begin{array}{cc|c} 2 & -2 & \\ 1 & 3 & \\ \hline 4 & 1 & \\ \hline 1 & 3 & \\ 2 & & \end{array} \right) - \left(\begin{array}{cc|c} -2 & 2 & \\ 3 & 1 & \\ \hline 1 & 4 & \\ \hline 1 & 3 & \\ 2 & & \end{array} \right)$$

What we see are the diagonal products $+(2 \cdot 3) \cdot 2$ and $-(-2 \cdot 1) \cdot 2$. Factor out the 2:

$$2 \cdot \left((2 \cdot 3) - (-2 \cdot 1) \right) = 2 \cdot \det \left(\begin{array}{cc|c} + & - & \\ 2 & -2 & \\ 1 & 3 & \\ \hline & & \end{array} \right)$$

We are multiplying the bottom entry “2” by the determinant which appears kitty-corner to “2” in the original matrix:

$$\left(\begin{array}{c|cc} 1 & 2 & -2 \\ 3 & 1 & 3 \\ \hline 2 & 4 & 4 \end{array} \right)$$

The reason why we take the *positive* of the determinant and not the negative is due to the original matrix being precisely *two* column switches away (i.e. an *even* permutation) from:

- having the entry 2 from the original first column moved to the diagonal
- maintaining the order of all the other columns

as is illustrated:

$$\left(\begin{array}{c|cc} 1 & 2 & -2 \\ 3 & 1 & 3 \\ \hline 2 & 4 & 1 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 2 & 1 & -2 \\ 1 & 3 & 3 \\ 4 & 2 & 1 \end{array} \right)$$

$$\rightarrow \left(\begin{array}{cc|c} 2 & -2 & 1 \\ 1 & 3 & 3 \\ 4 & 1 & 2 \end{array} \right)$$

Notice that it is the same distance to the diagonal for the entry “2” vertically or horizontally. So, even if we were permuting rows instead of columns, it would still be an even permutation that would both maintain the ordering of the other rows and send “2” to the diagonal.

$$\left(\begin{array}{ccc|c} 1 & 2 & -2 & 1 \\ 3 & 1 & 3 & 3 \\ 2 & 4 & 1 & 2 \end{array} \right)$$

Putting the pieces together:

$$\begin{aligned}
 & 1 \cdot \det \underbrace{\begin{pmatrix} + & & - \\ 1 & 3 & \\ \times & \times & \times \\ 4 & 1 & \end{pmatrix}}_{1 \cdot 1 - (3 \cdot 4)} + 3 \cdot \left(- \det \underbrace{\begin{pmatrix} + & & - \\ 2 & -2 & \\ \times & \times & \times \\ 4 & 1 & \end{pmatrix}}_{-(2 \cdot 1 - (-2 \cdot 4))} \right) + 2 \cdot \det \underbrace{\begin{pmatrix} + & & - \\ 2 & -2 & \\ \times & \times & \times \\ 1 & 3 & \end{pmatrix}}_{2 \cdot 3 - (-2 \cdot 1)} \\
 & = \underbrace{(1, 3, 2)}_{\text{Chosen Column}} \bullet \underbrace{(-11, -10, 8)}_{\text{Signed Determinants}} = 1 \cdot (-11) + 3 \cdot (-10) + 2 \cdot 8 = -25
 \end{aligned}$$

Signed determinants like the ones in our example are called *cofactors*.

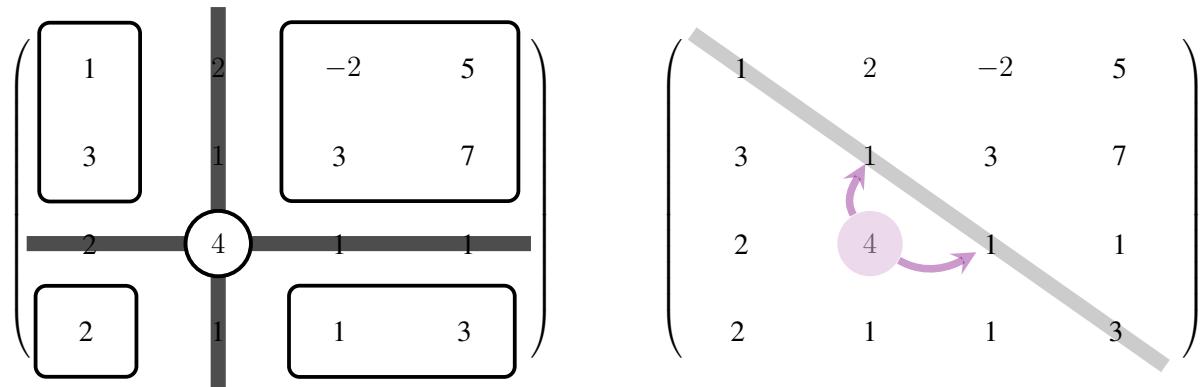
Kitty-corner

The submatrix kitty-corner to a position (i, j) in a matrix is the matrix formed by blocking out row i and column j .

Cofactor

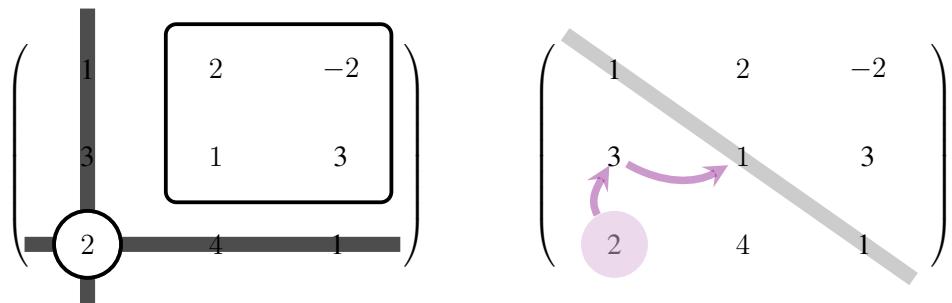
The cofactor C_{ij} associated with the position $(\underbrace{i}_{\text{row}}, \underbrace{j}_{\text{column}})$ in a matrix is the determinant of the submatrix kitty-corner to the position (i, j) multiplied by ± 1 according to whether the number of horizontal/vertical steps to the diagonal is even (+) or odd (-).

Example 3. In the following matrix, the cofactor C_{32} is illustrated. It is the negative of the determinant of the submatrix shown on the left (after removing the row and column in which the entry 4 appears).



$$C_{32} = -\det \begin{pmatrix} 1 & -2 & 5 \\ 3 & 3 & 7 \\ 2 & 1 & 3 \end{pmatrix} = -(-23) = 23$$

Example 4. The following illustrates that the sign of the cofactor C_{31} below is determined by length of any mixed path of horizontal and vertical moves to the diagonal.



$$C_{31} = +\det \begin{pmatrix} 2 & -2 \\ 1 & 3 \end{pmatrix} = 8$$

Important Note about Cofactors

The value of a cofactor has nothing to do with the entry in the matrix at position (i, j) . It has everything to do with the *position* (i, j) .

Diagonal Cofactors

Cofactors of the kind C_{jj} always have a $(+)$ associated with them—that is they are simply the determinant of what is kitty-corner with no change in sign. This is because there is 0 distance to the diagonal.

6.2.2 Generalizing to other Permutation Partitions

Let's go back to our motivational example of the last subsection when we partitioned S_3 into chunks P_1 , $P_2 = (1\ 2) \circ P_1$, and $P_3 = (1\ 3\ 2) \circ P_1$. Notice that these are all *left* composition shifts of P_1 . The collection P_1 is the subgroup of S_3 that fixes 1: *leaves it alone*. Left shifts (via the group operation) of a subgroup have a special name. They are known as *left cosets* (companion sets) to the subgroup.

Cosets

Let G be a group with the operation \star between its elements. Let $H \subset G$ be subgroup (meaning that H is a group with respect to \star and is a subset of G). Then for any $g \in G$, the set $g \star H = \{g \star x : x \in H\}$ is called a *left coset* of H in G . The set $H \star g = \{x \star g : x \in H\}$ is called a *right coset* of H in G . If the operation \star is commutative meaning that $a \star b = b \star a$, then the left coset $g \star H$ is the same as the right coset $H \star g$. In that case, we dispense with the words left and right and simply say "cosets."

Example 5. The nonzero fibers of a linear transformation $f : D \rightarrow C$ are cosets of the kernel $\ker(f) = f^{-1}(0_C)$. They are *additive shifts* of the kernel subspace which itself is a subgroup with respect to $(+)$.

Partitions by Cosets

Cosets partition a group. That is, they divide it into disjoint parts.

In the last subsection we illustrated partitioning the permutations into the (left) cosets of the subgroup that fixes the first column. We could have likewise used the subgroup that fixes the second column or the third column and looked at its cosets. Or we could have chosen the subgroup that fixes the first row or the second row or the third row. For each subgroup, we look at its cosets. Yet all of these choices result in the following process:

Determinant by Cofactors:

Let A be a square matrix and let v be a vector representing one of its rows or columns. Let c_v be the vector of cofactors corresponding to the positions in the vector v . Then,

$$\det(A) = c_v^T \cdot v = c_v \bullet v$$

Cofactor Function

Let g be a linear transformation given by the matrix c_v^T . Then, $g : D \rightarrow \mathbb{R}$ outputs the determinant $g(x)$ when the row or column v is replaced by the vector $x \in D$.

Example 6. Suppose that we want to compute the determinant of the matrix using the indicated row as the vector v :

$$v \quad \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix}$$

Then the vector of cofactors corresponding to v is

$$\begin{aligned} c_v = (C_{31}, C_{32}, C_{33}) &= \left(+ \det \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}, - \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, + \det \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right) \\ &= (2, -1, 1) \end{aligned}$$

Therefore, thinking of all vectors as being “columns” by default, we say that $c_v^T = (2 \quad -1 \quad 1)$. Therefore, the determinant of our matrix is:

$$c_v^T \cdot v = (2 \quad -1 \quad 1) \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 3$$

The vector c_v only depends on the position of v in the matrix.

Example 7. Suppose that we switch out the vector in the third row of the matrix in the last example by the vector $(3, 1, 0)$:

$$v \quad \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 3 & 1 & 0 \end{pmatrix}$$

The vector c_v only depends on the rows above v . Therefore, we already have everything that we need to

compute the determinant of our matrix. We use the same c_v as in the last example. The determinant is:

$$c_v^T \cdot v = \begin{pmatrix} 2 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix} = 5$$

Example 8. The matrix for the cofactor function g of the matrix in the last two examples is the same. It is given by the matrix $\begin{pmatrix} 2 & -1 & 1 \end{pmatrix}$.

Cofactor Expansion

When we use a cofactor function to compute a determinant that is determined by a specific row or column, we say that we have computed the determinant using a cofactor expansion along that row or column.

Example 9. In the last three examples we have been considering a cofactor expansion along the third row of the matrix.

6.2.3 Using Cosets of Smaller Subgroups

We can actually compute the determinant of a 4×4 matrix *using only* 2×2 submatrices if we are clever about how we make our partition of S_4 . Again, we use a coset partition. We take left cosets of the subgroup that leaves the first two columns in the first two columns. Let H be this subgroup. *It is smaller than the subgroup of what keeps a row or a column fixed.* Then,

$$H = \{\text{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

Since $|H| = 4$ and all left cosets of H are the same size and are disjoint, there are

$$\frac{|S_4|}{|H|} = \frac{4!}{4} = \frac{\not{4} \cdot 3 \cdot 2 \cdot 1}{\not{4}} = 6$$

different left cosets. The sum of the permuted diagonals from each left coset will be represented as a product of two 2×2 determinants. That is, we will consider six products of 2×2 determinants and add these up. *This beats finding all 24 signed permuted diagonals and adding them up!*

Let's discuss how this will work. Each left coset will be a shift of H on the left. We choose six distinct elements of S_4 that provide the necessary shifts *and* that always put the destination of column 3 in front of the destination of column 4. To get these shifting elements, we need a definition:

Central (or Principal) Submatrix

A central matrix (often known as a principal submatrix) is a square submatrix whose diagonal is in line with the diagonal of the original matrix.

Example 10. Here are two 2×2 central submatrices:

$$\left(\begin{array}{ccccc} & 2 & 0 & 1 & \\ 1 & & & & \\ 0 & 1 & 1 & & \\ & 0 & 2 & & \\ 1 & & & 1 & \\ 2 & 1 & 2 & & 2 \end{array} \right)$$

$$\left(\begin{array}{ccccc} 1 & & 0 & 1 & \\ 0 & 1 & & & \\ 1 & & 2 & & \\ 2 & 1 & 2 & 1 & \\ & 0 & 1 & 1 & \\ & 2 & & & 2 \end{array} \right)$$

Example 11. Here is a 3×3 central submatrix:

$$\left(\begin{array}{ccccc} & 2 & 0 & 1 & \\ 1 & & & & \\ 0 & 1 & 1 & 1 & \\ & 0 & 2 & 1 & \\ 1 & & & 1 & \\ 2 & 1 & 2 & 2 & 2 \end{array} \right)$$

Example 12. Every entry in the diagonal is itself a 1×1 central submatrix.

So, now let's divide our 4 matrix with a line down the middle:

$$\left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right)$$

Every permutation in H respects this line and never sends a column across it. Now, let's consider the 2×2 submatrices on the left of the line. There are six possibilities:

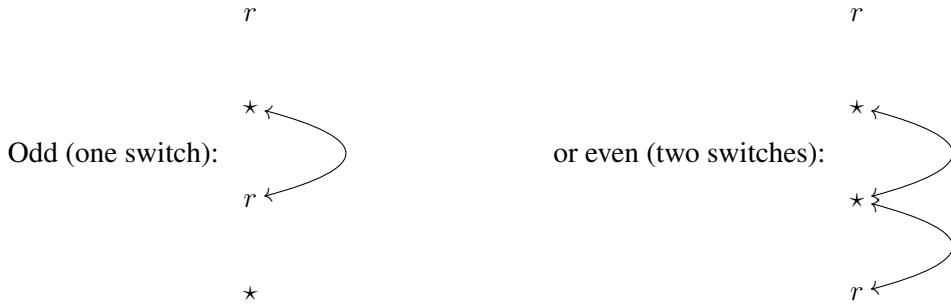
$$\left(\begin{array}{cc|cc} \boxed{1} & 2 & 0 & 1 \\ 0 & \boxed{1} & 1 & 1 \\ 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right) \quad \left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & \boxed{1} & 1 & 1 \\ \boxed{1} & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right)$$

$$\left(\begin{array}{cc|cc} \boxed{1} & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right) \quad \left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & \boxed{1} & 1 & 1 \\ 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right)$$

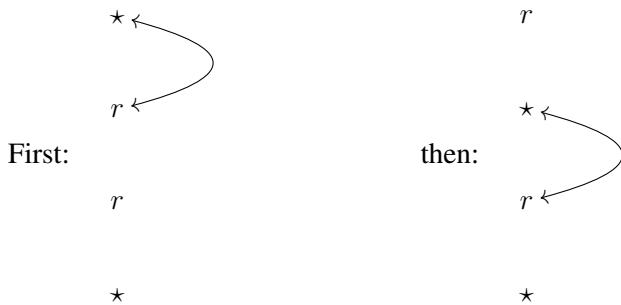
$$\left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right) \quad \left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ \boxed{1} & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right)$$

Each of these six submatrices can actually represent a whole left coset of H . We consider the unique permutation that sends one of these to become a central submatrix along the diagonal and leaves the *order* of the columns that begin on the right of the line alone (even though their positions change). That permutation *is* the desired shift that will describe our left coset of H . We only need to determine whether this shift is an even permutation or an odd one.

One way to see this is to realize that the parity (oddness or evenness) of the permutation can also be found by considering row permutations. To make the matrix central in a row sense simply means to bring the submatrix ***to the top***. It is like we have four rows where we have chosen two of them (labeled as r) and we would like to switch both r 's ***to the top*** while keeping the \star 's in order. This is done by *one adjacent switch at a time*:



Or if we want to bring two up together:



Notice that this would be an even permutation. In fact, to bring two that are initially touching requires the same number of adjacent switches for both rows. So, two touching rows always result in an even permutation. One between is odd and two between is even.

The determinant of the submatrix on the left multiplied by the determinant of the kitty-corner submatrix on the right multiplied by ± 1 depending on if the left submatrix represents an even or odd shift gives the sum of all signed diagonal products in a left coset of H . Add all six of these signed products and you get the sum of *all* 24 signed permuted diagonals. *This is the determinant of the 4×4 matrix!* For instance:

+ 0 apart \implies even

$$\left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right)$$

$$(1) \cdot (2)$$

- 1 apart \implies odd

$$\left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right)$$

$$(-2) \cdot (0)$$

+ 2 apart \implies even

$$\left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right)$$

$$(-3) \cdot (-1)$$

+ 0 apart \implies even

$$\left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right)$$

$$(-1) \cdot (-2)$$

- 1 apart \implies odd

$$\left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right)$$

$$(-2) \cdot (-2)$$

+ 0 apart \implies even

$$\left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{array} \right)$$

$$(1) \cdot (-1)$$

So that the determinant of this 4×4 matrix is:

$$+(1 \cdot 2) - (-2 \cdot 0) + (-3 \cdot (-1)) + (-1 \cdot (-2)) - (-2 \cdot (-2)) + (1 \cdot (-1)) = 2$$

When one becomes adept with the notions of cosets, one may find many different determinant finding techniques. But for us, the kitty-corner techniques discussed thus far will suffice.

6.2.4 Airdropping and Cofactor Techniques



Video Remember that airdropping by rows or columns does not change the determinant. Sometimes we can use airdropping to simplify a determinant by cofactors.

Airdropping with Cofactor Strategy

Airdrop until a row or a column has only one nonzero element. Then, use the cofactor vector associated with that row or column to compute the determinant.

Example 13. Let's compute the determinant of the matrix

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

Let's try to use the above strategy:

$$\begin{array}{ccc} \left(\begin{array}{ccc} 3 & 2 & 1 \\ 1 & 1 & 3 \\ 2 & 1 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 3 & 0 & 1 \\ 1 & -5 & 3 \\ 2 & -1 & 1 \end{array} \right) \\ \left(\begin{array}{ccc} 3 & 2 & 1 \\ 1 & 1 & 3 \\ 2 & 1 & 1 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{ccc} 0 & 0 & 1 \\ -10 & -5 & 3 \\ -1 & -1 & 1 \end{array} \right) \end{array}$$

$$\begin{pmatrix} 0 & 0 & 1 \\ -10 & -5 & 3 \\ -1 & -1 & 1 \end{pmatrix}$$

Since the sign associated with the 1 in the right top corner is + and because all of the other entries in the top row are 0's, the determinant of the matrix is simply:

$$1 \cdot \det \begin{pmatrix} -10 & -5 \\ -1 & -1 \end{pmatrix} = 5.$$

6.2.5 Matrix Multiplication and Determinants

Elementary Matrix

An elementary matrix is the matrix representing the linear transformation which itself gives an elementary row *or* column operation. That is, it is the same as applying an elementary row or column operation to an identity matrix.

Example 14. Consider the determinant of an elementary matrix that represents airdropping

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which represents airdropping double the first row to the second row or equivalently this could be thought of as airdropping double the second column onto the first column. The determinant of this matrix is 1.

The determinant of an elementary matrix that represents airdropping is 1.

Example 15. What about an elementary matrix that represents switching like:

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

This represents switching the first and second rows or equivalently this could be thought of as switching the second column and first columns. The determinant of this matrix is -1 .

The determinant of an elementary matrix that represents one row or column switch is -1 .

Example 16. What about an elementary matrix that represents rescaling a row or a column? Consider:

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

This matrix represents rescaling either the last row or column by 2. The determinant is also itself 2.

The determinant of an elementary matrix that represents rescaling a row or a column is the very scalar that we are rescaling by.

Theorem 6.2.7

Applying an elementary row or column operation does the same thing to the determinant of the matrix as does multiplying by the determinant of the elementary matrix itself.

Proof. Airdropping does not change the determinant—and neither does multiplying by 1. Switching two rows or two columns changes all their even permutations to odd ones and odd permutations to even ones thus changing the sign of the determinant which is the same as multiplying by -1 . Rescaling a row or a column by a number multiplies all permuted diagonals by that one number which multiplies the whole determinant by that number. \square

Corollary 6.2.8

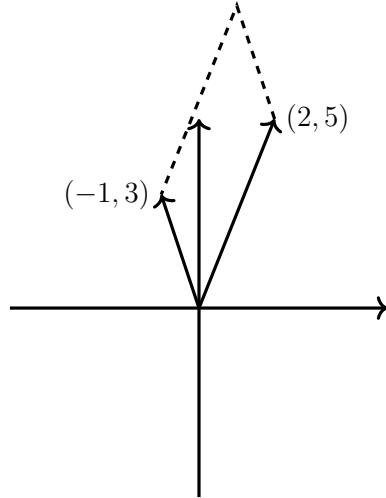
Let A and B be two square matrices of the same size. Then:

$$\det(AB) = \det(A)\det(B)$$

Proof. Suppose first that A and B have the identity as their Smith normal form. Then, A could represent a product of many elementary matrices to the identity on both sides that reverse the operations that take us to the identity. The matrix B is built the very same way. The product AB is therefore the product of a list of elementary matrices to the identity. The determinant of this matrix is the same as the product of determinants of all the elementary matrices by the last theorem. This product is itself equal to the product of determinants of the elementary matrices yielding A and those yielding B thus yielding our result. \square

This idea is extremely useful for determining how the area of a parallelogram or the volume of a higher dimensional parallelogram changes under a linear transformation.

Example 17. Suppose that two sides of a parallelogram are given by vectors $(2, 5)$ and $(-1, 3)$:

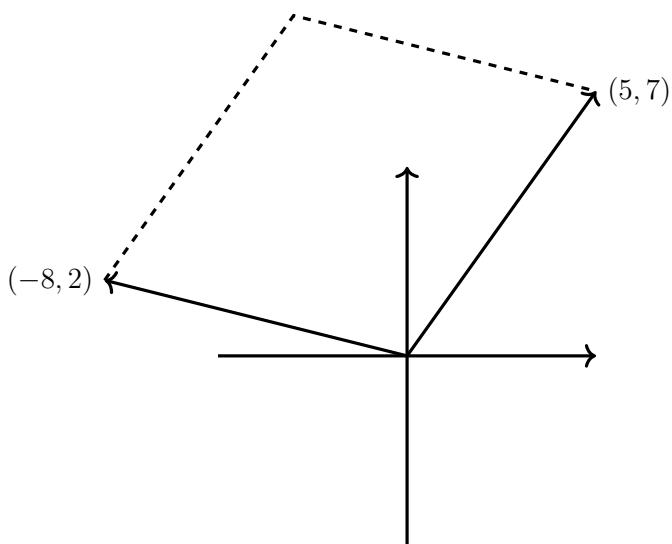


The area of this parallelogram is given by

$$\det \begin{pmatrix} 2 & -1 \\ 5 & 3 \end{pmatrix} = 6 + 5 = 11.$$

Applying the linear transformation $\begin{pmatrix} 5 & -1 \\ 1 & 1 \end{pmatrix}$ to this parallelogram, produces a new parallelogram:

$$\begin{pmatrix} 5 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 \\ 5 & 3 \end{pmatrix} = \begin{pmatrix} 5 & -8 \\ 7 & 2 \end{pmatrix}$$



How has the area of the original parallelogram changed under this transformation? It has been multiplied by:

$$\det \begin{pmatrix} 5 & -1 \\ 1 & 1 \end{pmatrix} = 6.$$

Hence, the area of the new parallelogram is 66. This could have also been found by taking the determinant

$$\det \begin{pmatrix} 5 & -8 \\ 7 & 2 \end{pmatrix} = 10 + 56 = 66.$$

Multiplying determinants is in sync directly with multiplying matrices. Multiplicative inverses of matrices correspond to scalar multiplicative inverses of the matrices themselves.

Corollary 6.2.9

$$\det(A^{-1}) = \frac{1}{\det(A)}$$

Example 18. Consider rewriting the parallelogram of the last example in terms of the basis $a = (1, 1)$ and

$b = (-2, 1)$ as follows where the pretending matrix U^{-1} is the inverse of the unpretending one U :

$$\underbrace{\frac{1}{3} \cdot \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}}_{U^{-1}} \underbrace{\begin{pmatrix} 2 & -1 \\ 5 & 3 \end{pmatrix}}_A \underbrace{\begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix}}_U$$

We have:

$$\begin{aligned} \det(U^{-1} \cdot AU) &= \det(U^{-1}) \cdot \det(A) \cdot \det(U) \\ &= \frac{1}{\det(U)} \cdot \det(A) \cdot \det(U) = \det(A) \end{aligned}$$

In other words, the area of the parallelogram is exactly the same no matter which basis we express it in!!!!

Theorem 6.2.10

Change of basis does not change the determinant of a matrix.

6.2.6 Diagonal Blocks and Determinants

Suppose that we wish to compute the determinant of

$$M = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 4 & 2 & 0 & 0 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 2 & -1 \end{pmatrix}$$

We can write M as a diagonal block matrix

$$M = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

where 0 signifies a block of 0's and

$$A = \begin{pmatrix} 1 & 2 \\ 4 & 2 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix}.$$

Notice that

$$M = \begin{pmatrix} A & 0 \\ 0 & \text{id} \end{pmatrix} \cdot \begin{pmatrix} \text{id} & 0 \\ 0 & B \end{pmatrix}$$

by matrix block multiplication where id is an identity block. Therefore,

$$\det M = \det \begin{pmatrix} A & 0 \\ 0 & \text{id} \end{pmatrix} \cdot \det \begin{pmatrix} \text{id} & 0 \\ 0 & B \end{pmatrix}$$

Let's consider

$$\det \begin{pmatrix} A & 0 \\ 0 & \text{id} \end{pmatrix} = \det \begin{pmatrix} 1 & 2 & 0 & 0 \\ 4 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Consider a cofactor expansion on the last column. Only one entry—the $+1$ on the diagonal—in that column is nonzero:

$$\left(\begin{array}{ccc|c} 1 & 2 & 0 & 0 \\ 4 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

Hence the determinant of the matrix is

$$+1 \cdot \det \begin{pmatrix} 1 & 2 & 0 \\ 4 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Repeat the same idea on this next determinant:

$$\left(\begin{array}{cc|c} 1 & 2 & 0 \\ 4 & 2 & 0 \\ 0 & 0 & 1 \end{array} \right)$$

We see that the determinant of $\begin{pmatrix} A & 0 \\ 0 & \text{id} \end{pmatrix}$ is simply $\det A$. Similarly, the determinant of $\begin{pmatrix} \text{id} & 0 \\ 0 & B \end{pmatrix}$ is $\det B$. Therefore,

$$\det M = \det A \cdot \det B.$$

Theorem 6.2.11

Suppose that the matrix A is a diagonal block matrix. Then the determinant of A is the product of the determinants of its blocks.

Key Concepts from this Section

- **diagonal matrix:** (page 582) A diagonal matrix is one in which all the entries outside the diagonal from top left to bottom right are zeros:

$$\begin{pmatrix} * & & 0's \\ & \ddots & \\ 0's & & * \end{pmatrix}$$

- **theorem 6.2.1 airdrop to diagonal:** (page 584) Column airdropping is enough to turn any square matrix with entries in a field into a diagonal matrix.
- **corollary 6.2.2 squares come from diagonals:** (page 584) Every square matrix is the result of column airdrops to a diagonal matrix.
- **permuted diagonal product:** (page 585) Given a matrix, permute its columns or its rows and then take the product of the entries that appear in the diagonal from the top left to the bottom right. This product is a permuted diagonal product.
- **determinant of a matrix:** (page 587) Suppose that the columns of a $n \times n$ matrix A are listed as c_1, c_2, \dots, c_n . Let $\tau \in S_n$ and note the matrix given by permuting the columns according to τ by A_τ . Further, let $\text{diag } A_\tau$ be the product down the diagonal of A_τ from top left to bottom right. Then we define the determinant (\det) of A as follows:

$$\det A = \sum_{\tau \text{ even}} \text{diag } A_\tau - \sum_{\tau \text{ odd}} \text{diag } A_\tau$$

- **theorem 6.2.3 permutations of rows or columns:** (page 587) We get the exact same even and odd diagonal products if we permute the rows or if we permute the columns.
- **corollary 6.2.4 determinant of transpose:** (page 587)

$$\det(A^T) = \det(A)$$

- **corollary 6.2.5 column or row airdrops:** (page 587) The n -dimensional volume of the parallelogram formed by the rows is the same as the one formed by the columns. We can “slide” to a diagonal matrix by row airdrops or column airdrops or a mixture of both and obtain the same determinant.

- **upper triangular matrix:** (page 588) An upper triangular matrix is one in which every entry below the diagonal from top left to bottom right is 0.
 - **lower triangular matrices:** (page 588) A lower triangular matrix is one in which every entry above the diagonal from top left to bottom right is 0.
 - **theorem 6.2.6 determinants of triangular matrices:** (page 588) If a matrix is upper or lower triangular, the determinant is simply the product of the nonzero diagonal.
 - **slide to a diagonal:** (page 589) When we have a square matrix A , sliding to the diagonal means performing column or row airdrops only until A has turned into a diagonal matrix.
 - **kitty-corner:** (page 593) The submatrix kitty-corner to a position (i, j) in a matrix is the matrix formed by blocking out row i and column j .
 - **cofactor:** (page 593) The cofactor C_{ij} associated with the position $(\underbrace{i}_{\text{row}}, \underbrace{j}_{\text{column}})$ in a matrix is the determinant of the submatrix kitty-corner to the position (i, j) multiplied by ± 1 according to whether the number of horizontal/vertical steps to the diagonal is even (+) or odd (-).
 - **important note about cofactors:** (page 594) The value of a cofactor has nothing to do with the entry in the matrix at position (i, j) . It has everything to do with the *position* (i, j) .
 - **diagonal cofactors:** (page 594) Cofactors of the kind C_{jj} always have a (+) associated with them—that is they are simply the determinant of what is kitty-corner with no change in sign. This is because there is 0 distance to the diagonal.
 - **cosets:** (page 595) Let G be a group with the operation \star between its elements. Let $H \subset G$ be subgroup (meaning that H is a group with respect to \star and is a subset of G). Then for any $g \in G$, the set $g \star H = \{g \star x : x \in H\}$ is called a *left coset* of H in G . The set $H \star g = \{x \star g : x \in H\}$ is called a *right coset* of H in G . If the operation \star is commutative meaning that $a \star b = b \star a$, then the left coset $g \star H$ is the same as the right coset $H \star g$. In that case, we dispense with the words left and right and simply say “cosets.”
 - **partitions by cosets:** (page 595) Cosets partition a group. That is, they divide it into disjoint parts.
 - **determinant by cofactors:** (page 595) Let A be a square matrix and let v be a vector representing one of its rows or columns. Let c_v be the vector of cofactors corresponding to the positions in the vector v . Then,
- $$\det(A) = c_v^T \cdot v = c_v \bullet v$$
- **cofactor function:** (page 595) Let g be a linear transformation given by the matrix c_v^T . Then, $g : D \rightarrow \mathbb{R}$ outputs the determinant $g(x)$ when the row or column v is replaced by the vector $x \in D$.

- **cofactor expansion:** (page 597) When we use a cofactor function to compute a determinant that is determined by a specific row or column, we say that we have computed the determinant using a cofactor expansion along that row or column.
- **central (or principal) submatrix:** (page 597) A central matrix (often known as a principal submatrix) is a square submatrix whose diagonal is in line with the diagonal of the original matrix.
- **airdropping with cofactor strategy:** (page 602) Airdrop until a row or a column has only one nonzero element. Then, use the cofactor vector associated with that row or column to compute the determinant.
- **elementary matrix:** (page 603) An elementary matrix is the matrix representing the linear transformation which itself gives an elementary row *or* column operation. That is, it is the same as applying an elementary row or column operation to an identity matrix.
- **theorem 6.2.7 :** (page 604) Applying an elementary row or column operation does the same thing to the determinant of the matrix as does multiplying by the determinant of the elementary matrix itself.
- **corollary 6.2.8 :** (page 604) Let A and B be two square matrices of the same size. Then:

$$\det(AB) = \det(A) \det(B)$$

- **corollary 6.2.9 :** (page 606)

$$\det(A^{-1}) = \frac{1}{\det(A)}$$

- **theorem 6.2.10 :** (page 607) Change of basis does not change the determinant of a matrix.
- **theorem 6.2.11 :** (page 608) Suppose that the matrix A is a diagonal block matrix. Then the determinant of A is the product of the determinants of its blocks.

6.2.7 Exercises

Compute the Determinant

Compute the determinant of each of the following by using a strategic use of sliding and cofactors. Show how you do so.

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

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

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

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

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

$$6. \begin{pmatrix} 2 & 1 & -1 \\ -1 & -2 & 0 \\ 0 & -2 & -1 \end{pmatrix}$$

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

$$8. \begin{pmatrix} 0 & -2 & 1 \\ -1 & 0 & -2 \\ 2 & 0 & -1 \end{pmatrix}$$

$$9. \begin{pmatrix} 0 & 2 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 2 \end{pmatrix}$$

$$10. \begin{pmatrix} 0 & -2 & 1 \\ 2 & 0 & 0 \\ -2 & 0 & 2 \end{pmatrix}$$

$$11. \begin{pmatrix} 2 & -1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 2 & -2 & -2 \\ 0 & -2 & -1 & 2 \end{pmatrix}$$

$$12. \begin{pmatrix} 0 & -2 & -1 & 2 \\ 0 & 0 & -1 & -1 \\ 2 & 0 & 1 & -2 \\ -2 & 0 & 0 & 2 \end{pmatrix}$$

13.
$$\begin{pmatrix} -2 & 0 & 0 & -2 \\ 2 & 0 & -2 & 0 \\ 1 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix}$$

14.
$$\begin{pmatrix} 0 & 1 & 1 & -1 \\ 0 & 1 & -2 & 0 \\ 1 & -2 & 1 & -2 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

15.
$$\begin{pmatrix} 2 & -1 & 1 & -1 \\ -1 & -1 & 2 & -1 \\ -2 & -1 & 0 & 1 \\ 1 & 0 & 0 & 2 \end{pmatrix}$$

16.
$$\begin{pmatrix} 2 & -2 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 \\ -2 & 0 & -2 & 0 \end{pmatrix}$$

17.
$$\begin{pmatrix} 0 & -1 & 2 & -1 \\ 1 & 0 & 2 & 0 \\ 0 & -2 & 0 & 2 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

18.
$$\begin{pmatrix} 0 & 2 & 2 & -2 \\ -2 & 0 & 0 & 0 \\ 1 & -1 & -2 & 0 \\ -1 & 0 & 0 & -1 \end{pmatrix}$$

19.
$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ -2 & 2 & -1 & 0 \\ -2 & -1 & 0 & 2 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

20.
$$\begin{pmatrix} 2 & 1 & -2 & -2 \\ 0 & -2 & -2 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Determinants of 4×4 's using 2×2 Submatrices

In each of the following, use determinants of 2×2 submatrices as explained in the reading to find the determinant. Show how you do so.

21.
$$\begin{pmatrix} 2 & -2 & 1 & 2 \\ 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 \end{pmatrix}$$

22.
$$\begin{pmatrix} -1 & 1 & 2 & -1 \\ 2 & 0 & -1 & 0 \\ 0 & 0 & -2 & 0 \\ -1 & 2 & 0 & 0 \end{pmatrix}$$

23.
$$\begin{pmatrix} -2 & 0 & 0 & -2 \\ -2 & 0 & -1 & -1 \\ 2 & 2 & 1 & 2 \\ 2 & 1 & 0 & 2 \end{pmatrix}$$

24.
$$\begin{pmatrix} 2 & -2 & 2 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & -1 & -1 & -1 \\ 2 & 1 & -1 & -2 \end{pmatrix}$$

25.
$$\begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ -2 & 0 & -1 & 0 \end{pmatrix}$$

26.
$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & -2 \\ 2 & 1 & 1 & 0 \\ 0 & 2 & 1 & -1 \end{pmatrix}$$

27.
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 2 & -1 & 2 \\ -1 & 2 & 0 & -2 \end{pmatrix}$$

28.
$$\begin{pmatrix} 0 & 2 & 0 & -1 \\ 0 & -2 & 1 & -1 \\ 2 & 0 & 0 & 2 \\ -1 & 1 & 0 & 0 \end{pmatrix}$$

29.
$$\begin{pmatrix} -1 & 0 & 0 & 1 \\ 2 & 0 & 0 & -1 \\ 0 & -2 & 1 & 0 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

30.
$$\begin{pmatrix} -1 & 0 & -2 & 0 \\ 2 & 0 & 0 & -1 \\ 0 & -1 & -1 & 0 \\ 0 & 0 & -2 & -2 \end{pmatrix}$$

Using Determinant Properties

For each of the following, identify determinants of elementary matrices and consider how determinants work across products and inverses. Show how you use these ideas to find the determinant.

31.
$$\begin{pmatrix} -1 & -2 & -1 \\ 0 & 2 & -2 \\ 2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1}$$

32.
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & -2 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ -2 & -1 & 2 \end{pmatrix}^{-1} \cdot \begin{pmatrix} -1 & 1 & -1 \\ -1 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}^{-1}$$

33.
$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 1 \\ 2 & 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 0 & -1 \\ 1 & -1 & -2 \\ 0 & 0 & 2 \end{pmatrix}^{-1}$$

34.
$$\begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & 1 \\ -2 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 0 \\ -1 & -1 & 0 \\ -1 & 0 & -1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1}$$

35. $\begin{pmatrix} 0 & 0 & -2 \\ 0 & -1 & 0 \\ -2 & 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 2 \\ -1 & -2 & 1 \\ 2 & 0 & -2 \end{pmatrix}^{-1}$

36. $\begin{pmatrix} 1 & -1 & 2 \\ 2 & 2 & 1 \\ 1 & 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & -2 \\ -1 & -1 & -1 \\ 0 & -2 & 2 \end{pmatrix}^{-1}$

37. $\begin{pmatrix} -2 & -1 & 2 \\ 1 & -1 & -2 \\ -1 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & -2 \\ 2 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}^{-1}$

38. $\begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}^{-1}$

39. $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & 0 & -1 \\ -1 & -1 & -1 \\ 0 & -1 & 0 \end{pmatrix}^{-1}$

40. $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 & 2 \\ 0 & -1 & 0 \\ 2 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1}$

41. $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1}$

42. $\begin{pmatrix} 2 & -2 & 0 \\ -1 & -1 & -1 \\ 0 & -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}^{-1}$

43. $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}^{-1}$

44. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -2 & 0 \\ 1 & 0 & 0 \\ 2 & -1 & 2 \end{pmatrix}^{-1}$

45. $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & -2 \\ -1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & -2 \\ 0 & 1 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} -2 & 2 & -2 \\ -2 & 0 & 0 \\ -1 & 0 & -2 \end{pmatrix}^{-1}$

46. $\begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 0 \\ -1 & -2 & -2 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 & -2 \\ 0 & 0 & -2 \\ -2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & 0 & -2 \\ -1 & -1 & 2 \\ 1 & 0 & -2 \end{pmatrix}^{-1}$

Diagonal Block Matrices

Compute the determinants of the following using the idea in the text for diagonal block matrices.

47. $\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & -2 & -2 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 2 & -1 \\ 0 & 0 & 0 & -1 & -2 \end{pmatrix}$

48. $\begin{pmatrix} -1 & -1 & 0 & 0 & 0 & 0 \\ -2 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & -2 & 2 \end{pmatrix}$

49. $\begin{pmatrix} -2 & 0 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 & 0 \\ 0 & -2 & -2 & 0 & 0 \\ 0 & 0 & 0 & -2 & -1 \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix}$

50. $\begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$

51. $\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 & 0 \\ 0 & -2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 2 & -2 \\ 0 & 0 & 0 & -1 & -2 \end{pmatrix}$

52. $\begin{pmatrix} -2 & -2 & 0 & 0 \\ -2 & -2 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$

53. $\begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -2 & -2 & 0 & 0 \\ 0 & -2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 & 1 \end{pmatrix}$

54. $\begin{pmatrix} -2 & 0 & 0 & 0 & 0 \\ 0 & -2 & -2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & -1 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}$

$$\mathbf{55.} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$\mathbf{56.} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

6.2.8 Solutions

1. -2

2. 3

3. -2

4. 2

5. 2

6. 1

7. -4

8. 10

9. -6

10. 8

11. -12

12. -4

13. 4

14. -9

15. 16

16. -16

17. 8

18. 4

19. 3

20. -1

21. -2

22. 8

23. 2

24. 12

25. -4

26. -8

27. 4**28.** 6**29.** 3**30.** -6**31.** -10**32.** 4**33.** 8**34.** -4**35.** 32**36.** -52**37.** -42**38.** 1**39.** -1**40.** -5**41.** -1**42.** 8**43.** -1**44.** 4**45.** -32**46.** 24**47.** 0**48.** 0**49.** 60**50.** 4**51.** 72**52.** 0**53.** 4**54.** 0**55.** 4**56.** -1

Inverses, Cramer's Rule, and Singular Matrices

6.3

6.3.1 Inverses by Cofactors	620
6.3.2 Cramer's Rule	623
6.3.3 Singular and Nonsingular Matrices	625
6.3.4 Exercises	629
6.3.5 Solutions	633

Questions to Guide Your Study:

- *How can cofactors help us find the inverse of a matrix?*
- *How can cofactors help us solve a system of equations?*

6.3.1 Inverses by Cofactors



Consider the following two matrices multiplied together:

$$c_{v_1}^T \begin{pmatrix} 1 & -6 & 2 \\ 1 & 3 & -1 \\ -1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \text{matrix } A$$

Notice that

$$c_{v_1}^T \cdot v_1 = \det(A).$$

But also notice that

$$c_{v_1}^T \cdot v_2 = 0$$

since the cofactor function $c_{v_1}^T$ calculates what the determinant of A would be if the column v_1 were replaced by the input of the function. If we choose to put v_2 as the input, we are calculating:

$$c_{v_1}^T \cdot v_2 = \det \begin{pmatrix} 2 & 2 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 3 \\ v_2 & v_2 & v_3 \end{pmatrix} = 0$$

Since we have a repeated column, the determinant is 0.

Any time we put a column into a cofactor function representing a different column, we get 0.

Any time we put a column into a cofactor function representing the same column, we get the determinant.

Hence, we have:

$$\begin{matrix} \text{Cofactor Functions} \\ c_{v_1}^T \\ c_{v_2}^T \\ c_{v_3}^T \end{matrix} \left(\begin{array}{ccc} 1 & -6 & 2 \\ 1 & 3 & -1 \\ -1 & 0 & 1 \end{array} \right) \cdot \left(\begin{array}{ccc} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 1 & 2 & 3 \\ v_1 & v_2 & v_3 \end{array} \right) = \begin{pmatrix} \det(A) & 0 & 0 \\ 0 & \det(A) & 0 \\ 0 & 0 & \det(A) \end{pmatrix}$$

We pretty much have found the inverse of A . All we need to do is to divide by the determinant of the matrix $\det(A) = 3$:

$$A^{-1} = \frac{1}{3} \cdot \begin{pmatrix} 1 & -6 & 2 \\ 1 & 3 & -1 \\ -1 & 0 & 1 \end{pmatrix}.$$

Adjugate Matrix

Given a matrix A , take the matrix of rows which represent the cofactor functions corresponding to the columns of A , the result is called the adjugate matrix. We notate it by

$$\text{adj}(A)$$

Inverse by Cofactors

$$A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$$

Example 1. Let's compute the inverse of the matrix:

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

We go down each column and compute the cofactors with their corresponding signs to yield:

$$c_{v_1} = (0, -1, 1) \quad c_{v_2} = (0, 2, 0) \quad c_{v_3} = (-2, 5, 1)$$

We can compute the determinant by using any of these cofactor vectors as a function with the corresponding column plugged in. Namely:

$$\det(A) = c_{v_1}^T \cdot v_1 = \begin{pmatrix} 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} = 2$$

Therefore,

$$A^{-1} = \frac{1}{2} \cdot \begin{pmatrix} 0 & -1 & 1 \\ 0 & 2 & 0 \\ -2 & 5 & 1 \end{pmatrix}.$$

Example 2. Let's compute the inverse of the matrix

$$A = \begin{pmatrix} -3 & -4 \\ 2 & 1 \end{pmatrix}$$

We have

$$c_{v_1} = (1, 4) \quad c_{v_2} = (-2, -3)$$

Notice something simplistic in this:

Taking the signed cofactor in a 2×2 matrix is the same as going to the kitty-corner entry and changing its sign only if we are off the diagonal that starts in the top left.

So, really the adjugate is given by swapping the entries on the diagonal and negating the entries off the diagonal since we have already switched columns to rows by considering the cofactor functions as rows:

$$\text{adj}(A) = \begin{pmatrix} 1 & -(-4) \\ -(2) & -3 \end{pmatrix}$$

Now just divide by the determinant which is 5:

$$A^{-1} = \frac{1}{5} \cdot \begin{pmatrix} 1 & 4 \\ -2 & -3 \end{pmatrix}$$

Inverse of a 2×2 Matrix

The inverse of a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given as:

$$\frac{1}{ad - bc} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

6.3.2 Cramer's Rule



Example 3. Suppose that we the following system of equations:

$$\begin{array}{rcl} x & +y & +2z = 1 \\ 2x & +y & -z = 5 \\ x & -2y & -z = -2 \end{array}$$

We can represent this system of equations as follows:

$$\underbrace{\begin{pmatrix} 1 & 1 & 2 \\ 2 & 1 & -1 \\ 1 & -2 & -1 \end{pmatrix}}_A \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ -2 \end{pmatrix}$$

Since A has an inverse, we can solve the system as follows:

$$\underbrace{A^{-1} \cdot A}_{\text{id}} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} 1 \\ 5 \\ -2 \end{pmatrix}$$

That is,

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \frac{1}{\det(A)} \cdot \begin{pmatrix} c_{v_1}^T \\ c_{v_2}^T \\ c_{v_3}^T \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 5 \\ -2 \end{pmatrix}$$

This tells us that:

$$x = \frac{1}{\det(A)} \cdot c_{v_1}^T \cdot \begin{pmatrix} 1 \\ 5 \\ -2 \end{pmatrix} \quad y = \frac{1}{\det(A)} \cdot c_{v_2}^T \cdot \begin{pmatrix} 1 \\ 5 \\ -2 \end{pmatrix} \quad z = \frac{1}{\det(A)} \cdot c_{v_3}^T \cdot \begin{pmatrix} 1 \\ 5 \\ -2 \end{pmatrix}$$

Now remember how cofactor functions work: $c_{v_1}^T$ computes the determinant of A assuming that the input replaces v_1 . Hence, we have:

$$x = \frac{\det \begin{pmatrix} 1 & 1 & 2 \\ 5 & 1 & -1 \\ -2 & -2 & -1 \end{pmatrix}}{\det(A)} \quad y = \frac{\det \begin{pmatrix} 1 & 1 & 2 \\ 2 & 5 & -1 \\ 1 & -2 & -1 \end{pmatrix}}{\det(A)} \quad z = \frac{\det \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 5 \\ 1 & -2 & -2 \end{pmatrix}}{\det(A)}$$

$$x = \frac{-12}{-12} = 1 \quad y = \frac{-24}{-12} = 2 \quad z = \frac{12}{-12} = -1$$

One can check that this solves the system.

Cramer's Rule

The technique of using cofactor functions to find specific parts of the solution to a system of equations just as in the previous example.

6.3.3 Singular and Nonsingular Matrices

Consider the different Smith normal forms that are possible with a 3×3 matrix. *There is a row of zeros if and only if there is a column of zeros.* This means that a 3×3 matrix under either a row or a column interpretation represents a surjective function if and only if it represents an injective function. Let's discuss how we can think of this in terms of determinants. To get the Smith normal form of a 3×3 matrix A , we can multiply on the right by a column operations matrix C and on the left by a row operations matrix R . Then, the Smith normal form is:

$$S = R \cdot A \cdot C$$

which tells us:

$$\det(S) = \det(R) \cdot \det(A) \cdot \det(C)$$

The determinant of a single row operation matrix is never zero. The same holds true for a column operations matrix. Therefore, if $\det(A) \neq 0$, *we must have that* $S = \text{id}_{3 \times 3}$. No other Smith normal form for a 3×3 yields a nonzero determinant! This means that:

Theorem 6.3.1

A square $n \times n$ matrix A represents an injective or a surjective function if and only if $\det(A) \neq 0$.

Nonsingular Square Matrix

A square matrix is called nonsingular if its determinant is nonzero.

Singular Square Matrix

A square matrix is called singular if its determinant is zero.

Corollary 6.3.2

If a matrix is singular then it is neither surjective nor injective. If it is nonsingular, then it is both injective and surjective.

Now how does this relate to what we have been talking about in this section? The system of equations in

the last example could be represented as:

$$\underbrace{\begin{pmatrix} 1 & 1 & 2 \\ 2 & 1 & -1 \\ 1 & -2 & -1 \end{pmatrix}}_A \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ -2 \end{pmatrix}$$

Let $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ be the column interpretation function of the matrix A . Since $\det(A) = -12 \neq 0$, we know that f is both injective and surjective. This means that there are *no empty fibers!* This also means that *there is only one element in each fiber!* Solving the system of equations is exactly the same thing as finding what is in the fiber $f^{-1}(1, 5, -2)$. We found that there was something—and there was only one thing: $(1, 2, -1)$.

Now, the very method of Cramer's rule involves division by $\det(A)$.

We would not have been able to do so if $\det(A)$ had been zero. Yet in our case, A is nonsingular.

Now if A were singular, what conclusion could we draw? Either:

- there is no solution (*because we are considering an empty fiber*) or
- there is more than one solution (*since all nonempty fibers are shifts of the fiber over zero and all have the same size, every single one of these must have more than one element so that the function is not injective.*).

In other words, if all we knew were that $\det(A)$ were zero, then we would only know that there is not a unique solution to the system. We would not even know if there is a solution. But we would know that if there were a solution it would not be the only one. In fact, since the fiber over zero is a vector space with more than one element of it, it has all of $\mathbb{R} \cdot (\text{a nonzero element})$ in it. Wait!

There are infinitely many solutions if there is any solution at all and $\det(A) = 0$.

Corollary 6.3.3

A matrix represents an isomorphism (admitting an inverse) if and only if it is a square matrix with a nonzero determinant. That is, it is a nonsingular matrix.

Example 4. Let's consider if there is a unique solution or not to the following system of equations:

$$\begin{array}{rccccl} x & +y & +2z & = & 1 \\ 2x & +y & -z & = & 2 \\ 3x & +2y & +z & = & 3 \end{array}$$

All we need to do is to check the following determinant:

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

This tells us that this matrix does not represent an injective nor a surjective function. So either there is either no solution or infinitely many. Reduced row echelon form of the augmented matrix yields:

$$\left(\begin{array}{ccc|c} 1 & 0 & -3 & 1 \\ 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

from which we can find a specific solution: $(1, 0, 0)$. Using the fast column technique from the nonpivot column on the left of the augmenting line, we see: $(3, -5, 1)$ is a basis for the kernel. Therefore, all solutions are given by:

$$(1, 0, 0) + \langle (1, -3, 1) \rangle$$

We can see in this case there are infinitely many solutions.

Example 5. Let's suppose that we would like to solve the system

$$\begin{array}{rcl} x & + y & = 1 \\ 2x & + 2y & = 1 \end{array}$$

Notice that

$$\det \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} = 0.$$

This means that either there are many solutions or no solutions at all. Indeed, the reduced row echelon form of the augmented matrix yields:

$$\left(\begin{array}{cc|c} 1 & 1 & 1 \\ 0 & 0 & -1 \end{array} \right)$$

Yet this means that $0 = -1$ which is a contradiction. Therefore, the desired fiber is empty and there is no solution.

Corollary 6.3.4

Every system of equations solves for a fiber of a function. Suppose that the matrix describing that function is A and that A is a square matrix. If $\det(A) \neq 0$, then there is exactly one solution to the system. Otherwise, there are either infinitely many solutions or no solutions at all.

Key Concepts from this Section

- **adjugate matrix:** (page 621) Given a matrix A , take the matrix of rows which represent the cofactor functions corresponding to the columns of A , the result is called the adjugate matrix. We denote it by

$$\text{adj}(A)$$

- **inverse by cofactors:** (page 622)

$$A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$$

- **inverse of a 2×2 matrix:** (page 623) The inverse of a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given as:

$$\frac{1}{ad - bc} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

- **cramer's rule:** (page 624) The technique of using cofactor functions to find specific parts of the solution to a system of equations just as in the previous example.
- **theorem 6.3.1 :** (page 625) A square $n \times n$ matrix A represents an injective or a surjective function if and only if $\det(A) \neq 0$.
- **nonsingular square matrix:** (page 625) A square matrix is called nonsingular if its determinant is nonzero.
- **singular square matrix:** (page 625) A square matrix is called singular if its determinant is zero.
- **corollary 6.3.2 :** (page 625) If a matrix is singular then it is neither surjective nor injective. If it is nonsingular, then it is both injective and surjective.
- **corollary 6.3.3 :** (page 626) A matrix represents an isomorphism (admitting an inverse) if and only if it is a square matrix with a nonzero determinant. That is, it is a nonsingular matrix.
- **corollary 6.3.4 :** (page 627) Every system of equations solves for a fiber of a function. Suppose that the matrix describing that function is A and that A is a square matrix. If $\det(A) \neq 0$, then there is exactly one solution to the system. Otherwise, there are either infinitely many solutions or no solutions at all.

6.3.4 Exercises

Finding Cofactors

Find the indicated cofactor for the given matrix.

1. Find C_{11} for $\begin{pmatrix} 1 & 2 & 0 & -1 \\ 2 & -1 & -2 & -2 \\ 2 & -1 & -1 & 0 \\ -1 & 0 & 1 & -1 \end{pmatrix}$

2. Find C_{32} for $\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & -1 & -2 & 2 \\ -1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}$

3. Find C_{23} for $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 1 & -2 & 2 \\ 1 & -1 & 2 & 0 \\ 2 & 0 & 1 & -1 \end{pmatrix}$

4. Find C_{34} for $\begin{pmatrix} 0 & -1 & 2 & -2 \\ -2 & -1 & 0 & 0 \\ 0 & -1 & -2 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix}$

5. Find C_{41} for $\begin{pmatrix} -2 & 2 & -1 & -2 \\ -2 & 0 & 1 & 1 \\ 1 & 0 & 2 & 2 \\ 0 & -2 & 0 & 0 \end{pmatrix}$

6. Find C_{23} for $\begin{pmatrix} 0 & -1 & 2 & 0 \\ 2 & -2 & 0 & 0 \\ -1 & 0 & 0 & 2 \\ -2 & 0 & 0 & -1 \end{pmatrix}$

Finding Inverses

Find the inverse to the given matrix using the cofactor method.

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

8. $\begin{pmatrix} 1 & -2 & -1 \\ -1 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix}$

9. $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 2 & 1 & 2 \end{pmatrix}$

10. $\begin{pmatrix} 1 & 2 & -1 \\ 2 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$

11.
$$\begin{pmatrix} 1 & -1 & 1 \\ 2 & -2 & -2 \\ 2 & 0 & 2 \end{pmatrix}$$

12.
$$\begin{pmatrix} 0 & 0 & -1 \\ 2 & 1 & 0 \\ -2 & 1 & 0 \end{pmatrix}$$

13.
$$\begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ -2 & 0 & 0 \end{pmatrix}$$

14.
$$\begin{pmatrix} 2 & 0 & -1 \\ 2 & -1 & -1 \\ 0 & 0 & -1 \end{pmatrix}$$

15.
$$\begin{pmatrix} 2 & 0 & -1 \\ -2 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}$$

16.
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 2 \\ -1 & 2 & 0 \end{pmatrix}$$

17.
$$\begin{pmatrix} -2 & 0 \\ 1 & 1 \end{pmatrix}$$

18.
$$\begin{pmatrix} 0 & 2 \\ 1 & -1 \end{pmatrix}$$

19.
$$\begin{pmatrix} -2 & 1 \\ 1 & 1 \end{pmatrix}$$

20.
$$\begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}$$

21.
$$\begin{pmatrix} -1 & 0 \\ -2 & -1 \end{pmatrix}$$

22.
$$\begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}$$

23.
$$\begin{pmatrix} -2 & -1 \\ 0 & -2 \end{pmatrix}$$

24.
$$\begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix}$$

25.
$$\begin{pmatrix} 1 & -2 \\ 2 & 2 \end{pmatrix}$$

26.
$$\begin{pmatrix} 0 & 2 \\ -1 & 2 \end{pmatrix}$$

Cramer's Rule

Write out the fraction of determinants that you would use to calculate the value that should be assigned to the given variable in the solution of the following systems of equations.

27. Find the value of x :

$$\begin{aligned}x + 2y + z &= 0 \\2x + y + 2z &= 0 \\-2x - y + 2z &= -4\end{aligned}$$

28. Find the value of y :

$$\begin{aligned}x - y + 2z &= -5 \\-x - 2y &= 0 \\-2x + 2y - z &= 7\end{aligned}$$

29. Find the value of z :

$$\begin{aligned}x + 2y + 2z &= 0 \\2x + z &= 4 \\2y &= -2\end{aligned}$$

30. Find the value of x :

$$\begin{aligned}-2x - y - 2z &= -8 \\x + 2y - z &= 3 \\-x - 2y + 2z &= -1\end{aligned}$$

31. Find the value of z :

$$\begin{aligned}-x - y - 2z &= 1 \\-x + y + z &= -3 \\-2x + 2y &= -2\end{aligned}$$

32. Find the value of z :

$$\begin{aligned}2x + y + 2z &= -4 \\x - 2y &= 4 \\x + 2y + 2z &= -6\end{aligned}$$

33. Find the value of y :

$$\begin{aligned}2x + y - 2z &= 0 \\-x - 2y &= -1 \\2x - y + z &= 3\end{aligned}$$

34. Find the value of z :

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

35. Find the value of x :

$$\begin{aligned}-x - 2z &= 4 \\x - 2y - 2z &= 6 \\2x - 2z &= 4\end{aligned}$$

36. Find the value of x :

$$\begin{aligned}x + y - 2z &= -2 \\-2x + 2z &= 0 \\-z &= -1\end{aligned}$$

Results of Singular Matrices

The solution of each of the following systems can be described as a fiber of a function f . That function is describable as a 3×3 matrix. Verify that the determinant of that matrix is zero so that the matrix is singular. Solve the system if possible. If not, indicate which fiber is empty.

37. $\begin{aligned}x - 2y + 5z &= -2 \\y - 2z &= 1 \\-x - z &= 0\end{aligned}$

38. $\begin{aligned}y + z &= -3 \\z &= -1 \\y &= -2\end{aligned}$

39. $x = 0$
 $-x - 2y - z = 2$
 $2x + 4y + 2z = -4$

40. $3y + 3z = -6$
 $-2y - 2z = 4$
 $y + z = -2$

41. $x + 4y - z = 2$
 $-x - 4y + z = -2$
 $2x + 8y - 2z = 4$

42. $y = 2$
 $z = 1$
 $y = 2$

43. $x - 2y + 7z = 3$
 $y - 4z = -1$
 $-x + z = -1$

44. $x - 3y + 6z = 2$
 $y - 3z = 0$
 $-x + 3z = -2$

45. $x - 3y + 7z = 4$
 $y - 4z = -2$
 $-x + 5z = 2$

46. $x + 2y - 2z = 0$
 $z = -1$
 $-2x - 4y = 4$

47. $x - 2y - z = 0$
 $z = 0$
 $-2x + 4y = 1$

48. $-x + 4y - z = 2$
 $z = 0$
 $-x + 4y - z = 1$

49. $-z = -1$
 $z = 0$
 $x - 2y + z = -3$

50. $x + y - 3z = -2$
 $y - 2z = 0$
 $= 1$

51. $2x - 8y + 5z = -3$
 $z = 0$
 $x - 4y + 3z = -1$

52. $8x - 16y + 23z = -11$
 $z = 0$
 $3x - 6y + 8z = -4$

6.3.5 Solutions

1. 3**2.** 4**3.** -1**4.** -6**5.** 0**6.** -5

$$\textbf{7. } \frac{1}{2} \cdot \begin{pmatrix} 0 & -2 & 0 \\ -1 & 6 & 2 \\ -1 & 2 & 0 \end{pmatrix}$$

$$\textbf{8. } -\frac{1}{2} \cdot \begin{pmatrix} -4 & -2 & -4 \\ 0 & 0 & -1 \\ -2 & -2 & -2 \end{pmatrix}$$

$$\textbf{9. } 1 \cdot \begin{pmatrix} -1 & 1 & 0 \\ 0 & -2 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\textbf{10. } -\frac{1}{4} \cdot \begin{pmatrix} 4 & -4 & 2 \\ -4 & 2 & -2 \\ 0 & 0 & -2 \end{pmatrix}$$

$$\textbf{11. } \frac{1}{8} \cdot \begin{pmatrix} -4 & 2 & 4 \\ -8 & 0 & 4 \\ 4 & -2 & 0 \end{pmatrix}$$

$$\textbf{12. } -\frac{1}{4} \cdot \begin{pmatrix} 0 & -1 & 1 \\ 0 & -2 & -2 \\ 4 & 0 & 0 \end{pmatrix}$$

$$\textbf{13. } -\frac{1}{8} \cdot \begin{pmatrix} 0 & 0 & 4 \\ -4 & 0 & -2 \\ 0 & -4 & -2 \end{pmatrix}$$

$$\textbf{14. } \frac{1}{2} \cdot \begin{pmatrix} 1 & 0 & -1 \\ 2 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

$$\textbf{15. } -\frac{1}{2} \cdot \begin{pmatrix} -2 & -1 & 0 \\ 0 & 0 & -2 \\ -2 & -2 & 0 \end{pmatrix}$$

$$\textbf{16. } -\frac{1}{4} \cdot \begin{pmatrix} -4 & 0 & 0 \\ -2 & 0 & -2 \\ -2 & -2 & -2 \end{pmatrix}$$

$$\textbf{17. } -\frac{1}{2} \cdot \begin{pmatrix} 1 & 0 \\ -1 & -2 \end{pmatrix}$$

$$\textbf{18. } -\frac{1}{2} \cdot \begin{pmatrix} -1 & -2 \\ -1 & 0 \end{pmatrix}$$

19. $-\frac{1}{3} \cdot \begin{pmatrix} 1 & -1 \\ -1 & -2 \end{pmatrix}$

20. $-\frac{1}{4} \cdot \begin{pmatrix} 0 & -2 \\ -2 & 2 \end{pmatrix}$

21. $1 \cdot \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}$

22. $-1 \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

23. $\frac{1}{4} \cdot \begin{pmatrix} -2 & 1 \\ 0 & -2 \end{pmatrix}$

24. $-1 \cdot \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix}$

25. $\frac{1}{6} \cdot \begin{pmatrix} 2 & 2 \\ -2 & 1 \end{pmatrix}$

26. $\frac{1}{2} \cdot \begin{pmatrix} 2 & -2 \\ 1 & 0 \end{pmatrix}$

27. $x = -\frac{1}{12} \cdot \det \begin{pmatrix} 0 & 2 & 1 \\ 0 & 1 & 2 \\ -4 & -1 & 2 \end{pmatrix} = 1$

28. $y = -\frac{1}{9} \cdot \det \begin{pmatrix} 1 & -5 & 2 \\ -1 & 0 & 0 \\ -2 & 7 & -1 \end{pmatrix} = 1$

29. $z = \frac{1}{6} \cdot \det \begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 4 \\ 0 & 2 & -2 \end{pmatrix} = 0$

30. $x = -\frac{1}{3} \cdot \det \begin{pmatrix} -8 & -1 & -2 \\ 3 & 2 & -1 \\ -1 & -2 & 2 \end{pmatrix} = 1$

31. $z = \frac{1}{4} \cdot \det \begin{pmatrix} -1 & -1 & 1 \\ -1 & 1 & -3 \\ -2 & 2 & -2 \end{pmatrix} = -2$

32. $z = -\frac{1}{2} \cdot \det \begin{pmatrix} 2 & 1 & -4 \\ 1 & -2 & 4 \\ 1 & 2 & -6 \end{pmatrix} = -1$

33. $y = -\frac{1}{13} \cdot \det \begin{pmatrix} 2 & 0 & -2 \\ -1 & -1 & 0 \\ 2 & 3 & 1 \end{pmatrix} = 0$

34. $z = -\frac{1}{4} \cdot \det \begin{pmatrix} 2 & -1 & -4 \\ 2 & -2 & -4 \\ 1 & 1 & -2 \end{pmatrix} = 0$

35. $x = -\frac{1}{12} \cdot \det \begin{pmatrix} 4 & 0 & -2 \\ 6 & -2 & -2 \\ 4 & 0 & -2 \end{pmatrix} = 0$

36. $x = -\frac{1}{2} \cdot \det \begin{pmatrix} -2 & 1 & -2 \\ 0 & 0 & 2 \\ -1 & 0 & -1 \end{pmatrix} = 1$

37. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (0, 1, 0) + a \cdot (-1, 2, 1) : a \in \mathbb{R} \}$$

38. r.r.e.f.

$$\left(\begin{array}{ccc|c} 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (0, -2, -1) + a \cdot (1, 0, 0) : a \in \mathbb{R} \}$$

39. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & -2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (-2, 0, 0) + a \cdot (-2, 1, 0) + b \cdot (-1, 0, 1) : a, b \in \mathbb{R} \}$$

40. r.r.e.f.

$$\left(\begin{array}{ccc|c} 0 & 1 & 1 & -2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (0, -2, 0) + a \cdot (1, 0, 0) + b \cdot (0, -1, 1) : a, b \in \mathbb{R} \}$$

41. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 4 & -1 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (2, 0, 0) + a \cdot (-4, 1, 0) + b \cdot (1, 0, 1) : a, b \in \mathbb{R} \}$$

42. r.r.e.f.

$$\left(\begin{array}{ccc|c} 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (0, 2, 1) + a \cdot (1, 0, 0) : a \in \mathbb{R} \}$$

43. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & -1 & 1 \\ 0 & 1 & -4 & -1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (1, -1, 0) + a \cdot (1, 4, 1) : a \in \mathbb{R} \}$$

44. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & -3 & 2 \\ 0 & 1 & -3 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (2, 0, 0) + a \cdot (3, 3, 1) : a \in \mathbb{R} \}$$

45. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & -5 & -2 \\ 0 & 1 & -4 & -2 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (-2, -2, 0) + a \cdot (5, 4, 1) : a \in \mathbb{R} \}$$

46. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 2 & 0 & -2 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

All Solutions:

$$(x, y, z) =$$

$$\{ (-2, 0, -1) + a \cdot (-2, 1, 0) : a \in \mathbb{R} \}$$

47. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(0, 0, 1) = \emptyset$$

48. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & -4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(2, 0, 1) = \emptyset$$

49. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(-1, 0, -3) = \emptyset$$

50. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & 0 & -1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(-2, 0, 1) = \emptyset$$

51. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & -4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(-3, 0, -1) = \emptyset$$

52. r.r.e.f.

$$\left(\begin{array}{ccc|c} 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right)$$

$$f^{-1}(-11, 0, -4) = \emptyset$$

Multilinear Functions

6.4

6.4.1 Determinants are Multilinear	638
6.4.2 Bilinear Transformations	640
6.4.3 Trilinear Transformations	642
6.4.4 Bilinear Transformations by Tensors	646
6.4.5 Fast Evaluation of Bilinear Transformations	650
6.4.6 Derivatives as Multilinear Forms	652
6.4.7 More Examples via Wedge Product	662
6.4.8 Determinants by Wedges and Properties of Wedges	664
6.4.9 Exercises	672
6.4.10 Solutions	679

Questions to Guide Your Study:

- *What is a multilinear transformation?*
- *How does knowing that determinants are multilinear help us compute them?*
- *How do matrices represent bilinear transformations?*
- *How can we represent trilinear transformations?*
- *What are tensors and how can we use them to evaluate multilinear transformations?*
- *What is a fast technique for evaluating a bilinear transformation that comes from tensors?*
- *How can we write a multivariable polynomial in terms of multilinear transformations?*
- *What is the wedge product and how can we build multilinear transformations with it?*
- *How can we use wedge products to compute determinants?*

6.4.1 Determinants are Multilinear

The determinant of an $n \times n$ matrix is like a function where we have input n column vectors and then we get out a number in \mathbb{R} :

$$\det : \mathbb{R}^n \times \mathbb{R}^n \times \cdots \mathbb{R}^n \longrightarrow \mathbb{R}.$$

Notice that if we focus on one column at a time, the determinant function reduces to a cofactor function c_v^T which itself is a linear transformation. So, focusing on just one input column as the input, the determinant becomes additive and scalable. If we multiply one input column by a scalar, we have multiplied the determinant which is the output by that same scalar. If our input column is the sum of two input columns, then our determinant is the sum of the determinants using each part of the sum individually as the input. Yet the neat thing is that there are n separate input slots that do this: the determinant function itself is linear when restricted to any of its n input components. *The determinant function is multilinear.*

Multilinear Function

Suppose we take a function $f : V_1 \times V_2 \times \cdots \times V_n \rightarrow W$ where V_1, V_2, \dots, V_n , and W are all vector spaces over the same field. Further, take any $(v_1, v_2, \dots, v_n) \in V_1 \times V_2 \times \cdots \times V_n$. Suppose that the function given by

$$x \mapsto f(x, v_2, \dots, v_n)$$

and the function

$$x \mapsto f(v_1, x, \dots, v_n)$$

and all of the functions down to

$$x \mapsto f(v_1, v_2, \dots, x)$$

are all linear transformations. Further suppose that this same idea applies for any choice of (v_1, v_2, \dots, v_n) . Then, we say that f is *multilinear*.

Four Defining Properties of Determinants

The determinant function on $n \times n$ matrices is completely determined by the following facts:

- The determinant $\det : \underbrace{\mathbb{R}^n \times \cdots \mathbb{R}^n}_{n \text{ times}} \rightarrow \mathbb{R}$ is multilinear.
- Every time you swap the positions of two of the column entries, it multiplies the output by -1 .
- Every time there are two identical column entries the output is 0.
- The determinant of the identity matrix is 1.



Example 1. Let's think about how we can gain insight into computing the determinant of

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

by using the above facts about the function $\det : \mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$. First, we switch two entries and it multiplies the determinant by -1 :

$$\det(A) = \det \left(\begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \right) = -\det \left(\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} \right)$$

Next, we add a multiple of the first entry to the second entry:

$$-\det \left(\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix} - \frac{1}{2} \cdot \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} \right)$$

Does this change the output of the determinant? Notice that because \det is multilinear:

$$= -\det \left(\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} \right) - \underbrace{\left(-\frac{1}{2} \right) \cdot \det \left(\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} \right)}_{=0 \text{ because two entries repeat}}$$

Ok, so we know we can freely do this and not affect the determinant:

$$\det(A) = -\det \left(\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix} - \frac{1}{2} \cdot \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} \right) = -\det \left(\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} \right)$$

Next, we can factor scalars out of each vector input:

$$\det(A) = -\det \left(2 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, 4 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, 3 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right)$$

Since \det is multilinear, all 3 of these scalar multiples come out in front:

$$\det(A) = -2 \cdot 4 \cdot 3 \cdot \det \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right) = -24 \cdot \underbrace{\det(\text{id}_{3 \times 3})}_1 = -24.$$

Notice that we used all four defining properties. Any and all determinants can be found by using these defining properties. That is why they are called defining properties!

6.4.2 Bilinear Transformations

Even from the time we introduced matrix multiplication we have been dealing with multilinear functions—ones that have two inputs: a row and a column. Suppose that we take a matrix

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

Remember that this matrix describes *two different* linear transformations? One with a row interpretation and one with a column interpretation? We have only been focusing on each of those transformations one at a time. But if we thought about them both at the same time we would have a multilinear function—only now we would call it a *bilinear* function since it has *two* inputs.

Bilinear Transformation

A multilinear function of the form $f : V_1 \times V_2 \rightarrow W$ that is linear with respect to input from V_1 and also input from V_2 is called *bilinear*. It has *two* components in which it is linear individually.

Example 2. Let's use the matrix

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

and think of it as a bilinear function f . For instance:

$$(2 \ 1 \ 0) \cdot \begin{pmatrix} 2 & 0 \\ 1 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 4$$

We can think

$$f \left(\begin{pmatrix} 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) = 4.$$

Therefore, as we define f we write:

$$f : \underbrace{\mathbb{R}^3}_{\text{row}} \times \underbrace{\mathbb{R}^2}_{\text{column}} \rightarrow \mathbb{R}$$

Notice that

$$f \left(3 \cdot \begin{pmatrix} 2 & 1 & 0 \end{pmatrix}, 2 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) = 2 \cdot 3 \cdot f \left(\begin{pmatrix} 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) = 2 \cdot 3 \cdot 4 = 24$$

since scalars come out of both components. *This is just like as for determinants: if we multiply one column by 2 and another by 3, we have multiplied the whole determinant by $2 \cdot 3$.*

Just like matrices uniquely describe linear transformations by giving images of basis vectors, matrices also uniquely describe bilinear transformations (with codomain \mathbb{R})! Let's consider this last example to see how. Notice that

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}}_{\substack{\text{Only take first} \\ \text{row}}} \cdot \begin{pmatrix} 2 & 0 \\ 1 & -1 \\ 1 & 1 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{\substack{\text{Only take first} \\ \text{column}}} = 2$$

Realize that 2 is the entry in the first row and column of the matrix A . Similarly, if we want to get out the entry -1 , we would need to pinpoint the second row and the second column. So, we would compute:

$$\underbrace{\begin{pmatrix} 0 & 1 & 0 \end{pmatrix}}_{\substack{\text{Only take} \\ \text{second row}}} \cdot \begin{pmatrix} 2 & 0 \\ 1 & -1 \\ 1 & 1 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 0 \\ 1 \end{pmatrix}}_{\substack{\text{Only take} \\ \text{second column}}} = -1$$

Bilinear Transformations as Matrices

Suppose that $f : \mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}$ is a bilinear transformation. Then f can be described as a matrix A such that the entry a_{ij} (i th row and j th column) of A is the image $f(e_i, e_j)$.

Example 3. The determinant function $\det : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ is a bilinear function and so can be described by a matrix! We simply compute

$$\det(e_1, e_1) = \det \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = 0 \quad \det(e_1, e_2) = \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$$

$$\det(e_2, e_1) = \det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1 \quad \det(e_2, e_2) = \det \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = 0$$

Therefore, the matrix describing the determinant function for 2×2 matrices is:

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

Determinant Matrix for 2×2

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

Example 4. Let's try to use this matrix to take the determinant of a 2×2 matrix. Suppose that we have

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

Then, we are plugging in the columns $(2, -1)$ and $(3, 1)$ into the determinant function. Hence, we compute:

$$(2 \quad -1) \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix} = (2 \quad -1) \cdot \begin{pmatrix} 1 \\ -3 \end{pmatrix} = 2 \cdot 1 + (-1) \cdot (-3) = 5$$

6.4.3 Trilinear Transformations

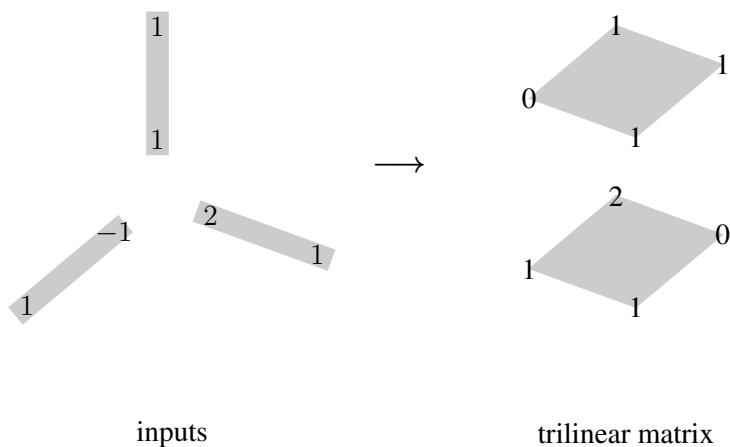
We have seen that a matrix can describe a bilinear transformation because we can think of it as a linear transformation in terms of row interpretation and in terms of a column interpretation. But, if we want something like a matrix to describe a *trilinear transformation*, one with *three inputs*, we will need something that not only has a row and a column interpretation—but a stacking interpretation as well adding another dimension to

our matrix! In fact we will be using the following principle:

Stacking Principle

For a trilinear matrix, we apply an input vector by taking a linear combination of what appears in planes perpendicular to the input vector. The coefficient to what is in that plane is the entry of the input vector that is in that same plane.

Here is an example:



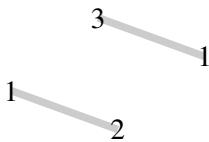
We will soon see that it does not matter which vector input we first begin with. Let's begin with the vector for which we will apply a *stacking interpretation*:



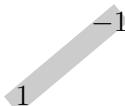
We multiply *each plane* by the corresponding component of this stacking vector and then add:

$$\begin{array}{c}
 1 \cdot \begin{array}{c} 1 \\ 0 \\ 1 \end{array} \\
 + \begin{array}{c} 1 \\ 2 \\ 0 \end{array} \\
 \hline
 1 \cdot \begin{array}{c} 3 \\ 1 \\ 2 \end{array}
 \end{array}$$

We are now left with a matrix which we will think of with parallel lines as follows:



We draw these so that we can input the vector:



to obtain:

$$\begin{array}{ccc} & \begin{matrix} 3 & -1 \\ + & \end{matrix} & = \\ \begin{matrix} 1 \\ 1 \\ 1 \end{matrix} & & \begin{matrix} -2 \\ 1 \end{matrix} \end{array}$$

Now, we apply the last input vector:



to obtain:

$$\begin{array}{ccc} & \begin{matrix} 2 \\ 1 \\ -2 \\ + \\ 1 \end{matrix} & = \\ & & -3 \end{array}$$

Recall that in a matrix multiplication like

$$(-1 \ 1) \cdot \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix},$$

it does not matter if we first multiply the two matrices on the left or the two on the right. This idea is called associativity of matrix multiplication. We can start evaluating at any part and then insert that result into the rest where it belongs and keep going. We should expect this to be true in our current situation. So we can start with any input and apply it to the three-dimensional matrix and obtain a two-dimensional matrix. Apply another input and obtain a one-dimensional matrix. Apply the last output and obtain a zero-dimensional matrix—a scalar.

Challenge for Reader: Try the same calculation above applying the same input vectors in a different order and verify that you obtain the same result.

A Fun Activity: The following SageMath exploration shows via an animation how we can use a three-dimensional matrix to compute the determinant of a 3×3 matrix.

SageMath Activity: 

Example 5. Yet, if we want to write everything on two-dimensional paper, let's do things a little differently. We can describe our trilinear form $f : \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ that we considered three-dimensionally above simply as

$$f : \underbrace{\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}}_{\text{First Level}} \quad \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}}_{\text{Second Level}}$$

Let's compute

$$f((1, -1), (3, 1), (1, 2))$$

First, let's input the last vector $(1, 2)$ by taking a linear combination of the levels:

$$1 \cdot \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} + 2 \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 3 & 2 \end{pmatrix}$$

Next let's input the other vectors as a row $\begin{pmatrix} 1 & -1 \end{pmatrix}$ and a column $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$ into what we have so far:

$$\underbrace{\begin{pmatrix} 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 \\ 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix}}_{\begin{pmatrix} -2 & 2 \end{pmatrix}} = -4.$$

Evaluate a Trilinear Transformation Using Matrix Levels

We can represent a trilinear transformation as a series of matrix levels. Suppose that the matrix levels are A_1, \dots, A_r where all of these matrices are $n \times m$ matrices. Then, we have a trilinear transformation $T : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^r$. To evaluate $T(v_1, v_2, v_3)$ we proceed as follows. Let $v_3 = (a_1, \dots, a_r)$. Then we take a linear combination of the matrix levels as follows:

$$M = a_1 A_1 + a_2 A_2 + \cdots + a_r A_r$$

Then, just compute:

$$\underbrace{v_1^T}_{\text{make } v_1 \text{ a row}} \cdot M \cdot \underbrace{v_2}_{\text{this is a column}}$$

6.4.4 Bilinear Transformations by Tensors

One could also think of computing the determinant of the 2×2 matrix

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

in the following way. The matrix we use has a row interpretation input of \mathbb{R}^2 and a column interpretation input of \mathbb{R}^2 . Let r_1 and r_2 be the standard basis vectors for the row interpretation input of \mathbb{R}^2 and let c_1 and c_2 be the standard basis vectors for the column interpretation input of \mathbb{R}^2 . Then, we have the following:

$$\begin{pmatrix} (r_1, c_1) \mapsto 0 & (r_1, c_2) \mapsto 1 \\ (r_2, c_1) \mapsto -1 & (r_2, c_2) \mapsto 0 \end{pmatrix}$$

The determinant bilinear function depends on the images of four separate things.

Question: how can we describe the matrix input A to the determinant function in terms of these four separate things?

First, the matrix A is two column vectors $\begin{pmatrix} 2 \\ -1 \end{pmatrix}$ and $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$. The first vector we turn and then accept as a row input $(2 \quad -1)$ into the determinant matrix. The second we keep as a column input. Then, we can write

$$\begin{pmatrix} 2 & -1 \end{pmatrix} = 2r_1 - r_2 \quad \begin{pmatrix} 3 \\ 1 \end{pmatrix} = 3c_1 + c_2$$

Therefore, our input into the determinant function is $(2r_1 - r_2, 3c_1 + c_2)$. Since the determinant is linear in each component, we have using just the linearity of the first component:

$$\det(2r_1 - r_2, 3c_1 + c_2) = 2 \det(r_1, 3c_1 + c_2) - \det(r_2, 3c_1 + c_2)$$

Doing this component-wise is what it means to be bilinear. Next we split this up using the second component:

$$\underbrace{3 \cdot 2 \det(r_1, c_1) + 2 \det(r_1, c_2)}_{2 \det(r_1, 3c_1 + c_2)} + \underbrace{(-3) \det(r_2, c_1) - \det(r_2, c_2)}_{-\det(r_2, 3c_1 + c_2)}$$

So, let's turn our multilinear function into something that is *just linear*. Create a new vector space whose four basis vectors are labeled as:

$$s_1 = (r_1, c_1), s_2 = (r_1, c_2), s_3 = (r_2, c_1), s_4 = (r_2, c_2)$$

Then, our matrix input A into the determinant function could have been labeled as:

$$6 \cdot (r_1, c_1) + 2 \cdot (r_1, c_2) - 3(r_2, c_1) - (r_2, c_2)$$

Then, our determinant function is simply replacing the four basis vectors by their images:

$$\det(A) = 6 \cdot \underbrace{0}_{\det(r_1, c_1)} + 2 \cdot \underbrace{1}_{\det(r_1, c_2)} - 3 \underbrace{-1}_{\det(r_2, c_1)} - \underbrace{0}_{\det(r_2, c_2)} = 5.$$

Now remember this is just the determinant bilinear transformation. *But every matrix can be thought of as a bilinear transformation.* So let's stick with this example and then extend what we find. How can we quickly go to this input? There is a secret: *just normal multiplication is bilinear since that is precisely what the distributive property is!* Hence, we can think of decomposing A —which can be written as $(2r_1 - r_2, 3c_1 + c_2)$ —by thinking of multiplication. We have a pairing of two vectors $2r_1 - r_2$ and $3c_1 + c_2$. Let's turn this one pairing into four pairings by using a multiplication distribution idea. To help us we think of this pairing idea (which behaves like multiplication) we use the symbol \otimes . We have:

$$(2r_1 - r_2, 3c_1 + c_2) = (2r_1 - r_2) \underset{\text{symbol for pairing}}{\underset{\otimes}{\text{ }}} (3c_1 + c_2)$$

Now, think of *FOIL* with this new symbol:

$$\underbrace{2r_1 \otimes 3c_1}_F + \underbrace{2r_1 \otimes c_2}_O + \underbrace{-r_2 \otimes 3c_1}_I + \underbrace{-r_2 \otimes c_2}_L$$

$$= 6r_1 \otimes c_1 + 2r_1 \otimes c_2 - 3r_2 \otimes c_1 - r_2 \otimes c_2$$

Then remembering $r_1 \otimes c_2 \mapsto 1$ and $r_2 \otimes c_1 \mapsto -1$ while $r_1 \otimes c_1$ and $r_2 \otimes c_2$ both map to 0, we have that this is:

$$= 2 \cdot 1 - 3(-1) = 5$$

as desired.

\otimes

The notation \otimes explained in the reading is read as “tensor” and is useful in turning a multilinear function into a linear one by creating a domain on which it actually can be linear and which describes the desired input into the multilinear function. It is a pairing idea and behaves just as if it were multiplication which distributes. Hence, one can expand things with it using FOIL.

$V \otimes_{\mathbb{R}} W$

Let V and W be \mathbb{R} -vector spaces. Then $V \otimes_{\mathbb{R}} W$ is the vector space whose basis is given as the symbols $a \otimes b$ where a is a basis vector of V and b is a basis vector of W . It is called the tensor product of V and W over \mathbb{R} .

What we did above was turn the *bilinear* determinant function $\det : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ into a *linear* function $\det : \mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{R}^2 \rightarrow \mathbb{R}$ whose domain is a **tensor product** and so that the following diagram is commutative:

$$\begin{array}{ccc} \mathbb{R}^2 \times \mathbb{R}^2 & \xrightarrow{(v,w) \mapsto (v \otimes w)} & \mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{R}^2 \\ & \searrow \text{det} & \downarrow \text{linear} \\ & & \mathbb{R} \end{array}$$

This linear map uniquely describes and determines our bilinear determinant map.



Example 6. Go back to our example of the matrix $\begin{pmatrix} 2 & 0 \\ 1 & -1 \\ 1 & 1 \end{pmatrix}$ describing a bilinear map. Remember

that we put two inputs in:

$$(2 \ 1 \ 0) \cdot \begin{pmatrix} 2 & 0 \\ 1 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 4$$

Let's think of this in terms of tensors. The matrix itself tells us the output of each pairing $r_i \otimes c_j$. So we just write the input

$$(2r_1 + 1r_2 + 0r_3, 1c_1 + 1c_2) = (2r_1 + 1r_2 + 0r_3) \otimes (1c_1 + 1c_2)$$

in terms of these in the tensor product of $\underbrace{\mathbb{R}^3}_{\text{rows}}$ and $\underbrace{\mathbb{R}^2}_{\text{columns}}$ over \mathbb{R} :

$$(2r_1 + 1r_2) \otimes (1c_1 + 1c_2) = 2 \underbrace{r_1 \otimes c_1}_{\downarrow 2} + 2 \underbrace{r_1 \otimes c_2}_{\downarrow 0} + \underbrace{r_2 \otimes c_1}_{\downarrow 1} + \underbrace{r_2 \otimes c_2}_{\downarrow -1} = 4$$

How is this useful? Well, we want a nice way to describe a multilinear function. Linear and bilinear functions can be described by a matrix. But as we saw above, trilinear functions have to have a three-dimensional array. What about an n -fold multilinear function where n is large. We cannot picture such a beast: we need n -dimensional paper! What tensors do is allow us to bring everything down to a simple linear transformation which can be described by a regular matrix!

Example 7. Let's write a basis for the vector space $\mathbb{R}^3 \otimes_{\mathbb{R}} \mathbb{R}^2$ and then write down a matrix that describes the linear transformation $\mathbb{R}^3 \otimes_{\mathbb{R}} \mathbb{R}^2 \rightarrow \mathbb{R}$ given by the bilinear transformation of the last example above. Then, we will use this matrix to perform the *same* computation we did in this last example. Essentially the basis is really just the 6 different positions in a 3×2 matrix. We can notate the positions as:

$$\begin{pmatrix} r_1 \otimes c_1 & r_1 \otimes c_2 \\ r_2 \otimes c_1 & r_2 \otimes c_2 \\ r_3 \otimes c_1 & r_3 \otimes c_2 \end{pmatrix}$$

where r_1 , r_2 and r_3 denote the standard basis vectors of \mathbb{R}^3 and c_1 and c_2 denote the standard basis vectors of \mathbb{R}^2 . The matrix itself that describes the bilinear transformation actually gives the destinations of all of these basis vectors:

$$\begin{pmatrix} r_1 \otimes c_1 \mapsto 2 & r_1 \otimes c_2 \mapsto 0 \\ r_2 \otimes c_1 \mapsto 1 & r_2 \otimes c_2 \mapsto -1 \\ r_3 \otimes c_1 \mapsto 1 & r_3 \otimes c_2 \mapsto 1 \end{pmatrix}$$

So, we can think:

$$\left(\begin{array}{cccccc} 2 & 0 & 1 & -1 & 1 & 1 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ r_1 \otimes c_1 & r_1 \otimes c_2 & r_2 \otimes c_1 & r_2 \otimes c_2 & r_3 \otimes c_1 & r_3 \otimes c_2 \end{array} \right)$$

In the last example, we saw that our input $((2, 1, 0), (1, 1)) \in \mathbb{R}^3 \times \mathbb{R}^2$ could be expressed as:

$$(2r_1 + 1r_2 + 0r_3, 1c_1 + 1c_2) = (2r_1 + 1r_2 + 0r_3) \otimes (1c_1 + 1c_2) = 2r_1 \otimes c_1 + 2r_1 \otimes c_2 + r_2 \otimes c_1 + r_2 \otimes c_2$$

We can input this as a column vector into our matrix we have just built as follows:

$$\underbrace{\begin{pmatrix} 2 & 0 & 1 & -1 & 1 & 1 \end{pmatrix}}_{\text{bilinear form linearized into a simple matrix function}} \cdot \begin{pmatrix} 2 \\ 2 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = r_1 \otimes c_1 + r_1 \otimes c_2 + r_2 \otimes c_1 + r_2 \otimes c_2 = 4.$$

We made a linear transformation that only has one input vector but that still describes the bilinear function that takes two inputs. The key was: *tensors* \otimes .

6.4.5 Fast Evaluation of Bilinear Transformations

Whether or not you followed our above discussion of \otimes , we have the following nice resulting idea:

Bilinear Matrix Entries

The result of a bilinear transformation $\mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}$ described by a $m \times n$ matrix is simply a linear combination of the entries of the matrix. Each scalar multiplier in this linear combination is just a product of an entry from the row vector input with an entry from the column vector input. To get the scalar multiple corresponding to a position in the i th row and j th column of the matrix simply multiply the i th entry of the row vector input with the j th entry of the column vector.

Understanding this can make computations fast. Here is an example:

Example 8. Let's discuss how to compute the following matrix product quickly:

$$(1 \ 1) \cdot \underbrace{\begin{pmatrix} 1 & 0 & -1 \\ 1 & 2 & 3 \end{pmatrix}}_A \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

The result is just an element of \mathbb{R} . Notice that the middle matrix A is a bilinear transformation and the two

vectors we are plugging in are on either side. Think of the entries of matrix A as being labeled as follows:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

Think: the first vector tells you about rows and the second vector tells you about columns. Since our vectors only have 1's or 0's, the only scalar multipliers we can have (being products of 1's and 0's) are simply 1's and 0's. Therefore, the result of this bilinear transformation *will just be a sum of some of the entries in the matrix!* Which ones? Look at the row vector: $\begin{pmatrix} 1 & 1 \end{pmatrix}$. Since there are 1's in both positions 1 and 2, we write:

$$a_1 \qquad \qquad \qquad a_2$$

Now, since there are 1's in positions 1 and 3 of the column vector $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, we extend a_1 by a_{11} and a_{13} and a_2 by a_{21} and a_{23} :



So our result will be the following sum of 4 of the entries of the matrix:

$$\underbrace{1}_{a_{11}} + \underbrace{-1}_{a_{13}} + \underbrace{1}_{a_{21}} + \underbrace{3}_{a_{23}} = 4$$

Example 9. Ok, let's try this when not all the entries of the input vectors are 1's. Suppose that we have the following computation:

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

We think:

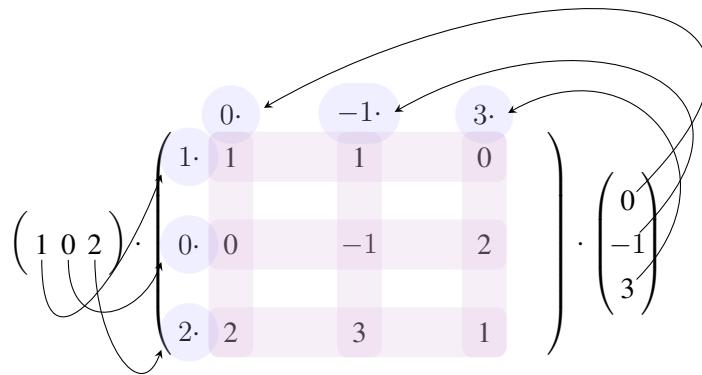
$$\begin{array}{ccc} \begin{array}{c} 1 \cdot a_1 \\ \cdot (-1) \\ \swarrow \end{array} & \begin{array}{c} 3 \\ \searrow \\ (1 \cdot 3)a_{13} \end{array} & \begin{array}{c} 2 \cdot a_3 \\ \cdot (-1) \\ \swarrow \end{array} \\ (1 \cdot (-1))a_{12} & & (2 \cdot (-1))a_{32} \\ & & \begin{array}{c} 3 \\ \searrow \\ (2 \cdot 3)a_{33} \end{array} \end{array}$$

So, the result is:

$$-\underbrace{1}_{a_{12}} + 3 \cdot \underbrace{0}_{a_{13}} - 2 \cdot \underbrace{3}_{a_{32}} + 6 \cdot \underbrace{1}_{a_{33}} = -1$$

Even though we are not thinking about it or even using the symbol \otimes , we are actually using tensor magic! After doing this a bit, this can even be done completely mentally and is a nice matrix multiplication skill to have!

Example 10. Another even simpler approach to the last example is to multiply the entries of the matrix as illustrated:



Multiplying, we arrive at:

$$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & -6 & 6 \end{pmatrix}$$

Now add the nonzero entries:

$$-1 + (-6) + 6 = -1.$$

6.4.6 Derivatives as Multilinear Forms

In this subsection we discuss functions $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ with the following properties:

- $D^n f$ exists for all n .
- $D^n f$ is a symmetric multilinear form (*this is defined in the reading below*).

The first derivative of a function $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ is a 1×2 matrix thought of as a function under the column interpretation. That is: $f(x, y) = x^3 - x \cdot y^2$ has a determinant as

$$Df : \begin{pmatrix} 3x^2 - y^2 & -2xy \end{pmatrix} \cdot \underbrace{\left(\begin{array}{c} \\ \end{array} \right)}_{\text{Input 1}}$$

Do you remember how we come up with it? The first column is the derivative with respect to x pretending that y is constant and the second column is the derivative with respect to y pretending that x is constant. How do we get the second derivative matrix? We take the transpose of this first derivative matrix:

$$\underbrace{\left(\begin{array}{c} \\ \end{array} \right)}_{\text{Input 1}} \begin{pmatrix} 3x^2 - y^2 \\ -2xy \end{pmatrix}$$

so that we think of it as a function of row vectors. Then as a column, we take derivatives with respect to x and then y treating the other variable constant:

$$\text{Derivative with } x \text{ variable and } y \text{ constant: } \begin{pmatrix} 6x \\ -2y \end{pmatrix} \quad \text{Derivative with } x \text{ variable and } y \text{ constant: } \begin{pmatrix} -2y \\ -2x \end{pmatrix}$$

Just like as for the first derivative, we arrange our results into two columns and this is the second derivative matrix with two inputs:

$$D^2f : \underbrace{\left(\begin{array}{c} \\ \end{array} \right)}_{\text{Input 1}} \cdot \begin{pmatrix} 6x & -2y \\ -2y & -2x \end{pmatrix} \cdot \underbrace{\left(\begin{array}{c} \\ \end{array} \right)}_{\text{Input 2}}$$

Notice that our tendency is to always read the new input in column interpretation. We put these inputs there so we realize that the second derivative is a *bilinear* function. But now, *how do we do a third derivative?* The third derivative will be a *trilinear* function which will actually tell us a lot about our original function thought of in this way. We will be able to finally see how the inputs are useful. What we will do is to leave input 1 in a row interpretation and input 2 in a column interpretation and then put our new input 3 in a stacking interpretation. The first level will be the derivative with respect to x while keeping y constant and the second level will be the derivative with respect to y while keeping x constant. We are taking partial derivatives of all the components of the second derivative matrix:

$$D^3f : \underbrace{\begin{pmatrix} 6 & 0 \\ 0 & -2 \end{pmatrix}}_{\text{First Level: partial with respect to } x} \quad \underbrace{\begin{pmatrix} 0 & -2 \\ -2 & 0 \end{pmatrix}}_{\text{Second Level: partial with respect to } y}$$

$$\begin{array}{c} \text{Row: } \left(\begin{array}{c} \\ \end{array} \right) \\ \text{Input 1} \end{array} \quad \begin{array}{c} \text{Column: } \left(\begin{array}{c} \\ \end{array} \right) \\ \text{Input 2} \end{array} \quad \begin{array}{c} \text{Stacking: } \left(\begin{array}{c} \\ \end{array} \right) \\ \text{Input 3} \end{array}$$

Let's plug in the vector (x, y) for *every input* of this trilinear form and see what happens:

$$\begin{array}{c} \text{Row: } \left(\begin{array}{cc} x & y \\ \hline \text{Input 1} \end{array} \right) \\[10pt] \text{Column: } \left(\begin{array}{c} x \\ y \\ \hline \text{Input 2} \end{array} \right) \\[10pt] \text{Stacking: } \left(\begin{array}{c} x \\ y \\ \hline \text{Input 3} \end{array} \right) \end{array}$$

First, we plug in input 3 by taking a linear combination of the levels:

$$x \cdot \begin{pmatrix} 6 & 0 \\ 0 & -2 \end{pmatrix} + y \cdot \begin{pmatrix} 0 & -2 \\ -2 & 0 \end{pmatrix} = \begin{pmatrix} 6x & -2y \\ -2y & -2x \end{pmatrix}$$

Wait, when we plug in (x, y) into the third input we get the second derivative matrix! How could we notate this? We could say thinking of $D^3 f : \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ as a trilinear form that:

$$D^3 f(-, -, (x, y)) = D^2 f(-, -)$$

where we use $-$ to signify that we still have yet to plug in input 1 and input 2. Ok, now let's plug in (x, y) for input 2 in $D^3 f(-, -, (x, y)) = D^2 f(-, -)$ (which is a column interpretation) to have:

$$D^3 f(-, (x, y), (x, y)) : \underbrace{\left(\begin{array}{c} \\ \end{array} \right)}_{\text{Input 1}} \cdot \begin{pmatrix} 6x & -2y \\ -2y & -2x \end{pmatrix} \cdot \left(\begin{array}{c} x \\ y \end{array} \right) = \underbrace{\left(\begin{array}{c} \\ \end{array} \right)}_{\text{Input 1}} \cdot \begin{pmatrix} 6x^2 - 2y^2 \\ -4xy \end{pmatrix}$$

Note that this is twice the transpose of the first derivative! Now, let's plug in (x, y) for input 1 which is a row interpretation:

$$D^3 f((x, y), (x, y), (x, y)) : \underbrace{\left(\begin{array}{cc} x & y \\ \hline \text{Input 1} \end{array} \right)}_{\text{Input 1}} \cdot \begin{pmatrix} 6x^2 - 2y^2 \\ -4xy \end{pmatrix} = 6x^3 - 6xy^2$$

Notice that the formula for $D^3 f((x, y), (x, y), (x, y))$ is 6 times the formula for f . It is like we are taking an antiderivative when we plug more vectors (x, y) into our trilinear form. This is not far from the truth. To see what is happening, we need:

Theorem 6.4.1 Product/Boxing Rule for Derivatives

Suppose that we have a function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ which is described by a matrix expression. In this expression may be multiple occurrences of the n different input variables. Split the occurrences in two parts. The same variable may be present in both parts 1 and 2. Yet, if we take the derivative matrix with respect to our n variables *assuming that everything in part 2 behaves like a constant* and add to that the derivative matrix that *assumes that everything in part 1 is a constant* we arrive at the matrix for Df . *If we have 3 parts, it works the same way!*

Proof. A proof in a special case is given as we prove the minimality of the least squares solution in section 5.4. We will give the general idea here. The idea is that we make a function g with twice as many variables. The function g is the same as f except we made everything in part 1 as being from one copy of the variables and in part 2 from the other copy. We then precompose g with a function h which makes the variables come back to equal each other as they should. That is, $g \circ h = f$. The derivative Dh is just two identity matrix blocks in a column. The derivative Dg is two blocks in a row. The first block is the derivative only using part 1 variables with part 2 held constant. The second block is the derivative only using part 2 variables with part 1 held constant. The chain rule and matrix block multiplication then yields the result. \square

Keep in mind that no matter how many times we plug (x, y) in to each input or not, all of our derivatives and multilinear forms can be thought of as functions with domain \mathbb{R}^2 and codomain \mathbb{R}^m where m is the number of entries some multidimensional array. In this way, what we get are functions of x and y . Sometimes different matrix expressions *yield the same function!*

In addition to the product rule, we will use the idea that our multilinear forms taken from derivatives are *symmetric* which means that as *functions* we have the following equalities (thinking of these as *functions* instead of matrices so that interpretation does not matter):

$$D^3 f(-, -, (x, y)) = D^3 f((x, y), -, -) = D^3 f(-, (x, y), -)$$

$$D^3 f(-, (x, y), (x, y)) = D^3 f((x, y), -, (x, y)) = D^3 f((x, y), (x, y), -)$$

$$D^2 f(-, (x, y)) = D^2 f((x, y), -)$$

Essentially this means that the bilinear function $D^2 f$ is represented by a *symmetric matrix* and the trilinear function is represented by a *symmetric three-dimensional array of numbers!*

Symmetric Multilinear Form

A multilinear form $f : V \times V \times \cdots \times V \rightarrow W$ is symmetric if when we plug in the same vector $v \in V$ into k of the inputs, we get the same *function* back no matter which k inputs we put v into. A function can be the same even if interpretations in a matrix representation switch. For instance $v \mapsto A \cdot v$ is the same function as $v^T \mapsto v^T \cdot A^T$. One way we write the vectors as columns and in the other as rows. But they still are the same function!

Ok, let's picture our function $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ above by the following rule:

$$f : (x, y) \mapsto \frac{1}{6} \cdot D^3 f((x, y), (x, y), (x, y))$$

Let's use the product rule with three parts:

$$\frac{1}{6} \cdot D^3 f(\underbrace{(x, y)}_{\text{part 1}}, \underbrace{(x, y)}_{\text{part 2}}, \underbrace{(x, y)}_{\text{part 3}})$$

Suppose that we take the case when the variables come from Part 1 and the other parts are held as constants. Realize that we are plugging (x, y) as a vector into a “constant” matrix $\frac{1}{6} \cdot D^3 f(\underbrace{\quad}_{\text{part 1}}, \underbrace{(x, y)}_{\text{part 2}}, \underbrace{(x, y)}_{\text{part 3}})$. This means we are assuming that our function is a *linear transformation*. A derivative simply gives the matrix that best approximates the function at a point. If the function is a linear transformation described by a matrix, the derivative function itself is given by the matrix describing the function. That is, the derivative with respect to part 1 is simply found by *removing the input to part 1* because that gives us the matrix function that describes the derivative: $\frac{1}{6} \cdot D^3 f(-, (x, y), (x, y))$. Similarly the derivative with respect to part 2 is $\frac{1}{6} \cdot D^3 f((x, y), -, (x, y))$ and with respect to part 3 is $\frac{1}{6} \cdot D^3 f((x, y), (x, y), -)$. All three of these “partial” derivatives represent the *same* function by our symmetry principle of derivatives. The product rule tells us the the first derivative is the sum of these three “partial” derivatives which are the same. Hence, the function that is given by

$$(x, y) \mapsto \underbrace{\frac{1}{2}}_{3 \cdot \frac{1}{6}} \cdot D^3 f(-, (x, y), (x, y))$$

is the first derivative. We could have chosen to remove any component in the way we wrote this due to symmetry—but out of convenience, we chose the first.

Now, to take the next derivative, we have only part 2 and part 3: $\frac{1}{2} \cdot D^3 f(-, \underbrace{(x, y)}_{\text{part 2}}, \underbrace{(x, y)}_{\text{part 3}})$. The derivative with respect to each is found by removing an input. Then by symmetry when we add the two results together we get the second derivative as:

$$\frac{1}{2} \cdot D^3 f(-, -, (x, y)) + \frac{1}{2} \cdot D^3 f(-, (x, y), -) = D^3 f(-, -, (x, y))$$

When we take the next derivative, there is only one part, and we simply remove the input so that the third derivative of our function (as desired) is:

$$D^3 f(_, _, _)$$

That is, we successfully used the product rule to find that the third derivative of f was precisely $D^3 f$ if we wrote the formula for f as $(x, y) \mapsto \frac{1}{6} \cdot D^3 f((x, y), (x, y), (x, y))$.

In fact, $x \rightarrow x^3$ is a trilinear form $g : \mathbb{R} \times \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ given by three-dimensional array of numbers *with only one number* such that x plugged into each input. When we take derivatives we get: $x^3 \rightarrow 3x^2 \rightarrow 6x \rightarrow 6$. Notice that we have multiplied by 6. Similarly, x^2 is a bilinear form and taking derivatives, we have: $x^2 \rightarrow 2x \rightarrow 2$ where we multiply by 2. The function f we gave above was like a constant trilinear form with (x, y) plugged in three times. It was like: $\underbrace{\text{constant}}_{\text{trilinear matrix}}((x, y), (x, y), (x, y))$. Therefore, taking a derivative just consisted of removing an input (x, y) (*going down one power*) and then multiplying by 3. If we start with a “trilinear constant matrix” (with nothing plugged in) and start taking antiderivatives, we divide by 1, then by 2 and then by 3.

Taking an antiderivative is just plugging in another (x, y) vector and dividing by a constant.

This very idea allows us to write multivariable polynomial approximations to functions (multivariable Taylor series).

Realize that if two functions f and g have the same derivative function, then their difference $f - g$ has a derivative matrix function of zero. The only way to have a function with a zero derivative matrix when we take partial derivatives is for $f - g$ to be a constant function. This means that even now in our current setting, there is a unique antiderivative of a derivative function *up to a constant shift*. So, the change of the antiderivative of a derivative is well-defined—it does not depend on the constant matrix shift. This just cancels out in the difference.

So, suppose that f as a function has derivative Df . Then $f(x, y) - f(0, 0)$ is the change of the antiderivative of Df as the input to f changes from $(0, 0)$ to (x, y) . Thinking of Df as a derivative matrix, let $Df_{(a,b)}$ mean the derivative matrix where we replace all x 's in that matrix by a 's and all y 's by b 's. Then the change of $Df_{(x,y)}$ from $(0, 0)$ to (a, b) can be denoted as: $Df_{(a,b)} - Df_{(0,0)}$.

Let the symbol $\int_{(0,0)}^{(x,y)} \square$ be used to denote the change of the antiderivative of \square . Now we can write:

$$f : (x, y) \mapsto f(0, 0) + \int_{(0,0)}^{(x,y)} Df$$

Notice that we are taking the change of the antiderivative of Df between *two fixed points* $(0, 0)$ and (x, y) . This means that we need *new variable names* for the variables that occur in the matrix entries of Df . What about x_1 and y_1 ? Using this idea, we iterate this process for Df thought of as a function $(x_1, y_1) \mapsto (\text{something})$:

$$Df : (x_1, y_1) \mapsto Df_{(0,0)} + \int_{(0,0)}^{(x_1,y_1)} D^2 f$$

Now, nest such a process repeatedly as follows:

$$f : (x, y) \mapsto f(0, 0) + \int_{(0,0)}^{(x,y)} \left(Df_{(0,0)} + \int_{(0,0)}^{(x_1,y_1)} \left(D^2f_{(0,0)} + \int_{(0,0)}^{(x_2,y_2)} D^3f_{(0,0)} + \dots \right. \right)$$

Assuming that eventually the \dots has a negligible effect, we get a good approximation for f just by stopping somewhere. We think of $D^3f_{(0,0)}$ as being a constant trilinear form *with no vectors plugged in*. Yes—we write $D^3f_{(0,0)}$ so it looks like we are setting $x_3 = 0$ and $y_3 = 0$ in the *entries* of the trilinear matrix—but there are no vectors we are plugging in. It is just the trilinear matrix! Similarly, $D^2f_{(0,0)}$ is a constant bilinear matrix with no vectors multiplied to it and so forth.

If we were to multiply a zero vector to any of these multilinear matrices, we would get a zero object (number, matrix,etc.) back. This fact tells us that change of any of these from $(0, 0)$ to (x_k, y_k) (for the relevant index k) is simply the multilinear matrix itself with (x_k, y_k) plugged in.

The antiderivative with x_k and y_k plugged into the matrix entries *is the same as the change of the antiderivative* from the input $(0, 0)$ to the input (x_k, y_k)

So really, we are just taking antiderivatives in the above nesting which we can write as follows:

$$f : (x, y) \mapsto f(0, 0) + \int_{(0,0)}^{(x,y)} Df_{(0,0)} + \int_{(0,0)}^{(x,y)} \int_{(0,0)}^{(x_1,y_1)} D^2f_{(0,0)} + \int_{(0,0)}^{(x,y)} \int_{(0,0)}^{(x_1,y_1)} \int_{(0,0)}^{(x_2,y_2)} D^3f_{(0,0)} + \dots$$

So, we take the “third” antiderivative of the constant trilinear form $D^3f_{(0,0)}$ (*after all three antiderivative processes our variables are back to x and y*). Then, we add that to the second antiderivative of $D^2f_{(0,0)}$ (*which again is in terms of x and y*). To finish us off, we add on the first antiderivative of $Df_{(0,0)}$ and then the output of f at $(0, 0)$. The result? A good approximation for the function f itself. If \dots is eventually zero, then we have not just approximation, but equality.

A change of antiderivative $\int_{(0,0)}^{(x,y)}$ is equal to a multilinear form with vectors (x, y) plugged in!

Hence, we arrive at the following theorem.

Theorem 6.4.2 Multivariable Taylor Series (centered at $(0, 0)$)

Let $D^m f_{(0,0)}$ signify that we plug in $x = 0$ and $y = 0$ into the multilinear matrix entries. *It does not refer to a vector that we multiply the multilinear matrix by!*

$$f(x, y) = \underbrace{f(0, 0)}_{\text{constant part}} + \underbrace{Df_{(0,0)}((x, y))}_{\text{linear part}} + \underbrace{\frac{1}{2!} D^2f_{(0,0)}((x, y), (x, y))}_{\text{bilinear part}} + \underbrace{\frac{1}{3!} D^3f_{(0,0)}((x, y), (x, y), (x, y))}_{\text{trilinear part}} + \dots$$

Multivariable Polynomial

A multivariable polynomial is a linear combination of products of variables.

Total Degree

The total degree of a multivariable polynomial is the highest sum of exponents that occur among all the individual terms.

Example 11. The expression $xy^2 - 2xyz^4$ is a multivariable polynomial. The first term x^1y^2 has a sum of exponents: $1 + 2 = 3$. The second term $2x^1y^1z^4$ has a sum of exponents $1 + 1 + 4 = 6$. The highest sum is 6. Therefore, the total degree 6 of this multivariable polynomial is 6.

Identifying Multilinear Parts

Any term of a multivariable polynomial whose exponents add to 2 like xy is in the bilinear part. If they add to 3 like xy^2 they are in the trilinear part and so forth.



Example 12. Let's identify the different multilinear parts of the expression for the following function and write down a multilinear matrix for each part:

$$f(x, y) = 2 + x + y + x^2 + xy + y^3$$

Using the definition of multilinear parts by adding exponents of variables in terms we have:

$$\underbrace{2}_{\text{constant part}} + \underbrace{x + y}_{\text{linear part}} + \underbrace{x^2 + xy}_{\text{bilinear part}} + \underbrace{y^3}_{\text{trilinear part}}$$

Notice that the matrix for Df is

$$Df : \begin{pmatrix} 1 + 2x + y & 1 + x + 3y^2 \end{pmatrix}$$

If we plug in $x = 0$ and $y = 0$, we get:

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

We could have gotten this matrix more quickly by *just looking at the linear part*: We can think of a function $g(x, y) = x + y$ describing the linear part and find its derivative matrix. We get $\begin{pmatrix} 1 & 1 \end{pmatrix}$ so that the linear part

of $f(x, y)$ is given by:

$$\begin{pmatrix} 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

For the bilinear part, let's move more quickly. Instead of computing $D^2 f$, we can think of a function $h(x, y) = x^2 + xy$ that *just describes the bilinear part* and find its second derivative:

$$x^2 + xy \longrightarrow \begin{pmatrix} 2x + y & x \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

Therefore, the bilinear part of $f(x, y)$ is expressible as:

$$\frac{1}{2} \cdot \begin{pmatrix} x & y \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

For the trilinear part, it suffices to consider a function $k(x, y) = y^3$ and take three derivatives:

$$y^3 \longrightarrow \begin{pmatrix} 0 & 3y^2 \\ 0 & 6y \end{pmatrix} \longrightarrow \left(\underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}}_{\text{first level (partial } x\text{)}} \quad \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 6 \end{pmatrix}}_{\text{second level (partial } y\text{)}} \right)$$

Divide this trilinear matrix by $3! = 6$ to have:

$$\left(\underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}}_{\text{first level (partial } x\text{)}} \quad \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{\text{second level (partial } y\text{)}} \right)$$

The trilinear part is obtained by plugging in:

Row: $\underbrace{\begin{pmatrix} x & y \end{pmatrix}}_{\text{Input 1}}$	Column: $\underbrace{\begin{pmatrix} x \\ y \end{pmatrix}}_{\text{Input 2}}$	Stacking: $\underbrace{\begin{pmatrix} x \\ y \end{pmatrix}}_{\text{Input 3}}$
--	--	--

Example 13. Let's come up with a total degree 2 multivariable approximation for $f(x, y) = e^{x+y}$. We just need:

$$f(x, y) \approx \underbrace{f(0, 0)}_{\text{constant part}} + \underbrace{Df_{(0,0)}((x, y))}_{\text{linear part}} + \underbrace{\frac{1}{2!} D^2 f_{(0,0)}((x, y), (x, y))}_{\text{bilinear part}}$$

We find derivatives:

$$e^{x+y} \longrightarrow \begin{pmatrix} e^{x+y} & e^{x+y} \\ e^{x+y} & e^{x+y} \end{pmatrix} \longrightarrow \begin{pmatrix} e^{x+y} & e^{x+y} \\ e^{x+y} & e^{x+y} \end{pmatrix}$$

Plugging in $x = 0$, $y = 0$ to each of these, we get $f(0, 0) = 1$, $Df : \begin{pmatrix} 1 & 1 \end{pmatrix}$, $D^f : \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Therefore,

$$f(x, y) \approx 1 + \begin{pmatrix} 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \frac{1}{2} \cdot \begin{pmatrix} x & y \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

$$f(x, y) \approx 1 + x + y + \frac{1}{2} \cdot (x^2 + 2xy + y^2)$$

Note: we have assumed that derivative multilinear forms are symmetric. But look at any bilinear part of a multivariable polynomial $ax^2 + bxy + cy^2$. It can be written as the result of a symmetric bilinear matrix with the vector (x, y) plugged in as a row and a column if we just think of splitting the coefficient b of xy in half to get:

$$ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \cdot \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

But then the second derivative of this matrix expression using the product rule ends up being:

$$2 \cdot \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

which is symmetric. So really, if there is any symmetric bilinear representation at all, then the second derivative itself will also be symmetric!

Theorem 6.4.3

Any function defined by a multivariable Taylor series has mixed partial derivatives which are equal. That is, $f_{xy} = f_{yx}$.

Before leaving this topic, we mention one important note that will become useful as we look at applications of something called “eigenvalues” (still to come). That is, if we use $f(x, y) \approx$ (Taylor Polynomial), near $(0, 0)$ and we know that the linear part of the Taylor polynomial is just 0, then the bilinear part takes the lead in the approximation after $f(0, 0)$. That is, the bilinear part approximates the change $f(x, y) - f(0, 0)$.

The bilinear part takes the lead over the trilinear part and any other part. To give us some intuition on this

point, think of a single variable polynomial $3x^4 + 5x^3 + 4x^2$. When x is small, $(\frac{1}{x})$ is huge. Think of inserting $(\frac{1}{x})$ for x , think of our polynomial as

$$3 \cdot \left(\frac{1}{x}\right)^4 + 5 \cdot \left(\frac{1}{x}\right)^3 + 4 \cdot \left(\frac{1}{x}\right)^2 = \frac{3 + 5x + 4x^2}{x^4}$$

and think of x as being very large. Notice that compared to x^4 , the contribution of $3 + 5x$ is very negligible if x is large. That is if x is 10^{100} then x^4 is 10^{300} times greater than x . Hence, we think that our polynomial is close to $\frac{4x^2}{x^4}$ for large x . Now if we go back and replace $(\frac{1}{x})$ with x and think of x as small again, we get the same approximation. What is negligible? The higher powers. That is:

When x is close to zero, the smaller the power, the greater the contribution of the term. The smaller power gives the leading term for behavior near $x = 0$. *Just backwards from $x \rightarrow \infty$.*

Practical Interpretation of Bilinear part of a Multivariable Polynomial

Assuming that the first derivative is a zero matrix, the bilinear part of a multivariable polynomial approximates the change of the function from the point $(0, 0)$ to (x, y) . *We have an analogous statement assuming all previous derivative matrices are the zero matrix up to a specified derivative.*

6.4.7 More Examples via Wedge Product

We will let x , y , and z to refer to the different coordinate positions of a vector such as $(\begin{smallmatrix} 1 & 3 & 2 \\ x & y & z \end{smallmatrix})$ in \mathbb{R}^3 . First, let's define:

dx

Define $dx : \mathbb{R}^3 \rightarrow \mathbb{R}$ to be a function which just picks out the x coordinate of a vector.

For instance, we have:

$$dx(3, -1, 5) = 3.$$

The matrix for dx under a column interpretation of multiplication is simply the row matrix $(1 \ 0 \ 0)$. We say that dx as a row vector is an element of what we call the *dual space* to \mathbb{R}^3 :

Dual Space

The dual space of a \mathbb{R} -vector space V is defined to vector space consisting of linear transformations $V \rightarrow \mathbb{R}$. If V is represented by column vectors, then the dual space is just matrices which are row vectors. The dual space is notated as V^* or $\text{Hom}_{\mathbb{R}}(V, \mathbb{R})$.

Sometimes the vectors in this dual vector space are called *dual vectors* or even *covectors*. But this is extraneous terminology if we can simply see that dx just picks out an x -coordinate. Similarly to how we define dx , we can define dy and dz . These in their own right are linear transformations.

Now, we introduce a way of putting these linear transformations together to produce bilinear functions. These bilinear functions are actually very useful. They can help us find areal projects of 3-dimensional objects, surface areas, understand vector cross products, and much much more. A lot of what is taught in a multivariable calculus class can be simplified with such bilinear functions.

Wedge Product

We define $dx \wedge dy$ to be the bilinear function $\mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$ that computes the 2×2 determinant of the top part of two vectors. That is, pick out the x coordinates as the top row and the y coordinates as the bottom row. So if $v = (v_1, v_2, v_3)$ and $w = (w_1, w_2, w_3)$, then

$$dx \wedge dy(v, w) = \det \begin{pmatrix} v_1 & w_1 \\ v_2 & w_2 \end{pmatrix}.$$

$$(v \quad w) = \begin{pmatrix} v_1 & w_1 \\ v_2 & w_2 \\ v_3 & w_3 \end{pmatrix}$$

$$dx \wedge dy(v, w) = \det \begin{pmatrix} v_1 & w_1 \\ v_2 & w_2 \end{pmatrix}.$$

We define $dy \wedge dx$ to simply be the determinant of the same submatrix only with x and y values switched.

Example 14. Let $v = (1, 4, 5)$ and $w = (-1, 1, 0)$. Then, we think:

$$(v \quad w) = \begin{pmatrix} 1 & -1 \\ 4 & 1 \\ 5 & 0 \end{pmatrix}$$

Hence,

$$dx \wedge dy(v, w) = \det \begin{pmatrix} 1 & -1 \\ 4 & 1 \end{pmatrix} = 5.$$

To compute $dy \wedge dx$, we take the y -coordinates as the first row and the x -coordinates as the second row. Quite literally we are thinking first pick out y (i.e. dy) and then pick out dx (i.e. dx):

$$dy \wedge dx(v, w) = \det \begin{pmatrix} 4 & 1 \\ 1 & -1 \end{pmatrix} = -5.$$

Theorem 6.4.4

$$dy \wedge dx(v, w) = -dx \wedge dy(v, w)$$

Example 15. Similarly, we can compute something like

$$dz \wedge dx(v, w)$$

for the same v and w as in the last example when we think:

$$(v \quad w) = \begin{pmatrix} & \\ & \\ & \\ \left(\begin{matrix} 1 & -1 \\ 4 & 1 \\ 5 & 0 \end{matrix} \right) & \end{pmatrix} \quad \curvearrowright$$

Therefore,

$$dz \wedge dx(v, w) = \det \begin{pmatrix} 5 & 0 \\ 1 & -1 \end{pmatrix} = -5.$$

6.4.8 Determinants by Wedges and Properties of Wedges

Consider the following wedge product of covectors $dx : \mathbb{R}^3 \rightarrow \mathbb{R}$, $dy : \mathbb{R}^3 \rightarrow \mathbb{R}$, and $dz : \mathbb{R}^3 \rightarrow \mathbb{R}$:

$$dx \wedge dy \wedge dz : \mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$$

It should make sense that this *trilinear* function *just computes the determinant* of a 3×3 matrix when we plug in the columns. This is because we are taking the row in the x position first, then the row in the y position and

then the row in the z position: *this is the whole matrix as is!* Suppose for instance that we have a matrix:

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

The determinant of this matrix is -3 . Hence,

$$dx \wedge dy \wedge dz ((1, 1, 1), (2, 0, 1), (0, -1, 1)) = -3.$$

As a trilinear function, it takes addition and scalar multiplication in each input and lets it pass to the output. In this subsection, *we will develop some of the properties* of \wedge . In particular, we will see that it shares a lot of characteristic as the symbol \otimes in how it interacts. Remember that \otimes is a pairing idea? The symbol \wedge combines \otimes (which can be put in the input of a trilinear functions) and a determinant function into one nice succinct idea. We will have to play with some ideas to see how this will pan out.

If we let f represent our trilinear function of taking the determinant, a_i represents a basis for the first vector input, b_i the second and c_i the third, then:

$$f((1, 1, 1), (2, 0, 1), (0, -1, 1)) = f(\underbrace{a_1 + a_2 + a_3}_{(1, 1, 1)}, \underbrace{2b_1 + b_3}_{(2, 0, 1)}, \underbrace{-c_2 + c_3}_{(0, -1, 1)})$$

To pass addition and scalar multiplication to the output, we first need to think of f as being linear. To do this, we need to use the symbol \otimes and think of it as the “multiplication:”

$$\begin{aligned} (a_1 + a_2 + a_3) \otimes (2b_1 + b_3) \otimes (-c_2 + c_3) &= a_1 \otimes 2b_1 \otimes (-1)c_2 + a_1 \otimes (2)b_1 \otimes c_3 + a_1 \otimes b_3 \otimes (-1)c_2 + a_1 \otimes b_3 \otimes c_3 \\ &\quad + a_2 \otimes 2b_1 \otimes (-1)c_2 + a_2 \otimes (2)b_1 \otimes c_3 + a_2 \otimes b_3 \otimes (-1)c_2 + a_2 \otimes b_3 \otimes c_3 \\ &\quad + a_3 \otimes 2b_1 \otimes (-1)c_2 + a_3 \otimes (2)b_1 \otimes c_3 + a_3 \otimes b_3 \otimes (-1)c_2 + a_3 \otimes b_3 \otimes c_3 \end{aligned}$$

Now, we can apply the determinant function f just as we would any linear function:

$$\begin{aligned} f(a_1 + a_2 + a_3) \otimes (2b_1 + b_3) \otimes (-c_2 + c_3) &= \\ f(a_1 \otimes 2b_1 \otimes (-1)c_2) + f(a_1 \otimes (2)b_1 \otimes c_3) + f(a_1 \otimes b_3 \otimes (-1)c_2) + f(a_1 \otimes b_3 \otimes c_3) &+ \\ f(a_2 \otimes 2b_1 \otimes (-1)c_2) + f(a_2 \otimes (2)b_1 \otimes c_3) + f(a_2 \otimes b_3 \otimes (-1)c_2) + f(a_2 \otimes b_3 \otimes c_3) &+ \\ f(a_3 \otimes 2b_1 \otimes (-1)c_2) + f(a_3 \otimes (2)b_1 \otimes c_3) + f(a_3 \otimes b_3 \otimes (-1)c_2) + f(a_3 \otimes b_3 \otimes c_3) &+ \end{aligned}$$

So, we are adding up a lot of determinants. Let’s look at one: $f(a_1 \otimes b_3 \otimes c_3)$. The symbol \otimes really is just like commas—how to put the inputs into tuples. It simply reminds us that “pairing” or rather “tupling” of inputs

can be thought of via a multiplication distributing idea before we can pass addition and scalar multiplication freely to the output as with a linear function. So, then:

$$f(a_1 \otimes b_3 \otimes c_3) = f(a_1, b_3, c_3) = f((1, 0, 0), (0, 0, 1), (0, 0, 1))$$

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

Notice that there is a row of zeros. This happens when a subscript is repeated. When subscripts do not repeat, the determinants we are left with are simply the signed permuted diagonals. So all we have done is just split the determinant up into the signed permuted diagonals and then added them up to get the determinant.

We are almost to the point where we can see how \wedge itself acts with scalar addition and scalar multiplication! Take the vector $(1, 1, 1) = 1 \cdot e_1 + 1 \cdot e_2 + 1 \cdot e_3$ and turn it into $1 \cdot dx + 1 \cdot dy + 1 \cdot dz$ where we are replacing e_1 with dx , e_2 with dy , and e_3 with dz . We will call this process:

Dualizing a vector

To dualize a vector $v = (1, 2, 3)$, turn it into $v^* = dx + 2dy + 3dz$.

If we think of what $dx : \mathbb{R}^3 \rightarrow \mathbb{R}$ is as a matrix, we have $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$. So $dx + dy + dz$ as a matrix is really $\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$: dualizing just changes a column vector to a row vector! With this thought, instead of turning $(1, 1, 1)$ into $a_1 + a_2 + a_3$, we could have dualized it to $dx + dy + dz$. Similarly, we could change $(2, 0, 1)$ to $2dx + dz$. Then, applying \otimes we would have gotten terms like $dz \otimes 2dx \otimes (-1)dy$ instead of $a_3 \otimes 2b_1 \otimes (-1)c_2$. Yet notice something interesting: it takes just as many column switches to get the matrix

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

which corresponds to $a_3 \otimes 2b_1 \otimes (-1)c_2$ into a nice diagonal:

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

as it takes to switch the order (dz, dx, dy) to (dx, dy, dz) . Every column switch multiplies (-1) to the determinant and every switch in $dz \wedge dx \wedge dy$ to get to $dx \wedge dy \wedge dz$, multiplies the output of this function by (-1) .

The term $dz \wedge 2dx \wedge (-1)dy$ means to take the z row (i.e. the third row) as the top, twice the first row as the middle and the negative of the second row as the bottom and then to take the determinant. Multiplying these

rows by -1 and 2 just multiplies the determinant by $(-1) \cdot 2$. Hence: $dz \wedge 2dx \wedge (-1)dy = 2(-1)dz \wedge dx \wedge dy$. Further, switch dz and dx and then dz and dy (two switches) to see that this is $= -2dx \wedge dy \wedge dz$ with -2 still out front because we have multiplied by -1 twice. If we plug in the identity matrix, which is given by the column vectors (a_1, b_2, c_3) , we should get a determinant of -2 :

$$\underbrace{f(a_3 \otimes 2b_1 \otimes (-1)c_2)}_{\text{a determinant}} = \underbrace{dz \wedge 2dx \wedge (-1)dy}_{\text{a trilinear function}} \underbrace{(a_1, b_2, c_3)}_{\text{input identity matrix}} = -2 \cdot \underbrace{dx \wedge dy \wedge dz(a_1, b_2, c_3)}_1 = -2$$

This discussion shows us that if we were to replace all of our \otimes s that we use in computing a determinant with \wedge 's, all of the a_1 's, b_1 's and c_1 's with dx 's, the a_2 's, b_2 's, and c_2 's with dy 's, and the a_3 's, b_3 's, and c_3 's with dz 's, and then plugged in the identity matrix into everything, it would be the same as if we plugged everything into a determinant finding function f . So \wedge does everything that \otimes does without needing to plug into a determinant function!

Theorem 6.4.5

We can find the determinant of a 3×3 matrix given by column vectors v_1, v_2, v_3 by first dualizing the vectors and then wedging them:

$$v_1^* \wedge v_2^* \wedge v_3^*$$

When we rewrite this wedge product as (something) $\cdot dx \wedge dy \wedge dz$, that something is the determinant of the matrix.

Properties of \wedge

The \wedge operator behaves exactly like \otimes except that we can switch order with \wedge while we cannot with \otimes . Every switch gives multiplication by -1 . But this switching business actually takes the determinant and puts it out front if we make every term look like $dx \wedge dy \wedge dz$ and then combine them.

 **Example 16.** Let's find the determinant of $\begin{pmatrix} 2 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$ by using the wedge product. We dualize the columns and wedge them:

$$(2dx + dy) \wedge (dz) \wedge (dx - dy) =$$

$$\underbrace{2dx \wedge dz \wedge dx}_0 + dy \wedge dz \wedge dx + 2dx \wedge dz \wedge (-dy) + \underbrace{dy \wedge dz \wedge (-dy)}_0$$

Whenever we take a determinant with two rows repeated we get 0. Hence when we see $dx \wedge dx$ or $dy \wedge dy$

appearing, we get the 0 function (since wedge products are really an algebra of functions—but we are using the functions to correspond to vectors). We are left with:

$$\underbrace{dy \wedge dz \wedge dx}_{\text{needs 2 switches}} + \underbrace{2dx \wedge dz \wedge (-dy)}_{\text{1 switch: } \cdot(-1) \text{ cancels with the scalar multiple } (-1)}$$

$$= +dx \wedge dy \wedge dz + 2dx \wedge dy \wedge dz = 3 \cdot dx \wedge dy \wedge dz$$

So the determinant of the matrix is 3. Now—there are many faster techniques for finding the determinant. But still, this technique gives us greater insight in how to work with the wedge product. This in turn can make some of multivariable calculus simpler.

Key Concepts from this Section

- **multilinear function:** (page 638) Suppose we take a function $f : V_1 \times V_2 \times \cdots \times V_n \rightarrow W$ where V_1, V_2, \dots, V_n , and W are all vector spaces over the same field. Further, take any $(v_1, v_2, \dots, v_n) \in V_1 \times V_2 \times \cdots \times V_n$. Suppose that the function given by

$$x \mapsto f(x, v_2, \dots, v_n)$$

and the function

$$x \mapsto f(v_1, x, \dots, v_n)$$

and all of the functions down to

$$x \mapsto f(v_1, v_2, \dots, x)$$

are all linear transformations. Further suppose that this same idea applies for any choice of (v_1, v_2, \dots, v_n) . Then, we say that f is *multilinear*.

- **four defining properties of determinants:** (page 638) The determinant function on $n \times n$ matrices is completely determined by the following facts:

- The determinant $\det : \underbrace{\mathbb{R}^n \times \cdots \times \mathbb{R}^n}_{n \text{ times}} \rightarrow \mathbb{R}$ is multilinear.
- Every time you swap the positions of two of the column entries, it multiplies the output by -1 .
- Every time there are two identical column entries the output is 0.
- The determinant of the identity matrix is 1.

- **bilinear transformation:** (page 640) A multilinear function of the form $f : V_1 \times V_2 \rightarrow W$ that is linear with respect to input from V_1 and also input from V_2 is called *bilinear*. It has *two* components in which it is linear individually.

- **bilinear transformations as matrices:** (page 641) Suppose that $f : \mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}$ is a bilinear transformation. Then f can be described as a matrix A such that the entry a_{ij} (i th row and j th column) of A is the image $f(e_i, e_j)$.
- **determinant matrix for 2×2 :** (page 642)

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

- **trilinear transformation:** (page 642) A multilinear function that has three input vectors.
- **stacking principle:** (page 643) For a trilinear matrix, we apply an input vector by taking a linear combination of what appears in planes perpendicular to the input vector. The coefficient to what is in that plane is the entry of the input vector that is in that same plane.
- **evaluate a trilinear transformation using matrix levels:** (page 645) We can represent a trilinear transformation as a series of matrix levels. Suppose that the matrix levels are A_1, \dots, A_r where all of these matrices are $n \times m$ matrices. Then, we have a trilinear transformation $T : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^r \rightarrow \mathbb{R}$. To evaluate $T(v_1, v_2, v_3)$ we proceed as follows. Let $v_3 = (a_1, \dots, a_r)$. Then we take a linear combination of the matrix levels as follows:

$$M = a_1 A_1 + a_2 A_2 + \cdots + a_r A_r$$

Then, just compute:

$$\underbrace{v_1^T}_{\text{make } v_1 \text{ a row}} \cdot M \cdot \underbrace{v_2}_{\text{this is a column}}$$

- **\otimes :** (page 648) The notation \otimes explained in the reading is read as “tensor” and is useful in turning a multilinear function into a linear one by creating a domain on which it actually can be linear and which describes the desired input into the multilinear function. It is a pairing idea and behaves just as if it were multiplication which distributes. Hence, one can expand things with it using FOIL.
- **$V \otimes_{\mathbb{R}} W$:** (page 648) Let V and W be \mathbb{R} -vector spaces. Then $V \otimes_{\mathbb{R}} W$ is the vector space whose basis is given as the symbols $a \otimes b$ where a is a basis vector of V and b is a basis vector of W . It is called the tensor product of V and W over \mathbb{R} .
- **tensor product:** (page 648) See $V \otimes_{\mathbb{R}} W$
- **bilinear matrix entries:** (page 650) The result of a bilinear transformation $\mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}$ described by a $m \times n$ matrix is simply a linear combination of the entries of the matrix. Each scalar multiplier in this linear combination is just a product of an entry from the row vector input with an entry from the column vector input. To get the scalar multiple corresponding to a position in the i th row and j th column of the matrix simply multiply the i th entry of the row vector input with the j th entry of the column vector.

- **theorem 6.4.1 product/boxing rule for derivatives:** (page 654) Suppose that we have a function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ which is described by a matrix expression. In this expression may be multiple occurrences of the n different input variables. Split the occurrences in two parts. The same variable may be present in both parts 1 and 2. Yet, if we take the derivative matrix with respect to our n variables *assuming that everything in part 2 behaves like a constant* and add to that the derivative matrix that *assumes that everything in part 1 is a constant* we arrive at the matrix for Df . *If we have 3 parts, it works the same way!*
- **symmetric multilinear form:** (page 655) A multilinear form $f : V \times V \times \cdots \times V \rightarrow W$ is symmetric if when we plug in the same vector $v \in V$ into k of the inputs, we get the same *function* back no matter which k inputs we put v into. *A function can be the same even if interpretations in a matrix representation switch.* For instance $v \mapsto A \cdot v$ is the same function as $v^T \mapsto v^T \cdot A^T$. One way we write the vectors as columns and in the other as rows. *But they still are the same function!*
- **theorem 6.4.2 multivariable taylor series (centered at $(0, 0)$):** (page 658) Let $D^m f_{(0,0)}$ signify that we plug in $x = 0$ and $y = 0$ into the multilinear matrix entries. *It does not refer to a vector that we multiply the multilinear matrix by!*

$$f(x, y) = \underbrace{f(0, 0)}_{\text{constant part}} + \underbrace{Df_{(0,0)}((x, y))}_{\text{linear part}} + \underbrace{\frac{1}{2!} D^2 f_{(0,0)}((x, y), (x, y))}_{\text{bilinear part}} + \underbrace{\frac{1}{3!} D^3 f_{(0,0)}((x, y), (x, y), (x, y))}_{\text{trilinear part}} + \cdots$$

- **multivariable polynomial:** (page 659) A multivariable polynomial is a linear combination of products of variables.
- **total degree:** (page 659) The total degree of a multivariable polynomial is the highest sum of exponents that occur among all the individual terms.
- **identifying multilinear parts:** (page 659) Any term of a multivariable polynomial whose exponents add to 2 like xy is in the bilinear part. If they add to 3 like xy^2 they are in the trilinear part and so forth.
- **theorem 6.4.3 :** (page 661) Any function defined by a multivariable Taylor series has mixed partial derivatives which are equal. That is, $f_{xy} = f_{yx}$.
- **practical interpretation of bilinear part of a multivariable polynomial:** (page 662) Assuming that the first derivative is a zero matrix, the bilinear part of a multivariable polynomial approximates the change of the function from the point $(0, 0)$ to (x, y) . *We have an analogous statement assuming all previous derivative matrices are the zero matrix up to a specified derivative.*
- **dx :** (page 662) Define $dx : \mathbb{R}^3 \rightarrow \mathbb{R}$ to be a function which just picks out the x coordinate of a vector.
- **dual space:** (page 662) The dual space of a \mathbb{R} -vector space V is defined to vector space consisting of linear transformations $V \rightarrow \mathbb{R}$. If V is represented by column vectors, then the dual space is just matrices which are row vectors. The dual space is notated as V^* or $\text{Hom}_{\mathbb{R}}(V, \mathbb{R})$.
- **dual vectors:** (page 663) This is a name for elements of a dual vector space.

- **covectors:** (page 663) This is a name for elements of a dual vector space.
- **wedge product:** (page 663) We define $dx \wedge dy$ to be the bilinear function $\mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$ that computes the 2×2 determinant of the top part of two vectors. That is, pick out the x coordinates as the top row and the y coordinates as the bottom row. So if $v = (v_1, v_2, v_3)$ and $w = (w_1, w_2, w_3)$, then

$$dx \wedge dy(v, w) = \det \begin{pmatrix} v_1 & w_1 \\ v_2 & w_2 \end{pmatrix}.$$

- \wedge : (page 663) See wedge product.
- **theorem 6.4.4 :** (page 664)

$$dy \wedge dx(v, w) = -dx \wedge dy(v, w)$$
- **dualizing a vector:** (page 666) To dualize a vector $v = (1, 2, 3)$, turn it into $v^* = dx + 2dy + 3dz$.
- **theorem 6.4.5 :** (page 667) We can find the determinant of a 3×3 matrix given by column vectors v_1, v_2, v_3 by first dualizing the vectors and then wedging them:

$$v_1^* \wedge v_2^* \wedge v_3^*$$

When we rewrite this wedge product as $(\text{something}) \cdot dx \wedge dy \wedge dz$, that *something* is the determinant of the matrix.

- **properties of \wedge :** (page 667) The \wedge operator behaves exactly like \otimes except that we can switch order with \wedge while we cannot with \otimes . Every switch gives multiplication by -1 . *But this switching business actually takes the determinant and puts it out front if we make every term look like $dx \wedge dy \wedge dz$ and then combine them.*

6.4.9 Exercises

Four Defining Properties of Determinants

Use the four defining properties of determinants as given in the reading to evaluate the following determinants. Show your work!

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

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

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

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

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

$$6. \begin{pmatrix} 1 & 1 & -2 \\ 0 & 1 & 0 \\ -2 & -2 & 0 \end{pmatrix}$$

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

$$8. \begin{pmatrix} 2 & -1 & 0 \\ 2 & -2 & 0 \\ -1 & -2 & 1 \end{pmatrix}$$

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

$$10. \begin{pmatrix} 0 & 0 & -1 \\ -1 & -1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

Evaluating Trilinear Transformations with Stacking

Let v_1 follow a row interpretation, v_2 a column interpretation, and v_3 a stacking interpretation. For each of the following...

- (a) Find the domain and the codomain of the trilinear transformation T .

(b) Evaluate $T(v_1, v_2, v_3)$.

11. $\underbrace{\begin{pmatrix} -2 & 0 & 1 \\ 0 & 2 & -2 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} -1 & 2 & -1 \\ 0 & -2 & 0 \end{pmatrix}}_{\text{level 2}}$

$$\underbrace{(2, 0)}_{v_1}, \underbrace{(1, -1, 1)}_{v_2}, \underbrace{(0, 1)}_{v_3}$$

12. $\underbrace{\begin{pmatrix} 0 & -1 & -2 \\ -2 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} 1 & 1 & 0 \\ -1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{\text{level 2}}$

$$\underbrace{(-1, 0, 0)}_{v_1}, \underbrace{(-1, 1, 0)}_{v_2}, \underbrace{(1, 2)}_{v_3}$$

13. $\underbrace{\begin{pmatrix} 2 & 0 \\ -2 & 2 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}}_{\text{level 2}}$

$$\underbrace{(2, -2)}_{v_1}, \underbrace{(2, 0)}_{v_2}, \underbrace{(1, 2)}_{v_3}$$

14. $\underbrace{\begin{pmatrix} -1 & 0 & 1 \\ -2 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} -2 & 0 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{\text{level 2}}$

$$\underbrace{(0, 0, 1)}_{v_1}, \underbrace{(1, 0, 1)}_{v_2}, \underbrace{(-1, -1)}_{v_3}$$

15. $\underbrace{\begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{\text{level 2}}$

$$\underbrace{(0, 1)}_{v_1}, \underbrace{(2, 2, 1)}_{v_2}, \underbrace{(2, -1)}_{v_3}$$

16. $\underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} 1 & -2 \\ 0 & 0 \end{pmatrix}}_{\text{level 2}}$

$$\underbrace{(0, 1)}_{v_1}, \underbrace{(-2, -1)}_{v_2}, \underbrace{(0, 1)}_{v_3}$$

17. $\underbrace{\begin{pmatrix} -1 & 0 \\ -2 & 2 \\ -1 & -2 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \\ 0 & 1 \end{pmatrix}}_{\text{level 2}}$

$$\underbrace{(-2, -2, 2)}_{v_1}, \underbrace{(2, 0)}_{v_2}, \underbrace{(-1, 2)}_{v_3}$$

18. $\underbrace{\begin{pmatrix} -2 & -1 & 0 \\ 0 & 0 & -2 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}}_{\text{level 2}}$

$$\underbrace{(-2, 2)}_{v_1}, \underbrace{(0, 0, 1)}_{v_2}, \underbrace{(0, -1)}_{v_3}$$

19. $\underbrace{\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} -1 & 0 \\ -2 & -2 \end{pmatrix}}_{\text{level 2}}$

$$\underbrace{(2, -1)}_{v_1}, \underbrace{(-2, 0)}_{v_2}, \underbrace{(2, 0)}_{v_3}$$

20. $\underbrace{\begin{pmatrix} -1 & 1 & 0 \\ 2 & 2 & 2 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & -2 \end{pmatrix}}_{\text{level 2}}$

$$\underbrace{(2, -2)}_{v_1}, \underbrace{(-1, 1, 0)}_{v_2}, \underbrace{(-1, -1)}_{v_3}$$

Evaluating Bilinear Transformations (Fast Technique or Tensors)

Either use *tensors* or the *fast bilinear evaluation technique* in the reading to perform the following matrix multiplications.

$$21. \begin{pmatrix} 1 & 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 2 & -2 \\ 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 2 \end{pmatrix}$$

$$22. \begin{pmatrix} 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 & 2 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$$

$$23. \begin{pmatrix} 1 & -2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$24. \begin{pmatrix} 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$25. \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

$$26. \begin{pmatrix} 0 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 & 2 \\ 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$27. \begin{pmatrix} 2 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

$$28. \begin{pmatrix} -2 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & -1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ -1 \end{pmatrix}$$

$$29. \begin{pmatrix} -1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 0 & 0 \\ -2 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$30. \begin{pmatrix} -2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 \\ 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Representing Multivariable Polynomials with Multilinear Transformations

For each of the following multivariable polynomials $f(x, y)$:

- (a) find a linear transformation L expressed as a row matrix,
- (b) a bilinear transformation B expressed as a 2×2 matrix,
- (c) and a trilinear transformation T expressed as matrix levels....

...such that:

$$f(x, y) = f(0, 0) + \underbrace{T(v)}_{\text{linear part}} + \underbrace{B(v, v)}_{\text{bilinear part}} + \underbrace{T(v, v, v)}_{\text{trilinear part}} \quad \text{and} \quad v = (x, y)$$

31. $f(x, y) = -x^2y + 2y^3 - x^2 - 2y + 2$

32. $f(x, y) = x^2y - 2xy^2 + y^3 - 2y$

33. $f(x, y) = -x^2y + y^3 - 2x^2$

34. $f(x, y) = -2x^3 - x^2y - 2xy^2 - x^2 + 2xy + 2y^2 + x + 2$

35. $f(x, y) = x^2y + 2xy^2 + y^2 - 2x - 2y$

36. $f(x, y) = 2x^3 + xy^2 + y^3 - 2xy + 2y^2 - x + y$

37. $f(x, y) = -x^3 - x^2y - x^2 + xy + y^2 - y + 1$

38. $f(x, y) = -x^2y + 2y^3 - x^2 + xy + x$

39. $f(x, y) = x^3 + x^2y + 2x^2 + 2y + 2$

40. $f(x, y) = x^3 + xy^2 + x^2 + 2y^2 + x + 2y - 1$

Wedge Products

Evaluate the following:

41. $dy \wedge dz(-1, -1, -2), (-1, 0, -2)$

42. $dx \wedge dy(0, 2, -1), (-2, 0, -1)$

43. $dx \wedge dz(1, -1, -1), (1, 0, -1)$

44. $dy \wedge dz(0, 0, 1), (-1, 0, -1)$

45. $dy \wedge dz(-1, -1, 1), (-1, -2, -2)$

46. $dy \wedge dz(-2, -2, -1), (-1, -2, 2)$

47. $dx \wedge dz(0, -2, -1), (1, -2, -2)$

48. $dy \wedge dz(0, -2, 1), (2, 0, -1)$

49. $dx \wedge dz(0, -2, 2), (0, -1, 0)$

50. $dx \wedge dy(0, -2, 0), (1, 0, 0)$

Determinants via Wedge Products

Dualize the column vectors and then use wedge products to compute the following determinants.

51.
$$\begin{pmatrix} -2 & 2 & 0 \\ 1 & 1 & 2 \\ -2 & 0 & -1 \end{pmatrix}$$

52.
$$\begin{pmatrix} 0 & -1 & 2 \\ 2 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

53.
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & -2 & -1 \end{pmatrix}$$

54.
$$\begin{pmatrix} 2 & 0 & 1 \\ -2 & 1 & -2 \\ 2 & -1 & -1 \end{pmatrix}$$

55.
$$\begin{pmatrix} -2 & 0 & -2 \\ -1 & 1 & 0 \\ 2 & -2 & -1 \end{pmatrix}$$

56.
$$\begin{pmatrix} 2 & -2 & 2 \\ -2 & 2 & 0 \\ -2 & 0 & 0 \end{pmatrix}$$

57.
$$\begin{pmatrix} 0 & 2 & 0 \\ -1 & 0 & -1 \\ -1 & 1 & 2 \end{pmatrix}$$

58.
$$\begin{pmatrix} 1 & -1 & -2 \\ -1 & -2 & -2 \\ -1 & 0 & 1 \end{pmatrix}$$

59.
$$\begin{pmatrix} 0 & -1 & 2 \\ 0 & 0 & 1 \\ -1 & 1 & -1 \end{pmatrix}$$

60.
$$\begin{pmatrix} -2 & -1 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix}$$

Proof Practice

61. Prove that if all of the columns of a matrix A are orthogonal to each other, then $\det(A)$ is \pm the product of the lengths of all of the column vectors. *Hints: use the fact that the determinant is multilinear. Factoring out the lengths of the column vectors leaves you with a matrix B whose columns are orthonormal. Do you remember that this means that $B^T B = \text{id}$? How does this help? Write out a nice argument.*

62. Think of every complex number $a + bi \in \mathbb{C}$ as being an ordered pair $(a, b) \in \mathbb{R}^2$. Multiplying $x + iy$ by the complex number $a + bi$ is a linear transformation with input (x, y) and output $(ax - by, ay + bx)$ since $(a + bi) \cdot (x + iy) = (ax - by) + (ay + bx)i$. Show that in a column interpretation, the matrix describing this

linear transformation is

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

63. Suppose that we have a function $f : \mathbb{C} \rightarrow \mathbb{C}$. Under the representation we give in the last problem of \mathbb{C} as \mathbb{R}^2 , we can express f as a function $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ where $f(x, y) = (u(x, y), v(x, y))$ for some functions $u : \mathbb{R}^2 \rightarrow \mathbb{R}$ and $v : \mathbb{R}^2 \rightarrow \mathbb{R}$. If we want the derivative matrix Df to represent multiplication by a complex number to $x + iy$, use the last exercise to show that $u_x = v_y$ and $u_y = -v_x$. We would call f complex linear. The equations $u_x = v_y$ and $u_y = -v_x$ are called the *Cauchy Riemann Equations*.

64. Assume that u and v have and are equal to their multivariable series Taylor expansions. Then, if f is complex linear (so it satisfies the Cauchy Riemann Equations), show that $D^2 f$ is complex linear in each component separately and that it is a symmetric bilinear form. *Hint: use stacking for second vector input instead of a row. Also, since u and v are equal to their Taylor expansions, their derivatives are symmetric bilinear forms. This says that $u_{xy} = u_{yx}$ for instance.*

Commentary on the result of this last exercise: Since multiplying two complex numbers (i.e. two input vectors) is bilinear and is completely determined component-wise, this last exercise shows that $D^2 f$ actually gives a complex multiplication of its two inputs with a constant complex number to give another complex number. In fact, it is a symmetric multilinear transformation. This symmetry allows us to use the product rule for derivatives. Continuing this idea onward we can actually build a multivariable Taylor expansion for f in x and y which is actually a power series $a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \dots$ with $z = x + iy$ and complex coefficients a_0, a_1, \dots . Using the fact that u and v are equal to their Taylor expansions, one can do a little analysis to show that f is as well. But what we have here at least is that the multivariable Taylor expansion of f is expressible as a sum of powers of a complex variable $z \in \mathbb{C}$. Wait! Just knowing that *one* derivative of f behaves nicely and that u and v themselves are equal to their Taylor expansions ensures that f is equal to a whole Taylor series with complex input! Taylor series of a complex variable $z \in \mathbb{C}$ make nice functions. The functions e^z , $\cos(z)$, and $\ln(z + 1)$ are examples! This is the important complex number symmetry that allows functions to step away from just a real axis domain into the complex plane. Such expansion of domain plays a key role in performing many computations and solving many problems in math, science, and engineering.

65. Extra Exploration: Show that $f(x, y) = e^x \cos(y) + i \cdot e^x \sin(y)$ satisfies the Cauchy Riemann equations. The function f can be written as a function $\mathbb{C} \rightarrow \mathbb{C}$ expressible as a power series in the variable $z = x + iy$. Can you figure out what this power series is? That is, look at the linear form that describes the first derivative, the bilinear form that describes the second derivative, and the trilinear form that describes the third derivative. Make the inputs to the multilinear matrix entries of all these be $x = 0, y = 0$. The linear form at these inputs represents multiplication by a complex number k to a complex variable $z = x + iy$. The bilinear form represents multiplication of that same complex number k to z^2 (with both vector inputs as z). The trilinear form is similarly given by kz^3 (with all three vector inputs as z). What is k ? Is there a function of a real variable x which has a Taylor series determined by these same derivative values (i.e. all being k)? If so, you

have found a way to expand the domain of that function into the complex plane. Remember that you need to divide the n th derivative evaluated at $x = 0$ and $y = 0$ by $n!$ to get the desired Taylor series.

6.4.10 Solutions

1. -4

2. 12

3. -12

4. 3

5. -4

6. -4

7. -2

8. -2

9. -8

10. 1

11. Solutions by part:

(a) $T : \mathbb{R}^2 \times \mathbb{R}^3 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) -8

12. Solutions by part:

(a) $T : \mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) 1

13. Solutions by part:

(a) $T : \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) 16

14. Solutions by part:

(a) $T : \mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) -2

15. Solutions by part:

(a) $T : \mathbb{R}^2 \times \mathbb{R}^3 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) 4

16. Solutions by part:

(a) $T : \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) 0

17. Solutions by part:

(a) $T : \mathbb{R}^3 \times \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) 0

18. Solutions by part:

(a) $T : \mathbb{R}^2 \times \mathbb{R}^3 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) 2

19. Solutions by part:

(a) $T : \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) -4

20. Solutions by part:

(a) $T : \mathbb{R}^2 \times \mathbb{R}^3 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) -4

21. -8

22. -2

23. -2

24. 0

25. -1

26. -2

27. -2

28. 1

29. 0

30. 2

31. Solutions by part:

(a) $(0, -2)$

(b) $\frac{1}{2} \begin{pmatrix} -2 & 0 \\ 0 & 0 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \cdot \begin{pmatrix} 0 & -2 \\ -2 & 0 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \cdot \begin{pmatrix} -2 & 0 \\ 0 & 12 \end{pmatrix}}_{\text{level 2}}$

32. Solutions by part:

(a) $(0, -2)$

(b) $\frac{1}{2} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \cdot \begin{pmatrix} 0 & 2 \\ 2 & -4 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \cdot \begin{pmatrix} 2 & -4 \\ -4 & 6 \end{pmatrix}}_{\text{level 2}}$

33. Solutions by part:

(a) $(0, 0)$

(b) $\frac{1}{2} \begin{pmatrix} -4 & 0 \\ 0 & 0 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \cdot \begin{pmatrix} 0 & -2 \\ -2 & 0 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \cdot \begin{pmatrix} -2 & 0 \\ 0 & 6 \end{pmatrix}}_{\text{level 2}}$

34. Solutions by part:

(a) $(1, 0)$

(b) $\frac{1}{2} \begin{pmatrix} -2 & 2 \\ 2 & 4 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \cdot \begin{pmatrix} -12 & -2 \\ -2 & -4 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \cdot \begin{pmatrix} -2 & -4 \\ -4 & 0 \end{pmatrix}}_{\text{level 2}}$

35. Solutions by part:

(a) $(-2, -2)$

(b) $\frac{1}{2} \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \cdot \begin{pmatrix} 0 & 2 \\ 2 & 4 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \cdot \begin{pmatrix} 2 & 4 \\ 4 & 0 \end{pmatrix}}_{\text{level 2}}$

36. Solutions by part:

(a) $(-1, 1)$

(b) $\frac{1}{2} \begin{pmatrix} 0 & -2 \\ -2 & 4 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \cdot \begin{pmatrix} 12 & 0 \\ 0 & 2 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \cdot \begin{pmatrix} 0 & 2 \\ 2 & 6 \end{pmatrix}}_{\text{level 2}}$

37. Solutions by part:

(a) $(0, -1)$

(b) $\frac{1}{2} \begin{pmatrix} -2 & 1 \\ 1 & 2 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \cdot \begin{pmatrix} -6 & -2 \\ -2 & 0 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \cdot \begin{pmatrix} -2 & 0 \\ 0 & 0 \end{pmatrix}}_{\text{level 2}}$

38. Solutions by part:

(a) $(1, 0)$

(b) $\frac{1}{2} \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \cdot \begin{pmatrix} 0 & -2 \\ -2 & 0 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \cdot \begin{pmatrix} -2 & 0 \\ 0 & 12 \end{pmatrix}}_{\text{level 2}}$

39. Solutions by part:

(a) $(0, 2)$

(b) $\frac{1}{2} \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \cdot \begin{pmatrix} 6 & 2 \\ 2 & 0 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}}_{\text{level 2}}$

40. Solutions by part:

(a) $(1, 2)$

(b) $\frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \cdot \begin{pmatrix} 6 & 0 \\ 0 & 2 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \cdot \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}}_{\text{level 2}}$

41. 2

42. 4

43. 0

44. 0

45. 4

46. -6

47. 1

48. 2

49. 0

50. 2

51. -4

52. -2

53. 2

54. -6

55. 2

56. 8

57. 6

58. -1

59. 1

60. -6

61. Let $A = (c_1 \ c_2 \ \dots \ c_n)$ where c_1, \dots, c_n are the columns of A . Then,

$$\det(A) = \det(c_1, \dots, c_n)$$

We can write $c_i = |c_i|u_i$ where u_i is a unit vector. Therefore,

$$\det(A) = \det(|c_1|u_1, \dots, |c_n|u_n) = |c_1| \cdots |c_n| \det(u_1, \dots, u_n)$$

Consider the matrix $B = (u_1 \ \dots \ u_n)$. Its columns u_1, \dots, u_n are orthonormal so that $B^T B = \text{id}_{n \times n}$. This means that $1 = \det(B^T B) = \det(B^T) \det(B) = \det(B)^2$ which means that $\det(B) = \pm 1$. Therefore,

$$\det(A) = |c_1| \cdots |c_n| \det(B) = \pm |c_1| \cdots |c_n|$$

as desired.

62. The image of $e_1 = (1, 0)$ is given by multiplying $(a + bi) \cdot (1 + 0 \cdot i) = a + bi$. Therefore, $(1, 0) \mapsto (a, b)$. The image of $e_2 = (0, 1)$ is given by multiplying $(a + bi) \cdot (0 + 1 \cdot i) = -b + ai$. Therefore, $(0, 1) \mapsto (-b, a)$

63. Note that the matrix for Df is

$$\begin{pmatrix} u_x & v_x \\ u_y & v_y \end{pmatrix}.$$

The equations $u_x = v_y$ and $u_y = -v_x$ must hold if we want this matrix with column input to be of the form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

64. The first derivative is already a 2×2 matrix. So we use stacking for the second input vector of $D^2 f$. We start with:

$$Df : \begin{pmatrix} u_x & u_y \\ v_x & v_y \end{pmatrix}$$

Now take another derivative:

$$D^2 f : \underbrace{\begin{pmatrix} u_{xx} & v_{xx} \\ u_{yx} & v_{yx} \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} u_{xy} & v_{xy} \\ u_{yy} & v_{yy} \end{pmatrix}}_{\text{level 2}}$$

Since u and v are equal to their Taylor series, they are given by symmetric multilinear forms so that their mixed partials are equal. That is, $u_{yx} = u_{xy}$ and $v_{yx} = v_{xy}$. Use this idea and the equations $u_x = v_y$ and $u_y = -v_x$ to show that $D^2 f((x, y), -)$ and $D^2 f(- , (x, y))$ both give the same function and the result in each case is equivalent to 2×2 matrix of the form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

You get to fill in the details!

65. The result is $f(z) = 1 + z + \frac{1}{2!}z^2 + \frac{1}{3!}z^3 + \cdots = e^z$.

Cofactor and Wedge Intuition

6.5

6.5.1 Area of a Parallelogram is a Linear Transformation	685
6.5.2 Intuition for the Volume of a Parallelepiped	692
6.5.3 The Cross Product	695
6.5.4 Wedge Products on Surfaces	701
6.5.5 Surface Area	704
6.5.6 Changing Coordinates	708
6.5.7 Stoke's Theorem via Wedges	713
6.5.8 Exercises	725
6.5.9 Solutions	730

Questions to Guide Your Study:

- *How can we intuitively think about the matrix entries in the linear transformations that describe areas of parallelograms off of a fixed base?*
- *What about the matrix entries when we consider linear transformation that compute volumes of parallelepipeds off of a fixed base?*
- *What is negative area or volume intuitively?*
- *How is the cross product related to a cofactor function?*
- *What are some applications of the cross product?*
- *How can we write the cross product in terms of the wedge product?*
- *How can we use the wedge product in multivariable calculus?*

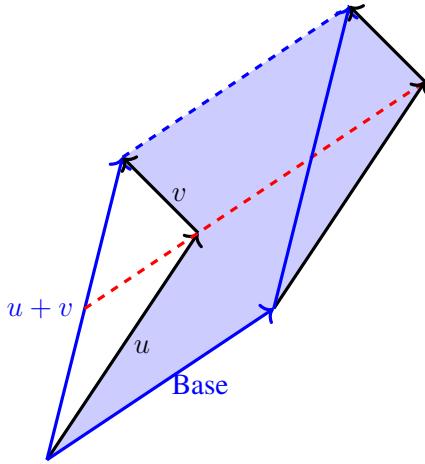
6.5.1 Area of a Parallelogram is a Linear Transformation

The idea of finding the area of a parallelogram is a linear transformation—if we fix a base arrow on it and let the other arrow be the input subject to that base we have fixed. Do you remember that determinants calculate area and volume? If we fix all the columns but one, and let taking the determinant just be a function of the

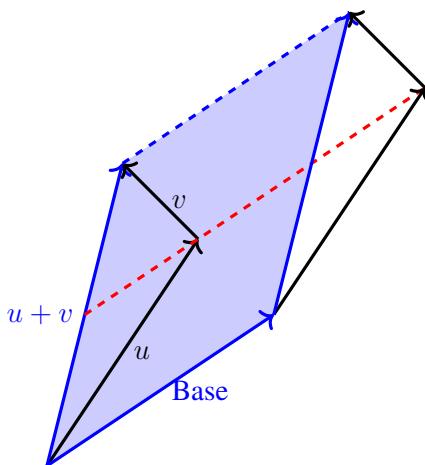
column we have not fixed, the determinant is a linear function which is actually just the cofactor function with matrix c_v^T .

Our goal is to have some visual intuition for this cofactor function which both describes the determinant and taking an area or a volume. But let's start with the area of a parallelogram in the xy -plane which is easier to visualize. This means that we will be working with 2×2 matrices.

Let's give some visual motivation. Suppose that we have an initial vector "Base" $\in \mathbb{R}^2$ and another vector $u + v \in \mathbb{R}^2$ (the sum of two vectors $u, v \in \mathbb{R}^2$). The following pictures illustrate how the addition operation $u + v$ passes nicely to the addition of areas. Notice how "sliding" along the middle dashed line changes the two separate parallelograms into one single parallelogram. *Sliding does not change the area!*

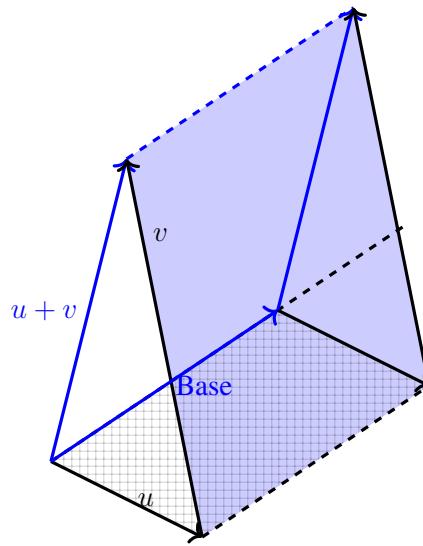


We have the area of two parallelograms. One is formed with sides u and the base arrow. The other is formed with sides v and a *copy* of the base arrow. Notice that when we slide these parallelograms into one:



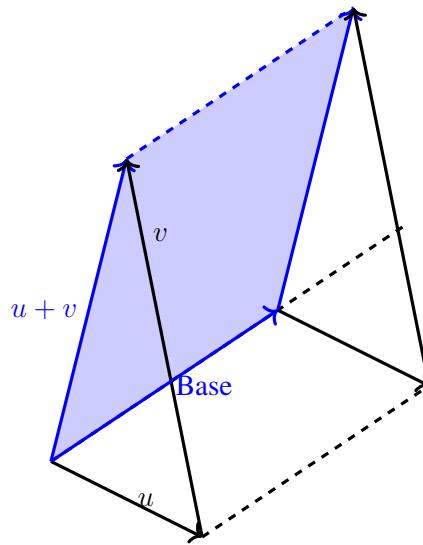
the area is unaltered. This new, bigger parallelogram is formed with sides $u + v$ and the base arrow. Notice how addition of the vectors u and v turned into the addition of areas!

Sometimes this addition involves negative areas. For instance, consider the following:



$$\square = \begin{pmatrix} \text{parallelogram} \\ \text{formed from a} \\ \text{copy of base} \\ \text{arrow and } v \end{pmatrix} \quad \square = \begin{pmatrix} \text{parallelogram} \\ \text{formed from a} \\ \text{copy of base} \\ \text{arrow and } u \end{pmatrix}$$

Notice for the addition of these two areas to equal the desired area between the base and $u + v$,

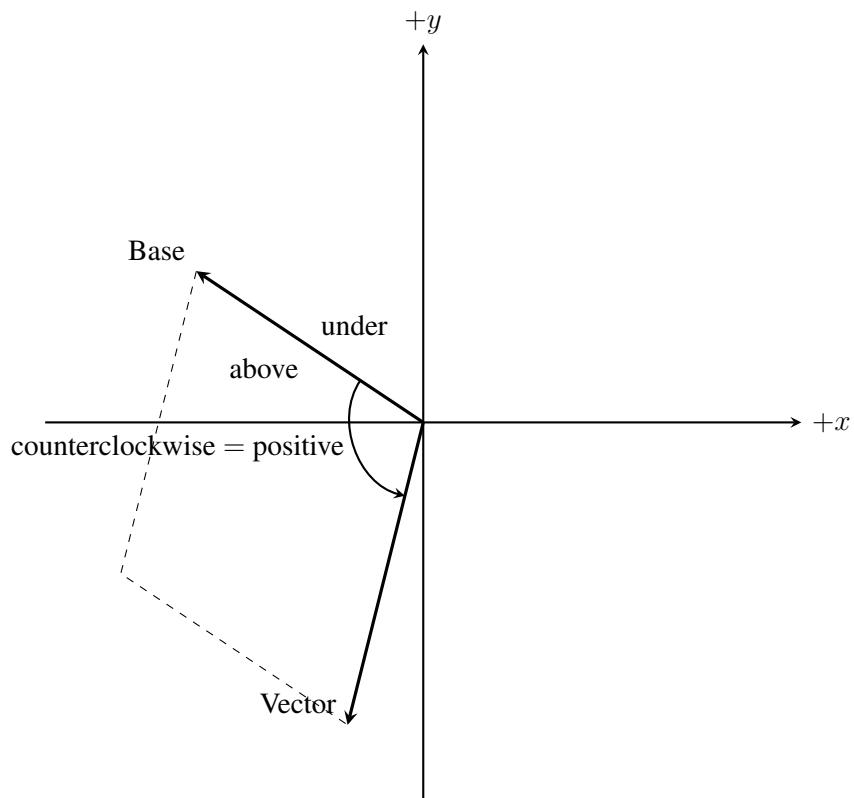


we need to think of the area \square as being negative. That is, area that occurs on the other side of the base should be negative.

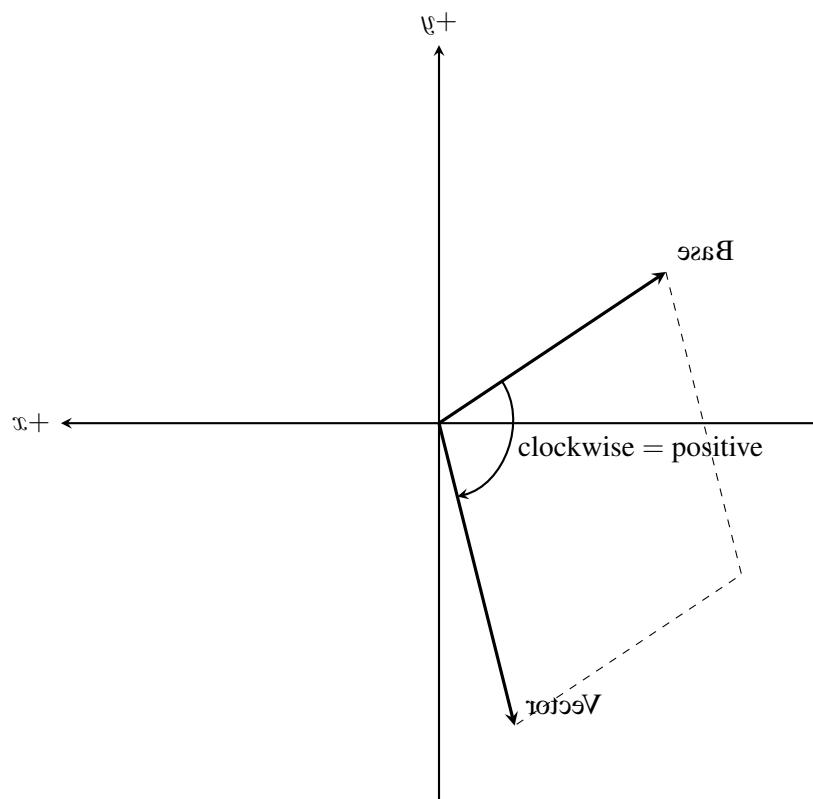
So, if we fix a base arrow, we have a well-defined area map from vectors in \mathbb{R}^2 to areas (in \mathbb{R}) which preserves addition. This map also preserves scalar multiplication which can be thought of as rescaling the

vector coming out of the base to make it longer or shorter. The effect is to multiply the height and thus the area of the parallelogram by the same amount.

Now here is a question: how do we know if the vector coming off the base will give us a parallelogram with negative area? Let's look straight on facing the front of the xy -plane (in contrast to its underside), with the positive x -axis pointing right and the positive y -axis pointing up. Our base vector and our vector coming off of the base both have their tails at the same point: the origin. Now there are only two consistent types of perspectives in determining whether the base vector is “above” or “below.” Either we adopt the convention that the nearest angle to the vector coming off of the base is counterclockwise from the base makes a positive area parallelogram or we decide that positive area should be measured clockwise from the base. We choose counterclockwise. When we look at the xy -plane head on, we want a positive area.

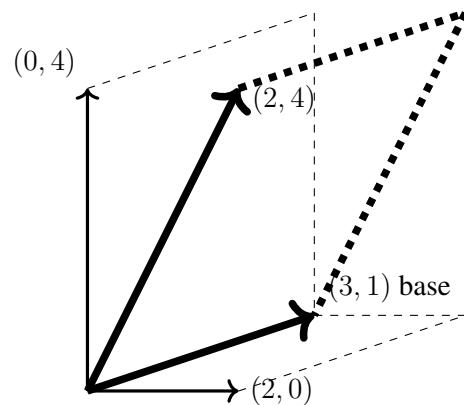


When we look at it from behind, the positive x -axis would be going to the left. Positive area would be calculated using clockwise rotation.

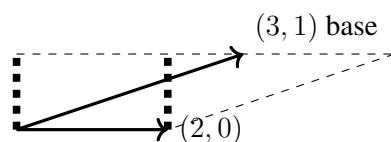


Note: Now as we extend these ideas to three dimensions, our base will be a parallelogram in a plane. We decide that vectors that come off of the base off of where that base parallelogram is measured as positive will form positive volume “parallelepipeds.”

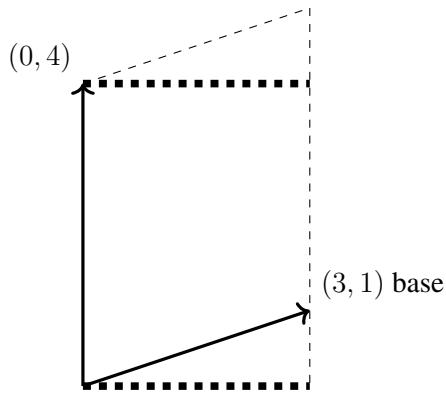
Consider the following example. Suppose that our base vector is $(3, 1) \in \mathbb{R}^2$ and we want to compute the area of $(2, 4)$ off of the base. Let’s use the idea that $(2, 4) = (2, 0) + (0, 4)$ and that this area map preserves addition of vectors to the addition of areas. Then, we have:



The area piece drawn below is considered as negative. Notice how we can slide the area into a rectangle. The area is $-(2 \cdot 1)$:



Now, the next area we will illustrate will be considered as positive *above the base*. Notice how in the following picture we can slide its area into a rectangle. The area is $3 \cdot 4$.



Using the diagrams to help, we compute the area of the parallelogram using the preservation of addition to areas:

$$3 \cdot 4 - (2 \cdot 1) = 10$$

As a matrix we could write:

$$\begin{pmatrix} + & - \\ 3 & 2 \\ 1 & 4 \end{pmatrix}$$

where we can think of multiplying the entries in the diagonal from upper left to lower right together and then subtract the product of the entries in the other diagonal. That is, we took the determinant of the 2×2 matrix.

Visually, we could see we had two areas: one associated with each coordinate 2 and 4 of the vector $(2, 4)$ off of the base. The area associated with “4” (which is $3 \cdot 4$) comes from the y -component of the vector off of the base. Think: $e_2 = (0, 1)$ is *counterclockwise* from $e_1 = (1, 0)$. Therefore, e_2 off of a base of e_1 is positive area. Any reflection to this parallelogram (i.e. multiplying the 4 or the 3 by -1) would make the parallelogram have negative area. But instead of reflecting, we simply stretch: stretch e_2 by 4 and e_1 by 2. *But the point is that the area of this parallelogram will be just the y-coordinate of the vector off of the base multiplied to the x coordinate of the base without any sign change! The multiplication of these coordinates are simply from transformations applied to an area that started as positive.*

Now, the other area is associated with the “2” coordinate of the vector off of the base—that is the x -coordinate of this vector. The area is $-2 \cdot 1$. Think: the $e_1 = (1, 0)$ (vector off of the base) is clockwise from $e_2 = (0, 1)$ (the base). So the area off of e_1 off of e_2 is negative. So ***we start with a negative area.*** We stretch e_1 to $2e_1$ and then the area is *still negative*: $2 \cdot (-1)$.

Notice that the determinant itself seems to know which way is above and which way is below: it understands the difference between counterclockwise and clockwise. Although there are many ways of considering this situation, we offer an idea which we will apply in higher dimensions as well. Essentially, we just switch axes enough times so that the rectangular object we are viewing is just a simple transformation of a *positive area or volume*. That transformation is just made up of multiplying by the coordinates of each edge that touches the origin. In the last example, we had a positive area $4 \cdot 3$. This came from taking the rectangle of e_2 off of e_1 and then stretching e_2 to 4 and e_1 to 3. *Before transformations*, this rectangle of e_2 off of e_1 had a positive area.

Now, for the other area $-2 \cdot 1$, we could have used the following idea. Every time we axis switch, we are changing our viewpoint from in front of something to behind something. That is, if we switch our positive x and positive y axes, we are going to the back of the plane so that clockwise would give positive and counterclockwise would be negative.

Every simple switch of two axes changes area or volume from positive to negative.

So what we could have done is perform an axis swap so that instead of $(2, 0)$ coming off of a base of $(1, 0)$, we have $(0, 2)$ coming off of a base of $(1, 0)$. *Now we compute the area as: $1 \cdot 2$. But remember that we performed an odd number of axis switches—just one.* This means that we change the sign of the area to -2 .

Also, remember:

We only get area when we multiply two things that are perpendicular.

Essentially, the rate of change of growth of the area in the x direction is this “signed” (positive or negative) projection $-(1)$ of the base vector on the y -axis (which is perpendicular to x). That is, for every additional unit the input vector takes on in the x -direction, the area will grow by -1 square units. You can think of this as being a “partial derivative” of the area function since it is the rate of change when the input changes in *just one direction*. Let $g : \mathbb{R}^2 \rightarrow \mathbb{R}$ be the area function that we have been considering.

$$\begin{array}{ll} \Delta x = +1 & \Delta g = -1 \cdot 1 = -1 \\ \begin{array}{c} \text{---} \\ \text{---} \end{array} & \frac{\Delta g}{\Delta x} = -1 \end{array}$$

The rate of change of growth of the area in the y direction is this “signed” (positive or negative) projection $+3$ of the base vector on the x -axis (which is perpendicular to y). That is, for every additional unit the input vector takes on in the y -direction, the area will grow by $+3$ square units. Again, this is like a “partial derivative.”

$$\begin{array}{ll} \begin{array}{c} \text{---} \\ \text{---} \end{array} & \Delta g = 3 \cdot 1 = 3 \\ \Delta y = +3 & \frac{\Delta g}{\Delta y} = 3 \end{array}$$

Remember that we are describing the cofactor function c_v^T where v is the second column with the first column (base) fixed. Let $g : \mathbb{R}^2 \rightarrow \mathbb{R}$ be this function. Since this function itself is a linear transformation, its matrix is its own derivative! Its derivative looks like:

$$\begin{pmatrix} g_x & g_y \end{pmatrix}$$

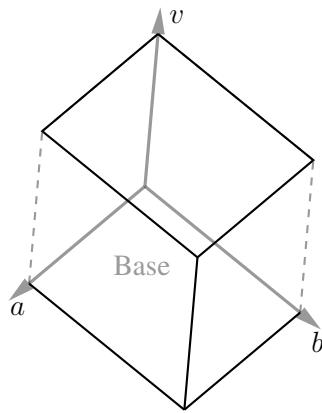
Let's compute the cofactor function matrix relative to the second column. We get:

$$\begin{pmatrix} -1 & 3 \end{pmatrix}.$$

Hence, naturally, we can think that the partial derivatives are $g_x = -1$ and $g_y = 3$ just as we visualized above.

6.5.2 Intuition for the Volume of a Parallelepiped

Suppose that in three dimensions we have the analog to a parallelogram: a parallelepiped.



The base is made up of two vectors a and b in \mathbb{R}^3 . The vector v is like input into our *volume* function $\mathbb{R}^3 \rightarrow \mathbb{R}$. We again wish this map to be a linear transformation preserving the addition of vectors to the addition of volumes. Let's suppose that our base vectors a and b are $(1, 3, 2)$ and $(2, 1, 4)$ respectively. Then, let's write these as columns in a matrix:

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

Suppose that our vector v is $(-2, 3, 1)$. Let's break v into its additive parts:

$$v = (-2, 0, 0) + (0, 3, 0) + (0, 0, 1)$$

Analogous to the two dimensional case, we would also find that “by sliding,” taking volumes by these parts of v , and then adding the results yet again gives us the final volume of the original parallelepiped with the vector v against the base. Essential to this addition preservation is thinking of positive volumes above the base (into the parallelepiped) and negative volumes below the base.

Let's consider each part *one at a time*. First, look at $(-2, 0, 0)$. We can “slide” (i.e. airdrop) by adding multiples of $(-2, 0, 0)$ to the vectors of the base to eliminate the x -coordinates (and the other coordinates are not affected):

$$\left(\begin{array}{ccc} 1 & 2 & -2 \\ 3 & 1 & 0 \\ 2 & 4 & 0 \end{array} \right) \longrightarrow \left(\begin{array}{ccc} 0 & 0 & -2 \\ 3 & 1 & 0 \\ 2 & 4 & 0 \end{array} \right)$$

Now, $(-2, 0, 0)$ is perpendicular (often called orthogonal in three dimensions) sharing no coordinates with our new base we have slid into: the parallelogram formed by $(0, 3, 2)$ and $(0, 1, 4)$. So the volume of this current part is

$$\text{Volume} = \text{height} \cdot \text{new base}$$

To tell if our oriented viewpoint of this new base is a positive one or a negative one, we consider whether it will take an even or an odd number of switches to put $(0, 3, 2)$ and $(0, 1, 4)$ into a proper viewpoint for viewing 2-dimensional area: x then y . *Every switch is a reflection of viewpoint. The sign of the volume/area switches from positive to negative or negative to positive.*

The positive view point of rectangular volume of a rectangle between e_1 , e_2 , and e_3 is:

- The base is positive itself in the xy -plane defined as e_2 off of e_1 .
- The vector coming off of the base is e_3 in the positive z direction.

The same switches which put the base as indicated into the xy -plane, put the vector off of the base in the z direction. So we only need to count switches that align the base properly. There may be a switch required between x and y and not z —so we should stick with counting switches which align the base properly.

To get $(0, 3, 2)$ into a proper viewpoint means: $(0, 3, 2) \rightarrow (3, 2, 0)$. Similarly, to get $(0, 1, 4)$ into a proper viewpoint: $(0, 1, 4) \rightarrow (1, 4, 0)$. If we want to think about two dimensional area the way we think about it in the xy plane, let's put it there. *We just want to shift our entries to the front.* Consider: $(0, y, z)$ changes to $(y, z, 0)$ with an even number of switches since

$$(0, y, z) \mapsto (y, 0, z) \mapsto (y, z, 0)$$

We change the orientation twice (*to negative and then back to positive*). Therefore, we can read the area of the base as the following 2-dimensional area *as is* (we do not change the sign)

$$\begin{pmatrix} + & - \\ 3 & 1 \\ 2 & 4 \end{pmatrix} \longrightarrow 3 \cdot 4 - 1 \cdot 2 = 10$$

We just used the same diagonal technique for computing area in the xy plane even though we were in the yz

plane! Therefore, the volume from the contribution of $(-2, 0, 0)$ is

$$-2 \cdot (3 \cdot 4 - 1 \cdot 2) = ((-2) \cdot 3 \cdot 4) - ((-2) \cdot 1 \cdot 2) = -20$$

Ok, now we go to the next part: $(0, 3, 0)$ sliding the vectors a and b to

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

To put $(x, 0, z)$ into $(x, z, 0)$ requires one switch. So our oriented viewpoint of the area of the base of this slid piece will be the negative of what we get from:

$$\begin{array}{c} + \\ \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \\ - \end{array} \longrightarrow 1 \cdot 4 - 2 \cdot 2 = 0 \xrightarrow{\text{change sign}} 0$$

Hence, the volume of this piece is

$$-3 \cdot (1 \cdot 4 - 2 \cdot 2) = -(3 \cdot 1 \cdot 4) + (3 \cdot 2 \cdot 2) = 0$$

Following the same logic, our last piece (with no switches required) comes from multiplying 1 to:

$$\begin{array}{c} + \\ \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \\ - \end{array} \longrightarrow 1 \cdot 1 - 2 \cdot 3 = -5$$

$$1 \cdot (1 \cdot 1 - 2 \cdot 3) = (1 \cdot 1 \cdot 1) - (1 \cdot 2 \cdot 3) = -5$$

Adding up all of the volumes yields:

$$(-20) + 0 + (-5) = -25$$

We call this number the oriented volume of the three vectors *in order* of base (a then b) *then* the (input) vector v . These vectors make up a square matrix:

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

The determinant of this square matrix is -25 . *It has negative oriented volume.* This means that our setup views the input vector v below the base formed by a and b .

The linear transformation that gives the oriented volume (determinant) off of the base formed by a and b is given by the matrix of signed projections:

$$\begin{pmatrix} +(10) & -(0) & +(-5) \end{pmatrix}$$

Plugging in the vector $(-2, 3, 1)$, we arrive at:

$$\begin{pmatrix} +(10) & -(0) & +(-5) \end{pmatrix} \cdot \begin{pmatrix} -2 \\ 3 \\ 1 \end{pmatrix} = -25$$

Notice that we have chosen the first two columns to be the base—this means that we fix them and then let the last column vector v be the input. One can check that the matrix of signed projections is indeed the cofactor function matrix c_v^T which is a linear transformation. If $g : \mathbb{R}^3 \rightarrow \mathbb{R}$ represents this transformation, then we have that its derivative matrix is exactly this matrix too:

$$Dg : \begin{pmatrix} g_x & g_y & g_z \end{pmatrix} = \begin{pmatrix} 10 & 0 & -5 \end{pmatrix}$$

6.5.3 The Cross Product

Suppose that g is the function that finds the volume of a parallelepiped off of two base vectors which themselves describe a plane. We have seen that the matrix for g is a cofactor function matrix. We also know that this matrix is the derivative matrix $\begin{pmatrix} g_x & g_y & g_z \end{pmatrix}$ of the function g . *What does this mean and why is this useful?* Suppose $(\Delta x, \Delta y, \Delta z)$ represents movement inside of the plane where the base is located. If we add such a vector $(\Delta x, \Delta y, \Delta z)$ onto a vector extending off of the base, it will not change the volume of the parallelepiped at all described by that vector off of the base—it just slides it. This means that the change in volume given by

$$\Delta g = \begin{pmatrix} g_x & g_y & g_z \end{pmatrix} \cdot \begin{pmatrix} \Delta x \\ \Delta y \\ \Delta z \end{pmatrix}$$

is 0. This means that the dot product of the cofactor vector and any vector *in the plane* is 0. *That is, the cofactor vector is orthogonal to the plane!* We give this vector a special name.

Cross Product

Given two column vectors u and w in \mathbb{R}^3 , create a 3×3 matrix A with any other column vector q so that $A = \begin{pmatrix} u & v & q \end{pmatrix}$. Then, we define the cross product between u and v as:

$$u \times v = c_q$$

where c_q is the vector of signed cofactors for the column q . It is the same no matter what the entries in q are.

Example 1. Let's compute the cross product $(1, 4, 3) \times (2, 1, -1)$. To do so, we create a matrix:

$$\begin{pmatrix} 1 & 2 & * \\ 4 & 1 & * \\ 3 & -1 & * \end{pmatrix}$$

and find the signed cofactors of $(*, *, *)$. Down the column $\begin{pmatrix} * \\ * \\ * \end{pmatrix}$ we have the signs $\begin{pmatrix} + \\ - \\ + \end{pmatrix}$ associated with the kitty-corner determinants as we find the cofactors. We have:

$$(1, 4, 3) \times (2, 1, -1) = \left(+ \det \begin{pmatrix} 4 & 1 \\ 3 & -1 \end{pmatrix}, - \det \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}, + \det \begin{pmatrix} 1 & 2 \\ 4 & 1 \end{pmatrix} \right) = (-7, 7, -7)$$

One of the important properties of the cross product is that it is orthogonal to the vectors involved.

Theorem 6.5.1

The cross product is orthogonal to each of the vectors involved.

$$(u \times v) \perp u \quad (u \times v) \perp v$$

Proof. The cross product is represented by a cofactor function in which if you plug in u or v , you would be computing the determinant of a matrix with a repeated column. Therefore, the result would be zero. Plugging in a vector into the cofactor matrix function (thought of as a row) is the same thing as taking a dot product. Having a zero dot product signifies orthogonality. \square

Example 2. Find the equation of the plane through the origin that contains the vectors $u = (1, 4, 3)$ and $w = (2, 1, -1)$. The plane itself is all points (i.e. vectors) (x, y, z) that are orthogonal to $u \times w = (-7, 7, -7)$. This condition is the same thing as saying that the dot product between (x, y, z) and $(-7, 7, -7)$ is 0:

$$(x, y, z) \bullet (-7, 7, -7) = 0$$

Evaluating this dot product, we get the equation of the plane:

$$-7x + 7y - 7z = 0.$$

Example 3. Let's suppose that the plane goes through the three points $(1, 1, -2)$, $(2, 0, 1)$, and $(-1, 1, 0)$. We want to find vectors that "lie" in the plane or that are parallel to it since this plane does not contain the origin. To do this we simply shift one of the points to the origin and apply that same shift to the other points. Let's shift $(-1, 1, 0)$ to the origin. To do that we add by its negative: $(1, -1, 0)$. Do this to one of the other points. Then, the vector originating at the origin and going to this new shifted point *will lie in the plane that has been shifted to the origin*. So, we take $u = (1, 1, -2) + (1, -1, 0) = (2, 0, -2)$ and $v = (2, 0, 1) + (1, -1, 0) = (3, -1, 1)$. Then, u and v are parallel to our plane. If we find the equation of the plane that contains u and v , we can then shift that plane back to pass through $(1, -1, 0)$.

We take $u \times v = (-2, -8, -2)$. Then, $(-2, -8, -2) \bullet (x, y, z) = -2x - 8y - 2z = 0$ is the equation of the parallel plane through the origin. But we want an equation of a plane that is parallel to this that passes through $(1, -1, 0)$. Take a point (x, y, z) and shift it in the same way that takes $(1, -1, 0)$ to the origin. That is, we add by the negative $(-1, 1, 0)$ so we get $(x - 1, y + 1, z)$. Now we would like $(x - 1, y + 1, z)$ to be in this plane $-2x - 8y - 2z = 0$ that passes through the origin. So the equation of this plane should hold if we plug in $x - 1$ for x , $y + 1$ for y and z for z :

$$-2(x - 1) - 8(y + 1) - 2z = 0.$$

What we now have is an equation that gives the condition for (x, y, z) to be in our desired plane. This last equation is the equation of our desired plane.

Note that if we switch the order $u \times v$ versus $v \times u$, then we switch columns in all of the submatrices for which we compute determinants. The effect?

Theorem 6.5.2 Anticommutativity of The Cross Product

$$u \times v = -v \times u.$$

In fact, we can get a lot of properties about cross products simply from being able to express them as tuples of wedge products:

Cross Product by Wedge Product

We can equivalently express the cross product in terms of the wedge product \wedge :

$$u \times v = (dy \wedge dz(u, v), dz \wedge dx(u, v), dx \wedge dy(u, v))$$

Remember that wedge products give multilinear transformations. Tuples of wedge products can also give multilinear transformations.

Theorem 6.5.3

The cross product is a bilinear transformation.

Proof. We can write:

$$u \times v = \underbrace{dy \wedge dz(u, v) \cdot e_1}_{\text{a bilinear transformation}} + \underbrace{dz \wedge dx(u, v) \cdot e_2}_{\text{a bilinear transformation}} + \underbrace{dx \wedge dy(u, v) \cdot e_3}_{\text{a bilinear transformation}}$$

It is not hard to check that simply multiplying the scalar output of a bilinear transformation whose codomain is \mathbb{R} by a vector is again a bilinear transformation. Therefore, it suffices to prove that a sum of bilinear transformations which have the same input (u, v) is again bilinear. This is an exercise! \square

Do you know what this means? The cross product is linear in each component. Thus, our wedge product equivalence leads to the following properties of the cross product.

Theorem 6.5.4 Bilinear Properties of the Cross Product

- $u \times (v + w) = u \times v + u \times w$
- $u \times (kv) = k \cdot (u \times v)$

Theorem 6.5.5 Zero Cross Product

Let $u \in \mathbb{R}^3$. Then:

$$u \times u = (0, 0, 0)$$

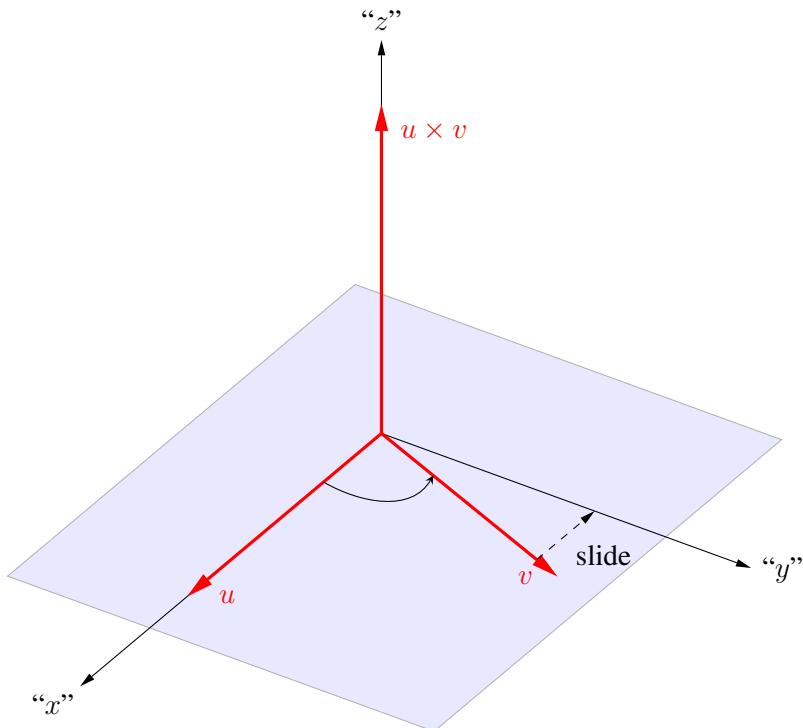
Proof. This is an exercise! Just use our cofactor function definition of cross product. \square

Theorem 6.5.6

The volume of a parallelepiped in \mathbb{R}^3 with vector w coming off of a base formed by vectors u and v is given by the absolute value of $(u \times v) \bullet w$.

Proof. This is an exercise! Just use our cofactor function definition of cross product. Think of the cofactor function as a row and the input as a column. Is plugging in the same as taking a dot product? \square

We have discussed some properties of the cross product. We even know $(u \times v) \perp u$ and $(u \times v) \perp v$. But do we know how to picture it? The cross product comes from the process of taking a determinant. Sliding *just in the first two columns* (i.e. column airdropping in this case) does not change the determinants of the 2×2 submatrices—that is, it does not change the *cross product!* We can slide v so that u and v appear orthogonal to each other as follows and then think of pretend xyz axes. The cross product $u \times v$ then goes along the pretend positive z axis in the same way that $e_1 \times e_2 = e_3$ (convince yourself that $e_1 \times e_2 = e_3$).



The vector $u \times v$ points in the direction that would yield a *positive* volume parallelepiped. This is because to get the volume of the parallelepiped of $u \times v$ off of the base parallelogram, you plug $u \times v$ into the cofactor function represented by $u \times v$. To do this, compute the dot product $(u \times v) \bullet (u \times v)$ which is positive since it is just a sum of squares. So the cross product should be in the direction of positive volume.

So, look at the plane where u and v lie. Then, look at this plane from the side in which v is closer in a counterclockwise rotation from u (where the parallelogram is positive). *This is the side of the plane that $u \times v$ will come out of!*

The wedge product description of the cross product

$$u \times v = (dy \wedge dz(u, v), dz \wedge dx(u, v), dx \wedge dy(u, v))$$

emphasizes that the components of the cross product are the *areal projections* of the parallelogram formed by u and v onto the yz , zx , or xy planes.

Let's consider how we can think about the actual area of the parallelogram between u and v . This area is the area of the base of the parallelepiped that the cofactor function gives the volume for. If we plug in a vector that is orthogonal to the base and has a length of 1, then the volume should be the same as the area. We know that the cross product $u \times v$ is orthogonal. We also know that plugging into the cofactor function is the same as taking the dot product with the cross product. Hence, the area of the parallelogram between u and v is:

$$(u \times v) \bullet \frac{u \times v}{|u \times v|} = \frac{(u \times v) \bullet (u \times v)}{|u \times v|} = \frac{|u \times v|^2}{|u \times v|} = |u \times v|.$$

Wait! This is like the Pythagorean theorem for area projections instead of length projections:

Area of a Parallelogram

The area of a parallelogram formed by two vectors $u, v \in \mathbb{R}^3$ is given by:

$$\sqrt{(dy \wedge dz(u, v))^2 + (dx \wedge dz(u, v))^2 + (dx \wedge dy(u, v))^2}$$

where since we are squaring, we do not worry about the order of wedging.

This same idea extends to the parallelogram between two vectors that lives in a higher dimensional space like \mathbb{R}^4 :

Area of a Parallelogram in \mathbb{R}^4

The area of a parallelogram formed by two vectors $u, v \in \mathbb{R}^4$ where coordinates are given by (x, y, z, w) is given by:

$$\sqrt{(dy \wedge dz(u, v))^2 + (dx \wedge dz(u, v))^2 + (dx \wedge dy(u, v))^2 + (dx \wedge dw(u, v))^2 + (dy \wedge dw(u, v))^2 + (dz \wedge dw(u, v))^2}$$

Proof. We only give a sketch. Instead of using a dot product which we can when we have a cofactor expansion, we actually are using another kitty-corner technique for the determinant to get six 2×2 submatrices down two columns of a 4×4 matrix. This was another technique based upon different permutation cosets. The only problem is that we have the two columns u and v . What about the other two columns? They need to be chosen so that the four dimensional volume computed by the determinant is equal the desired area. We also need all six products that we add to be the squares of the determinants of the 2×2 submatrices found from the columns u and v . We work out the details in section 7.2. \square

Example 4. Let's find the area of the parallelogram formed by the two vectors $u = (1, 2, 1)$ and $v = (0, 1, 1)$. We just need the squares of the areal projections. We do not even need to think about which areal projection

we are taking or whether they are positive or negative. It suffices just to consider the determinants of the three 2×2 submatrices of

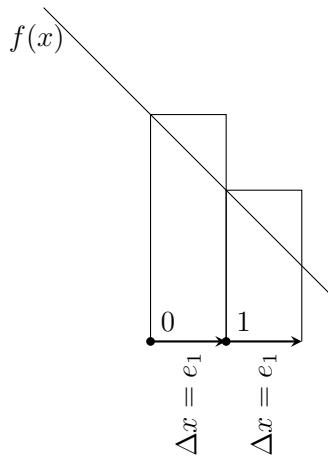
$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 1 & 1 \end{pmatrix}$$

We find:

$$\begin{aligned} & \sqrt{\left(\det\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\right)^2 + \left(\det\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right)^2 + \left(\det\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\right)^2} \\ & = \sqrt{1^2 + 1^2 + 1^2} = \sqrt{3}. \end{aligned}$$

6.5.4 Wedge Products on Surfaces

Suppose that $f(x) = 3 - x$. The expression “ $f(x)dx$ ” where dx is the function that picks out the x -coordinate of a vector in \mathbb{R}^1 gives us a rule for finding areas of rectangles as follows:



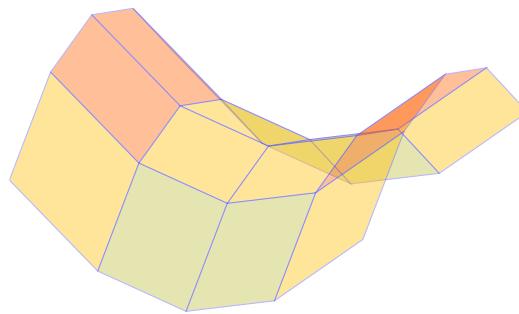
- To find the area of the first rectangle, we use the x value 0 *at the beginning of the subinterval* and we input the vector e_1 corresponding to Δx having length 1 into $f(x)dx$: $\underbrace{f(0)dx(e_1)}_{3} = 3$.
- To find the area of the second rectangle, we use the x value 1 *at the beginning of the subinterval* and we input the vector e_1 corresponding to Δx having length 1 into $f(x)dx$: $\underbrace{f(1)dx(e_1)}_{2} = 2$.
- Add the two rectangle areas together to get an approximation:

$$\int_0^2 3 - x \, dx \approx \underbrace{f(0)dx(e_1)}_3 + \underbrace{f(1)dx(e_1)}_2 = 5$$

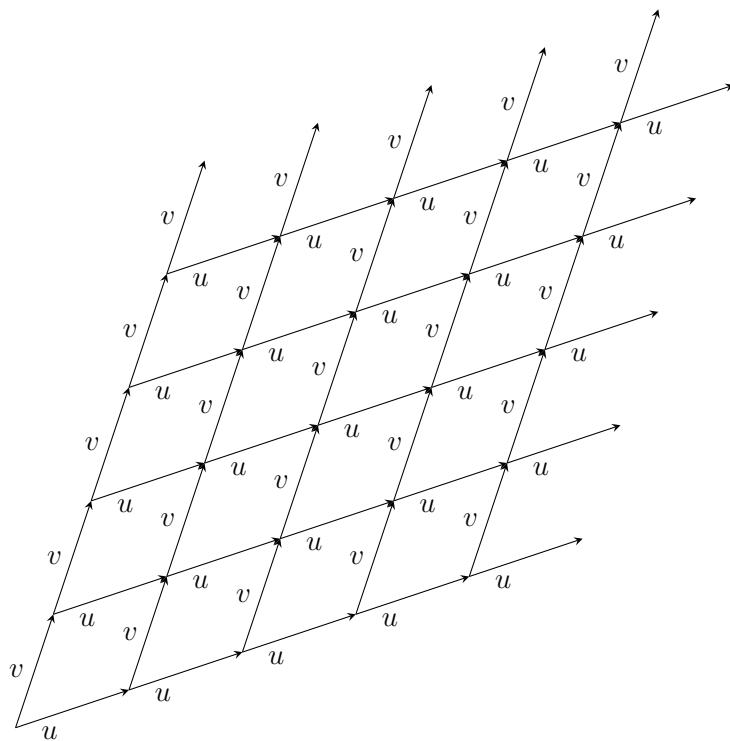
Yet, let's stop thinking of rectangle areas and just think that we have:

$$\frac{f(0)dx(e_1) = 3}{\Delta x = e_1} \rightarrow \frac{f(1)dx(e_1) = 2}{\Delta x = e_1}$$

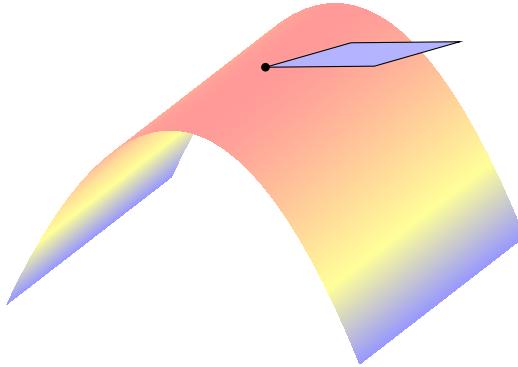
Over the interval $[0, 2]$, we had two subintervals. The expression $f(x)dx$ gives us a rule that assigns numbers to each subinterval. Then add these numbers up to get an approximation to the integral. We want to generalize this notion so we can integrate not only across the x -axis, but on surfaces and through volumes! The key is *wedge product expressions*. They give us number outputs. For instance, suppose that we would like to subdivide a surface into approximating *flat* parallelograms or rectangles as follows:



When we do so, each rectangle or parallelogram is formed by vectors. To keep things *oriented*, imagine starting with the following type of *flow between the vectors* forming the parallelograms and then bending such a grid onto the surface:



These are approximating parallelograms on the surface—*they are part of the tangent plane to the surface at the point where the vectors u and v start. So they are not really “bent” per se—but placed there.*



Want we want is a *number* associated with each parallelogram. We add these up and we get a sum. As these parallelograms get smaller and smaller (just as subintervals get smaller and smaller) we want the sum to converge to something—an integral. This integral can give us data about the surface. Let’s talk about this data briefly in a minute.

But first, how should we form our rules for how to get a number from each parallelogram? We use a wedge product expression like

$$xdy \wedge dz(u, v) - ydx \wedge dz(u, v) + zdx \wedge dy(u, v)$$

Notice that this expression changes as (x, y, z) changes and as (u, v) moves from one parallelogram to another. We pick the (x, y, z) at the tails of u and v in each parallelogram.

Now notice that $xdy \wedge dz$ focuses on a areal projection to the yz plane. So perhaps whatever we are measuring is proportional to how close this parallelogram is to being parallel to this plane. Perhaps there is a fluid flowing in a certain direction and this is a permeable surface. But the amount of fluid that passes through the surface depends on how much the direction of flow is orthogonal to the surface at that point. This is just one example of what a surface integral might tell us. But we do not get into those applications and details in this book. Simply, we look at how the wedge product can help us work with such integrals.

If we want to integrate our wedge product expression over a surface S , we would write:

$$\int_S xdy \wedge dz - ydx \wedge dz + zdx \wedge dy$$

The finer and finer our parallelogram mesh is the closer and closer our sums get together—they converge and limit to this “integral.” Integration techniques for these are learned in a multivariable calculus course. But what we discuss is how we can work with and change the wedge product expression. Let’s give a definition:

***n*-form**

We call a wedge product expression like $x^2dx + xydy$ a 1-form, an expression like $z^3dx \wedge dz - ydy \wedge dz$ a 2-form, an expression like $(6z + x)dy \wedge dz \wedge dx$ a 3-form and so forth.

Integral of a n -form over a n -dimensional region

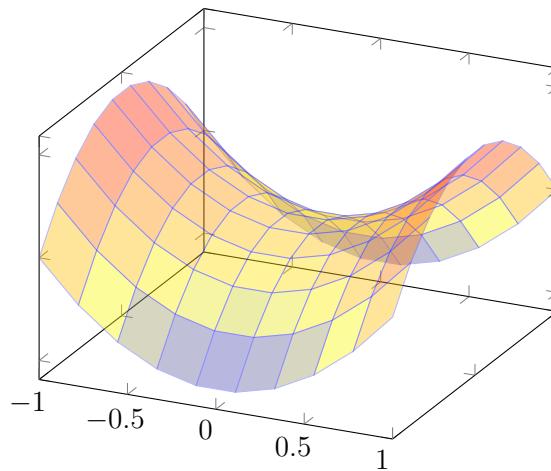
Create a mesh of n -dimensional parallelograms (parallelepipeds) over your region. The n -form gives a rule for how to get a number from each piece of the mesh. If the sums of these numbers get closer and closer to a number as we make the mesh finer and finer, we call that number the integral of the n -form over the region.

Integral of a Constant n -form

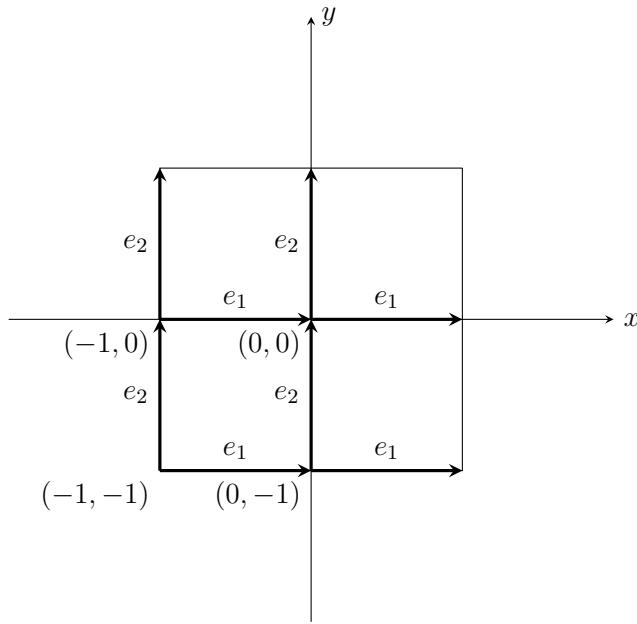
We say that a n -form is constant if it looks something like $1 \cdot dx \wedge dy$ (this is an example of a 2-form) where the expression in front “1” is just a constant. Any parallelogram mesh approximation to an integral *in this case* is *exact!* We are actually finding the integral itself when we use the approximation technique.

6.5.5 Surface Area

Example 5. Let's use a 2-form to approximate the surface area of $z = x^2 - y^2$ over the square $-1 \leq x \leq 1$ and $-1 \leq y \leq 1$:



But we will do so with only 4 parallelograms. These will lie above the following squares in the xy -plane:



The projection of the u vector of the parallelogram to the xy -plane will be e_1 , and the projection of v will be e_2 . We remember that to compute the area of a parallelogram with vector v coming off of base u , we compute:

$$\sqrt{(dy \wedge dz(u, v))^2 + (dx \wedge dz(u, v))^2 + (dx \wedge dy(u, v))^2}$$

Our goal is to change this expression so that it only has dx and dy in it. Then we will have an expression we can move across our squares in the xy -plane.

We realize that the rule for going from Δx and Δy to Δz is just given by the derivative of $z = g(x, y) = x^2 - y^2$ which is $Dg : \begin{pmatrix} g_x & g_y \end{pmatrix} = \begin{pmatrix} 2x & -2y \end{pmatrix}$. We just plug in $(\Delta x, \Delta y)$ as a column into this matrix function and we get out Δz :

$$\Delta z = \begin{pmatrix} 2x & -2y \end{pmatrix} \cdot \begin{pmatrix} \Delta x \\ \Delta y \end{pmatrix} = 2x\Delta x - 2y\Delta y$$

Now, remember that $\Delta z = dz(\Delta x, \Delta y, \Delta z)$. The symbols dx , dy , and dz are just rules that pick out components of vectors. So, we can write down:

$$dz(\Delta x, \Delta y, \Delta z) = (1 + y)dx(\Delta x, \Delta y, \Delta z) + xdy(\Delta x, \Delta y, \Delta z)$$

This tells us that rule to go from the linear functions dx and dy to the linear function dz is:

$$dz = 2xdx - 2ydy$$

Therefore, we think:

$$dx \wedge dz = dx \wedge (2xdx - 2ydy)$$

$$= 2x \underbrace{dx \wedge dx}_0 - 2y dx \wedge dy = -2y dx \wedge dy$$

We also have that

$$dy \wedge dz = dy \wedge (2xdx - 2ydy) = 2xdy \wedge dx - 2y \underbrace{dy \wedge dy}_0 = -2x \underbrace{dx \wedge dy}_{\text{switched order}}$$

Therefore, we have:

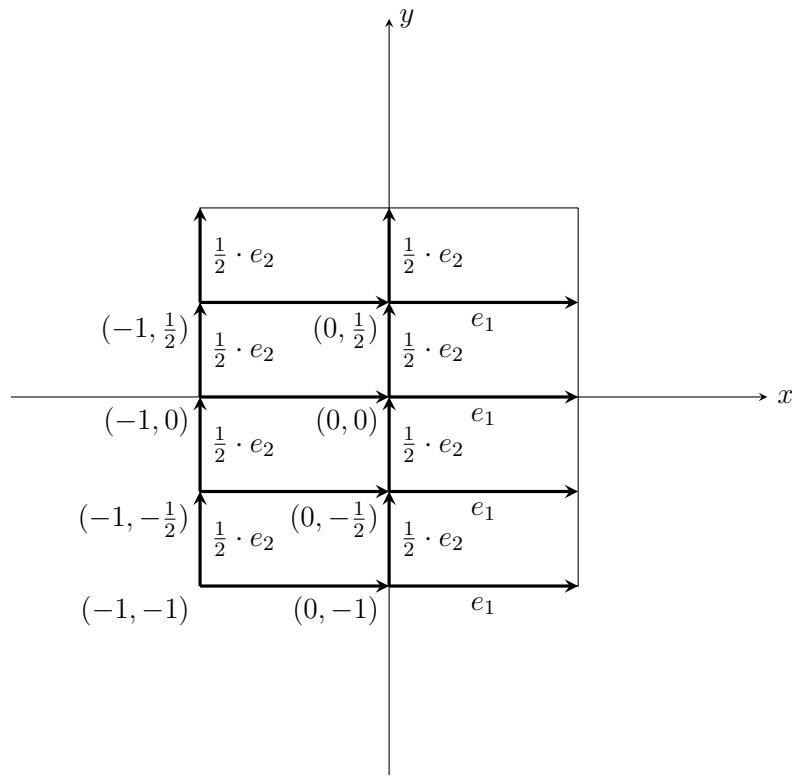
$$\begin{aligned} & \sqrt{(dy \wedge dz(u, v))^2 + (dx \wedge dz(u, v))^2 + (dx \wedge dy(u, v))^2} \\ &= \sqrt{\underbrace{(-2xdx \wedge dy(u, v))^2}_{dx \wedge dz} + \underbrace{(-2ydx \wedge dy(u, v))^2}_{dy \wedge dz} + (dx \wedge dy(u, v))^2} \\ &= \sqrt{((-2x)^2 + (-2y)^1 + 1) \cdot (dx \wedge dy(u, v))^2} = \sqrt{4x^2 + 4y^2 + 1} \cdot dx \wedge dy(u, v) \end{aligned}$$

Using this rule on our parallelograms reduces to just using it on the projections of the parallelograms to the xy -plane which are precisely the squares we are interested in. So, we have four squares in the xy -plane to plug into this 2-form. We take the (x, y) value at the lower left corner of each since this is where the tails of the (u, v) projections to (e_1, e_2) are.

- Square at $(-1, 0)$: $\sqrt{4 \cdot (-1)^2 + 4 \cdot 0^2 + 1} \cdot dx \wedge dy(e_1, e_2) = \sqrt{5}$
- Square at $(-1, -1)$: $\sqrt{4 \cdot (-1)^2 + 4 \cdot (-1)^2 + 1} \cdot dx \wedge dy(e_1, e_2) = 3$
- Square at $(0, -1)$: $\sqrt{4 \cdot (0)^2 + 4 \cdot (-1)^2 + 1} \cdot dx \wedge dy(e_1, e_2) = \sqrt{5}$
- Square at $(0, 0)$: $\sqrt{4 \cdot (0)^2 + 4 \cdot (0)^2 + 1} \cdot dx \wedge dy(e_1, e_2) = 1$

Therefore, our approximation to the surface area is $4 + 2\sqrt{5} \approx 8.47213595499958$.

Example 6. We can get an even better approximation to this last example by using more parallelograms. To do this, we can just consider what is happening on the xy -plane and then project that up onto the surface. So we just further partition our squares into *eight rectangles*:



- Rectangle at $(-1, 0)$: $\sqrt{4 \cdot (-1)^2 + 4 \cdot 0^2 + 1} \cdot dx \wedge dy (e_1, \frac{1}{2} \cdot e_2) = \frac{\sqrt{5}}{2}$
- Rectangle at $(-1, -1)$: $\sqrt{4 \cdot (-1)^2 + 4 \cdot (-1)^2 + 1} \cdot dx \wedge dy (e_1, \frac{1}{2} \cdot e_2) = \frac{3}{2}$
- Rectangle at $(0, -1)$: $\sqrt{4 \cdot (0)^2 + 4 \cdot (-1)^2 + 1} \cdot dx \wedge dy (e_1, \frac{1}{2} \cdot e_2) = \frac{\sqrt{5}}{2}$
- Rectangle at $(0, 0)$: $\sqrt{4 \cdot (0)^2 + 4 \cdot (0)^2 + 1} \cdot dx \wedge dy (e_1, \frac{1}{2} \cdot e_2) = \frac{1}{2}$
- Rectangle at $(-1, \frac{1}{2})$: $\sqrt{4 \cdot (-1)^2 + 4 \cdot (\frac{1}{2})^2 + 1} \cdot dx \wedge dy (e_1, \frac{1}{2} \cdot e_2) = \frac{\sqrt{6}}{2}$
- Rectangle at $(-1, -\frac{1}{2})$: $\sqrt{4 \cdot (-1)^2 + 4 \cdot (-\frac{1}{2})^2 + 1} \cdot dx \wedge dy (e_1, \frac{1}{2} \cdot e_2) = \frac{\sqrt{6}}{2}$
- Rectangle at $(0, -\frac{1}{2})$: $\sqrt{4 \cdot (0)^2 + 4 \cdot (-\frac{1}{2})^2 + 1} \cdot dx \wedge dy (e_1, \frac{1}{2} \cdot e_2) = \frac{\sqrt{2}}{2}$
- Rectangle at $(0, \frac{1}{2})$: $\sqrt{4 \cdot (0)^2 + 4 \cdot (\frac{1}{2})^2 + 1} \cdot dx \wedge dy (e_1, \frac{1}{2} \cdot e_2) = \frac{\sqrt{2}}{2}$

Adding these up, we have:

$$\sqrt{6} + \sqrt{5} + \sqrt{2} + 2 \approx 8.09977128265606$$

Or we can use technology:



[Link to run the code.](#)

```
var('y')
integral(integral(sqrt(4*x^2+4*y^2+1),x,-1,1),y,-1,1).n()
```

This gives us an extremely accurate approximation: 7.44625672301236. Both of our previous approximations were over estimates. But nonetheless, we have found a rule that we can apply to rectangles/parallelograms on the xy -plane to help us find surface area.

Finding Approximate Surface Area

To find surface area, start with the 2-form:

$$\sqrt{(dy \wedge dz(u, v))^2 + (dx \wedge dz(u, v))^2 + (dx \wedge dy(u, v))^2}$$

Use derivatives to relate dz to dx and dy and simplify to a 2-form that looks like:

$$(\text{expression}) \cdot dx \wedge dy(u, v)$$

Then, divide the shadow of the surface on the xy -plane into rectangles (or parallelograms) and plug these into the 2-form. Lastly, add up the results.

6.5.6 Changing Coordinates

For this section, we assume familiarity with polar and cartesian coordinates.

Example 7. The wedge product can also be used to change coordinates in an n -form. For instance, if we want to change from cartesian to polar, we think:

$$x = r \cos(\theta) \quad y = r \sin(\theta).$$

This means that after taking the derivative of $x(r, \theta)$ as a function $\mathbb{R}^2 \rightarrow \mathbb{R}$ and same with $y(r, \theta)$, that:

$$\Delta x = \begin{pmatrix} \cos(\theta) & -r \sin(\theta) \end{pmatrix} \cdot \begin{pmatrix} \Delta r \\ \Delta \theta \end{pmatrix} \quad \Delta y = \begin{pmatrix} \sin(\theta) & r \cos(\theta) \end{pmatrix} \cdot \begin{pmatrix} \Delta r \\ \Delta \theta \end{pmatrix}$$

Now think of a vector v which is equal to $(\Delta x, \Delta y)_{xy}$ in xy -coordinates and is equal to $(\Delta r, \Delta \theta)_{r\theta}$ in $r\theta$ -coordinates. The linear function dx picks out the x coordinate, dy picks out the y coordinate, dr picks out the r coordinate and $d\theta$ picks out the θ coordinate. Therefore,

$$dx(v) = \Delta x \quad dy(v) = \Delta y \quad dr(v) = \Delta r \quad d\theta(v) = \Delta \theta$$

So, we can write:

$$dx = \begin{pmatrix} \cos(\theta) & -r \sin(\theta) \end{pmatrix} \cdot \begin{pmatrix} dr \\ d\theta \end{pmatrix} \quad dy = \begin{pmatrix} \sin(\theta) & r \cos(\theta) \end{pmatrix} \cdot \begin{pmatrix} dr \\ d\theta \end{pmatrix}$$

Hence,

$$dx \wedge dy = (\cos(\theta)dr - r \sin(\theta)d\theta) \wedge (\sin(\theta)dr + r \cos(\theta)d\theta)$$

The only two terms that survive in the FOIL with the \wedge are:

$$\begin{aligned} & \cos(\theta)dr \wedge r \cos(\theta)d\theta - r \sin(\theta)d\theta \wedge \sin(\theta)dr \\ &= r \cos^2(\theta)dr \wedge d\theta + r \sin^2(\theta)dr \wedge d\theta = rdr \wedge d\theta \end{aligned}$$

This means that if we can express our region in terms of polar coordinates, then we would replace $dx \wedge dy$ in the integral with $rdr \wedge d\theta$.

How to Change Coordinates in an n -form

Just rewrite the d variable's in terms of the others by using derivatives. Then use the wedge product between these.

Let's see how we can use the change of coordinates we just found:

Example 8. Suppose that we want to compute the surface area of $z = x^2 - y^2$ over a circular region in the xy -plane. Suppose that the region is centered at the origin and has a radius of 2. Then, we change our 2-form which we used above for the surface area of $z = x^2 - y^2$ using the change we just found:

$$\sqrt{\underbrace{4x^2 + 4y^2}_{=4r^2} + 1} \cdot dx \wedge dy \mapsto \sqrt{4r^2 + 1} \cdot rdr \wedge d\theta$$

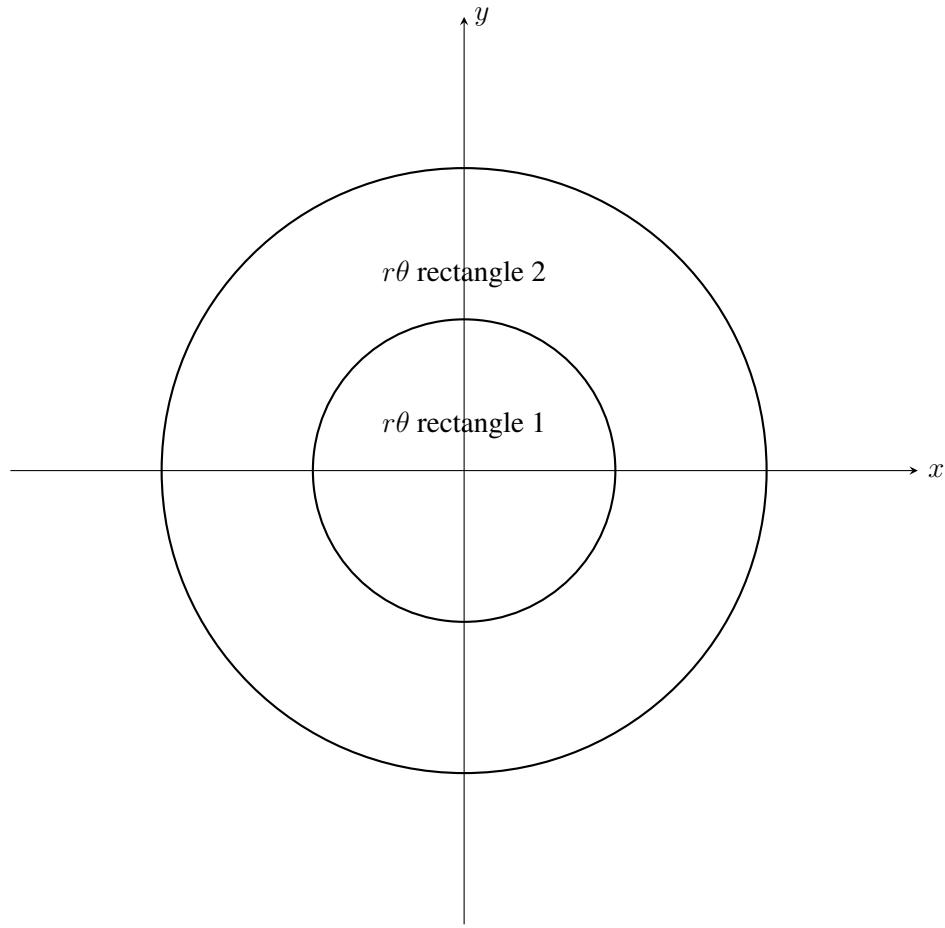
To get the circle we want can be done with two rectangles in $r\theta$ -coordinates where e_1 refers to r and e_2 refers to θ :

- Rectangle 1 at $(0, 0)$ where $0 \leq r \leq 1$ and $0 \leq \theta \leq 2\pi$:

$$\sqrt{4r^2 + 1} \cdot rdr \wedge d\theta(e_1, 2\pi \cdot e_2) = 0$$

- Rectangle 2 at $(1, 0)$ where $1 \leq r \leq 2$ and $0 \leq \theta \leq 2\pi$:

$$\sqrt{4r^2 + 1} \cdot rdr \wedge d\theta(e_1, 2\pi \cdot e_2) = 2\pi \cdot \sqrt{5}$$



Example 9. Let's think about another way that we can think about changing from cartesian to polar coordinates dealt with in the last couple of examples. Remember that we had a wedge product:

$$\underbrace{(\cos(\theta)dr - r\sin(\theta)d\theta)}_{dx} \wedge \underbrace{(\sin(\theta)dr + r\cos(\theta)d\theta)}_{dy}$$

Also remember that we can take the determinant of a matrix by dualizing the columns and taking the wedge product between them. That is, take the vectors:

$$a = (\cos(\theta), -r\sin(\theta)) \quad b = (\sin(\theta), r\cos(\theta))$$

and put them into the matrix:

$$J = \begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -r\sin(\theta) & r\cos(\theta) \end{pmatrix}$$

To take the determinant of this matrix by wedge product with respect to the ordered coordinates (r, θ) , we

dualize a and b with respect to these coordinates:

$$\underbrace{a^* = \cos(\theta)dr - r \sin(\theta)d\theta}_{dx} \quad \underbrace{b^* = \sin(\theta)dr + r \cos(\theta)d\theta}_{dy}$$

To find $\det(J)$, we compute:

$$\underbrace{a^* \wedge b^*}_{dx \wedge dy} = \underbrace{(\cos(\theta)dr - r \sin(\theta)d\theta)}_{a^*} \wedge \underbrace{(\sin(\theta)dr + r \cos(\theta)d\theta)}_{b^*}$$

After simplifying as we did above, we look at the ending coefficient of $dr \wedge d\theta$ (since the order of coordinates is “ r ” then “ θ ”) to get $\det(J)$:

$$\underbrace{r}_{\det(J)} dr \wedge d\theta$$

So what could we have done at the beginning? We could have taken the derivative of the change of coordinates function $g : (r, \theta) \mapsto (\underbrace{r \cos(\theta)}_x, \underbrace{r \sin(\theta)}_y)$ and gotten:

$$Dg : \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -r \sin(\theta) & r \cos(\theta) \end{pmatrix}$$

and we get the matrix J . That is, just take the determinant of the derivative matrix J of the change of coordinates function g and multiply it to the wedge product $dr \wedge d\theta$.

Jacobian Matrix

The Jacobian matrix of a change of coordinates function is simply the first derivative matrix of that change of coordinates function.

Theorem 6.5.7

To change coordinates of an n -form from $da_1 \wedge da_2 \wedge \cdots \wedge da_n$ to $db_1 \wedge db_2 \wedge \cdots \wedge db_n$, take the change of coordinates function g from the *new coordinates* (b_1, \dots, b_n) to the *old coordinates* (a_1, \dots, a_n) . Let J be the Jacobian (first derivative matrix) of g . Then:

$$da_1 \wedge da_2 \wedge \cdots \wedge da_n = \det(J) \cdot db_1 \wedge db_2 \wedge \cdots \wedge db_n$$

We do not have to use this theorem. Instead, just play with wedge products as we did in the first change of coordinates example. Still, more insight allows more flexibility in our calculations.

Example 10. This example assumes knowledge of cylindrical and spherical coordinates. Suppose that we want to change $\underbrace{dx \wedge dy \wedge dz}_{\text{cartesian}}$ to be in terms of $\underbrace{d\rho \wedge d\phi \wedge d\theta}_{\text{spherical}}$. We do this in two steps:

$$\underbrace{dx \wedge dy \wedge dz}_{\text{cartesian}} \longrightarrow \underbrace{dr \wedge d\theta \wedge dz}_{\text{cylindrical}} \longrightarrow \underbrace{d\rho \wedge d\phi \wedge d\theta}_{\text{spherical}}$$

First, we realize that to change from cartesian to cylindrical is the same thing as changing from cartesian (x, y) to polar (r, θ) and keeping z alone. We already know that $dx \wedge dy = rdr \wedge d\theta$ from our examples above. Hence,

$$dx \wedge dy \wedge dz = \underbrace{rdr \wedge d\theta}_{dx \wedge dy} \wedge dz$$

Now we change this to spherical coordinates (ρ, ϕ, θ) using:

$$r = \rho \sin(\phi) \quad z = \rho \cos(\phi)$$

Using these equations, we find:

$$dr = \sin(\phi)d\rho + \rho \cos(\phi)d\phi \quad dz = \cos(\phi)d\rho - \rho \sin(\phi)d\phi$$

Therefore,

$$dx \wedge dy \wedge dz = \underbrace{rdr \wedge d\theta \wedge dz}_{dx \wedge dy} = r \cdot \underbrace{(\sin(\phi)d\rho + \rho \cos(\phi)d\phi)}_{dr} \wedge d\theta \wedge \underbrace{(\cos(\phi)d\rho - \rho \sin(\phi)d\phi)}_{dz}$$

In the “FOIL”, we throw out the “F” and the “L” so we do not have repeats. We also collect the multipliers to the front of the wedge products:

$$\underbrace{(r \sin(\phi))(-\rho \sin(\phi))d\rho \wedge d\theta \wedge d\phi}_{\text{“O”}} + \underbrace{(\rho \cos(\phi))(\cos(\phi))d\phi \wedge d\theta \wedge d\rho}_{\text{“I”}}$$

One swap changes $d\rho \wedge d\theta \wedge d\phi$ to $d\rho \wedge d\phi \wedge d\theta$ and two swaps changed $d\phi \wedge d\theta \wedge d\rho$ to $d\phi \wedge d\theta \wedge d\rho$ so that we have:

$$(-1)^1(r \sin(\phi))(-\rho \sin(\phi))d\rho \wedge d\phi \wedge d\theta + (-1)^2(\rho \cos(\phi))(\cos(\phi))d\rho \wedge d\phi \wedge d\theta$$

$$= (r\rho) \underbrace{(\sin^2(\phi) + \cos^2(\phi))}_{=1} d\rho \wedge d\phi \wedge d\theta = r\rho d\rho \wedge d\phi \wedge d\theta$$

This should make sense if one realizes that changing from (z, r) to (ρ, ϕ) is exactly like changing from cartesian to polar with an angle ϕ . So we would be multiplying by ρ just like when we change from (x, y) to (r, θ) we multiply by r .

Using $r = \rho \sin(\phi)$, we have that $r\rho = \rho^2 \sin(\phi)$. Now we could have reached the same conclusion if we used the direct change of coordinates function:

$$g(\rho, \phi, \theta) = (\underbrace{\rho \sin(\phi) \cos(\theta)}_x, \underbrace{\rho \cos(\phi) \cos(\theta)}_y, \underbrace{\rho \cos(\phi)}_z)$$

and then took the determinant of its first derivative matrix (i.e. Jacobian):

$$\det \begin{pmatrix} \sin(\phi) \cos(\theta) & \sin(\phi) \sin(\theta) & \cos(\phi) \\ \rho \cos(\phi) \cos(\theta) & \rho \cos(\phi) \sin(\theta) & -\rho \sin(\phi) \\ -\rho \sin(\phi) \sin(\theta) & \rho \sin(\phi) \cos(\theta) & 0 \end{pmatrix} = \rho^2 \sin(\phi)$$

Computationally both methods work—but the latter involves more factoring and writing things out. Or we could have found the Jacobian for changing from cartesian to cylindrical and also for cylindrical to spherical. Multiplying the determinants of these two Jacobians would again yield $\rho^2 \sin(\phi)$.

6.5.7 Stoke's Theorem via Wedges

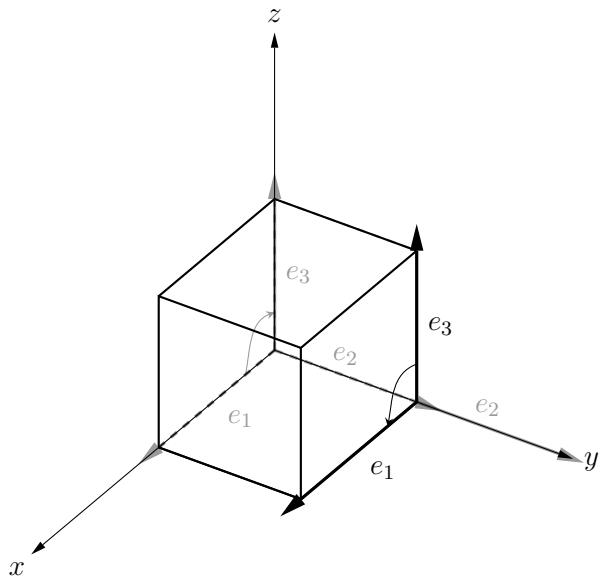
We tackle the following question:

Suppose we have a surface that simply and completely encloses a volume inside of it—like the surface of a football. How we can change a 2-form to a 3-form so that the surface integral of the 2-form is the same as volume integral (using approximating parallelepipeds) of the 3-form?

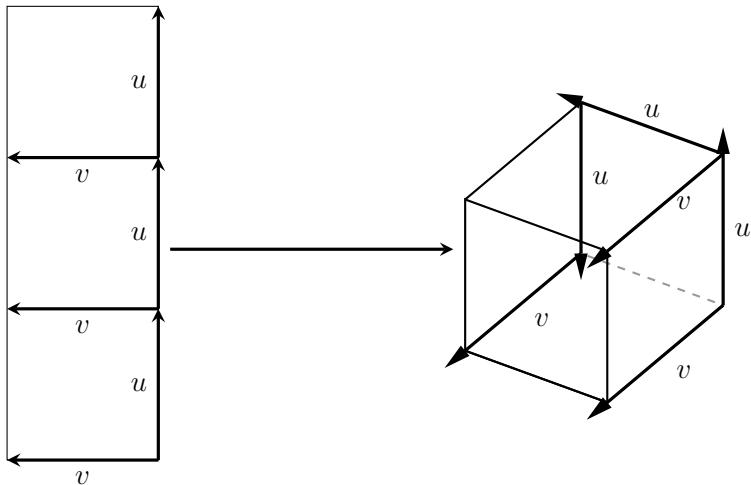
This question can be answered by first considering:

Can we find a 3-form with input (u, v, w) whose output is the same as a given 2-form with input (u, v) if we require that (u, v) gives a positive area parallelogram and (u, v, w) gives a positive volume parallelepiped?

Example 11. To answer this question, let's consider a simple scenario of an integral over a surface. Consider the following box whose faces comprise a parallelogram mesh for an integration:



Now how do the faces comprise a mesh with a flow of vectors (u, v) ? We picture just three of the parallelograms (squares) bent onto the faces:



Suppose that we would like to integrate $ydx \wedge dz$ over this surface. We will use $ydx \wedge dz$ as a rule to get a number for each face. The wedge product $dx \wedge dz$ looks at an areal projection onto the zx plane. Only two faces actually have a nonzero projection onto this plane—the faces at $y = 0$ and $y = 1$. With the mesh we have chosen, the face at $y = 1$ will be positively oriented from our current view point from the outside. That is, $+e_2$ will yield positive volume coming off of it. On this face, the vector e_1 comes off of the base of e_3 in a counterclockwise orientation.

In order to keep with this positive orientation with the (u, v) flow of the mesh, the face on the opposite side must yield positive volume when $-e_2$ going the other way comes off of the base. Therefore, the face at $y = 0$ viewed from the other side of our current view has e_1 coming off of a base of e_3 .

Let's focus on the face at $y = 1$:

$$dx \wedge dz \begin{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\ e_3 \quad e_1 \end{pmatrix} = \det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1$$

This is a 2-form. Now, how can we get a 3-form that will give us this same output if we plug in (e_3, e_1, e_2) ?

Note: We use e_2 since e_2 is in the direction of positive volume off of our base parallelogram of (e_3, e_1) .

We have put a gap between the rows of $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

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

Now,

$$\det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = (-1)^{\text{necessary switches}} \underbrace{C_{23}}_{\text{cofactor}}$$

The number of switches is the same as how many switches we need to change $(x, 0, z)$ to $(x, z, 0)$. This number of switches is exactly the same number of switches to push the y position in the third column to the bottom: $(0, y, 0) \mapsto (0, 0, y)$. *But this is also the same number of switches to push y to the top! (One switch for both.)*

So, *in our case, to get rid of the $(-1)^{\text{necessary switches}}$ in the determinant calculation*, it suffices to move the y in the third column to the top (it is an odd number of switches just like to the bottom). We can accomplish this task via a 3-form:

$$dy \wedge dx \wedge dz(e_3, e_1, e_2)$$

since putting the $dy \wedge$ at the front moves the y up:

$$dy \wedge dx \wedge dz \begin{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \\ e_3 \quad e_1 \quad e_2 \end{pmatrix} = \det \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = + \det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1.$$

Thus, the determinant of the 3×3 matrix and the 2×2 matrix are both -1 . Using what we have found, let's actually finish our integral approximation in two different ways! First, let's compute an approximation for our surface integral $\int_S y dx \wedge dz$ —only we are lucky because on each face that matters in our calculation, y is constant. *If our surface is the parallelogram mesh, then our approximation is not approximate. It is exact!*

So we have the face at $y = 1$. On this face, we plug in (e_3, e_1) and get: $\underbrace{(1)}_y \cdot dx \wedge dz(e_3, e_1) = 1 \cdot (-1) = -1$.

Let's now go to the face at $y = 0$. On this face, we plug in (e_1, e_3) since this face *faces* the other way. But $y = 0$ so our rule just yields 0 for this face. Therefore:

$$\int_S y dx \wedge dz = -1$$

Now, let's think of the interior volume of this surface. It is made up of one positive volume parallelepiped given by the vectors (e_3, e_1, e_2) . Notice that to get this, if we want to use $+e_2$, we have to use the face that would give a positive volume: (e_3, e_1) . We found a 3-form $dy \wedge dx \wedge dz$ that had the same behavior as $dx \wedge dz$ on our chosen input vectors. But what about the expression “ y ” that is at the front of $dx \wedge dz$?

Consider the face at $y = 0$. We know that here we plug in (e_1, e_3) and get $dx \wedge dz(e_1, e_3) = +1$ which is the opposite sign as for the other face. If y were replaced by a function $g(x, y, z)$ we could say that we are adding:

$$\begin{aligned} & g|_{y=1} \cdot dx \wedge dz(e_3, e_1) + g|_{y=0} \cdot dx \wedge dz(e_1, e_3) \\ &= g|_{y=1} \cdot dx \wedge dz(e_3, e_1) - g|_{y=0} \cdot dx \wedge dz(e_3, e_1) \\ &= \underbrace{(g|_{y=1} - g|_{y=0})}_{\int_{y=0}^{y=1} g_y dy} \cdot dx \wedge dz(e_3, e_1) \end{aligned}$$

The expression g_y simply means the partial derivative of g with respect to y . We use the fact that the change of a function of y like $g(1) - g(0)$ is equal to $\int_0^1 g'(y) dy$. The integration $\int_{y=0}^{y=1}$ allows us to actually make the move to a 3-form that moves across the interior. It will traverse parallelepipeds or boxes on a straight line parallel to the y -axis from one side of our closed surface to the other. So we let the volume integration “swallow” the $\int_{y=0}^{y=1}$. Therefore we use the 3-form

$$\underbrace{g_y}_1 \underbrace{dy \wedge dx \wedge dz}_{\text{Gives the same result as } dx \wedge dz \text{ as discussed above}}$$

where $g(x, y, z) = y$

Let's integrate this 3-form that we found over this volume V using the one and only one parallelepiped in the interior:

$$\int_V 1 \cdot dy \wedge dx \wedge dz = dy \wedge dx \wedge dz(e_3, e_1, e_2) = -1$$

The two calculations are the same!

This example worked because the number of switches to change $(0, y, 0)$ to $(y, 0, 0)$ had the same parity (oddness or evenness) as the number of switches to change $(0, y, 0)$ to $(0, 0, y)$. It also worked because the top y face at $y = 0$ had a positive area orientation viewed from the outside: *putting a vector off of the base which points outside, away from the object gives a positive volume off of that base*. So, let's examine some ideas and conditions that will allow us to generalize what we just did to other cases:

- If a tuple has an even number of entries like $(0, y, 0, 0)$ or $(0, y)$, then the number of switches to move y to the top has *exactly the opposite parity* as moving it to the bottom. If one is even, the other is odd and vice versa.
- If a tuple has an odd number of entries like $(0, y, 0)$ or $(0, y, 0, 0, 0)$, then the number of switches to move y to the top or the bottom always has the same parity. Both are even or both are odd.

It seems that the $(m - 1) \times (m - 1)$ submatrix determinant we want in even dimensions m will have *exactly the opposite sign* as the determinant of the $m \times m$ matrix after moving y to the top! What do we do? We get another multiplication by -1 if we say that the orientation of the top face (like $y = 1$ in our example) is negatively oriented with $+e_2$ coming off of the base. Then, to put a positive volume “parallelepiped” into the m -form, we would input $\underbrace{(u_1, \dots, u_{m-1})}_{\text{top face for } y}, -e_2$ into $dy \wedge ((m - 1)\text{-form})$. We generalize this idea as follows:

An m -form that evaluates like a $(m - 1)$ -form

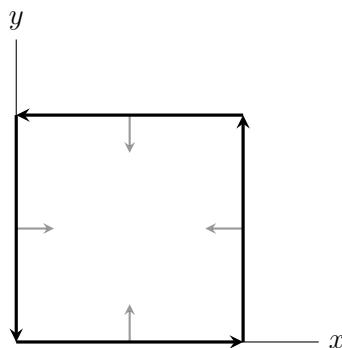
Let w be a variable corresponding to a standard basis vector e_r so that $e_r \perp \langle \underbrace{u_1, \dots, u_{m-1}}_{\text{makes a ‘parallelepiped’}} \rangle$.

If m is odd, we assume that (u_1, \dots, u_{m-1}) is positively oriented (in a volume/area sense) for $+e_r$ coming off the it as a base. We assume that it is negatively oriented (in a volume/area sense) with $+e_r$ coming off the base if m is even. Suppose that σ is a $(m - 1)$ -form with respect to variables corresponding to e_1, \dots, e_{r-1} . Then:

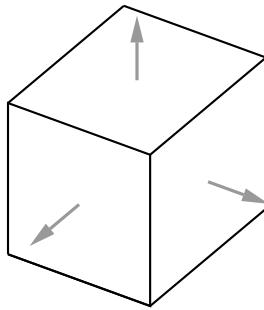
$$\sigma(u_1, \dots, u_{m-1}) = dw \wedge \sigma(u_1, \dots, u_{m-1}, (-1)^{m+1} e_r)$$

Example 12. Suppose that

So we are saying that we want the boundary to be positively oriented when vectors off the base point *inside the object* (like $-e_r$ if this is a “top edge”) when the interior is 2-dimensional. The *bottom* edge of the boundary has to be pointing to the right so that an upward vector (*into* the interior) makes a positive area off of the bottom edge being a base:



That is, positive boundary orientation for a 2-dimensional object is *counterclockwise*. But for a 3-dimensional region, positive orientation on the boundary comes from a vector pointing outside of the object (like $+e_r$ for a “top face”):



That is, to get positive volume off of the boundary face of the depicted cube serving as the base, we need the vector off this base extending outside of the cube.

What we have just done is decide how to orient boundaries so that we can easily find a wedge product expression through the interior that will give the same result as a wedge product expression on the boundary.

Variation from other texts: Sometimes a base on the boundary $(u_1, u_2, \dots, u_{m-1})$ is said to have the orientation so that an outward vector v_{out} away from the interior would make $\det(v_{\text{out}} \ u_1 \ \dots \ u_{m-1})$ be positive. See [3].

So then, one can *always use outward arrows in even and odd dimensions* to depict the orientation of the boundary. Yes, this does give the *same* orientation that we describe here in this section. And yes, one does not have to alternate the arrows between even and odd dimensions. *But intuitively we are no longer thinking about what makes volume or area positive or negative—just a determinant where the column for the vector out of the base is on the wrong side.*

The reason why this would work is that putting $dw \wedge$ to the front creates the exact same number of switches every time as would describe the desired cofactor. So wedging $dw \wedge$ cancels out the sign of the cofactor to just be the determinant of the desired submatrix itself. It is computationally concise—but intuitionally lacking.

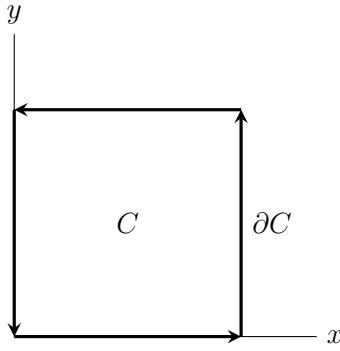
We can generalize our technique in the last example with the following theorem. In the statement of the theorem, some extra things are added beyond what we saw in the last example. Yet the things that are added just vanish through orthogonality ideas—or rather just the idea that things like $dx \wedge dx$ evaluate to 0. So really we have the tools—it is just about communication.

Generalized Stoke's Theorem

This is the technique we use for integrating through the interior instead of on the boundary of a *closed region*. Specifically, if we are integrating in the xy -plane, on the boundary we integrate things like $f dx$ or $f dy$. In both cases, just replace f with $Df \bullet (dx, dy) \wedge$ which is the same thing as $(f_x dx + f_y dy) \wedge$. Then integrate the result on the interior. (*Notice what is extra: we have both $f_x dx$ and $f_y dy$ wedged in front. But one of these goes away in the wedge product!*)

If we are integrating in \mathbb{R}^3 , on the boundary we integrate things like $f dx \wedge dy$ or $f dz \wedge dx$ or $f dy \wedge dz$. In all of these cases, just replace f with $Df \bullet (dx, dy, dz) \wedge$ which is the same thing as $(f_x dx + f_y dy + f_z dz) \wedge$. Then integrate the result on the interior.

Example 13. Suppose that we wish to integrate $(x+y)dx + ydy$ along the outside of the square $C : 0 \leq x \leq 1$ and $0 \leq y \leq 1$. Let ∂C represent the boundary of C :



Assuming that C has a positive area, the boundary of C is a counterclockwise path around C . To start off let's split the integration into two parts:

$$\int_{\partial C} (x+y)dx + ydy = \int_{\partial C} (x+y)dx + \int_{\partial C} ydy$$

Take the first integral and apply the generalized Stoke's theorem above as follows:

$$\begin{aligned} \int_{\partial C} \underbrace{(x+y)}_f dx &= \int_C (f_x dx + f_y dy) \wedge dx = \int_C f_y dy \wedge dx \\ &= \int_C dy \wedge dx \end{aligned}$$

We have a “constant” 2-form $dy \wedge dx$ so any partitioning into rectangles or parallelograms will give the exact integral—not just an approximation. If we take all of C itself thought of as a positive rectangle/parallelogram (e_2 off of a base of e_1), we have:

$$\int_C dy \wedge dx = dy \wedge dx(e_1, e_2) = -dx \wedge dy(e_1, e_2) = -1 \cdot 1 = -1.$$

Now for the second integral:

$$\int_{\partial C} y dy = \int_C (0dx + 1dy) \wedge dy = \int_C 0 = 0$$

Therefore, the final result is simply

$$-1 + 0 = -1.$$

Example 14. Let's compute the integral of the last example the long way and compare.

- The top with $y = 1$ and little pieces: $-\Delta x \cdot e_1$:

$$\begin{aligned} & (x + \underbrace{y}_1) dx (-\Delta x \cdot e_1) + \underbrace{y}_1 \cdot \underbrace{dy}_{0} (-\Delta x \cdot e_1) \\ &= (x + 1)(-\Delta x) \end{aligned}$$

Adding up all these pieces in a limit is like the usual integral:

$$\int_0^1 -(x + 1) dx = -\frac{3}{2}$$

- The bottom with $y = 0$ and little pieces: $+\Delta x \cdot e_1$:

$$\begin{aligned} & (x + \underbrace{y}_0) dx (-\Delta x \cdot e_1) + \underbrace{y}_0 \cdot \underbrace{dy}_{0} (+\Delta x \cdot e_1) \\ &= (x)(\Delta x) \end{aligned}$$

Adding up all these pieces in a limit is like the usual integral:

$$\int_0^1 x dx = +\frac{1}{2}$$

- The right with $x = 1$ and little pieces $+\Delta y \cdot e_2$:

$$\begin{aligned} & (\underbrace{x}_1 + y) dx \underbrace{(+\Delta y \cdot e_2)}_0 + y \cdot dy (+\Delta y \cdot e_2) \\ &= (y)(\Delta y) \end{aligned}$$

Adding up all these pieces in a limit is like the usual integral:

$$\int_0^1 y dy = +\frac{1}{2}$$

- The left with $x = 0$ and little pieces $-\Delta y \cdot e_2$:

$$\begin{aligned}
 & (\underbrace{x}_0 + y) dx \underbrace{(-\Delta y \cdot e_2)}_0 + y \cdot dy (-\Delta y \cdot e_2) \\
 & = -(y)(\Delta y)
 \end{aligned}$$

Adding up all these pieces in a limit is like the usual integral:

$$\int_0^1 -y \, dy = -\frac{1}{2}$$

Adding up these boundary integrations we get: $-\frac{3}{2} + \frac{1}{2} + \frac{1}{2} - \frac{1}{2} = -1$.

Can you see how going to the interior simplified the calculation?

Extra Note: The orientations on the boundaries are specifically chosen so that the process of changing from a $(m-1)$ -form to a m -form has the same integral outcome. Think about “cells” in a cellular complex like in section 4.5.

A m -form is like a function whose input is a m -cell and output is $\int_{m\text{-cell}} m\text{-form} \in \mathbb{R}$.

The process $m\text{-cell} \mapsto$ its boundary $B \mapsto \int_B \sigma$ where σ is a $(m-1)$ -form is the same process (i.e. function) as $m\text{-cell} \mapsto \int_{m\text{-cell}} d\sigma$ where we use “ $d\sigma$ ” to denote the m -form we get from our $m-1$ form as we apply Stoke’s theorem.

Lesson learned: boundary orientations are chosen simply to make the fascinating connection of Stoke’s theorem actually work! You may notice that our technique of taking boundaries in a cell complex actually follows these choices (i.e. go counterclockwise)!

Further Ideas: The ideas we have developed can be used to describe the “dual vector spaces” of the vector space versions of “homology groups” mentioned in section 4.5. The “dual” version of the boundary maps (going in the opposite direction since row interpretation—dual interpretation—reverses the direction of maps) actually corresponds to changing our $(m - 1)$ -forms into m -forms. Studying these maps with quotient vector spaces of kernels and ranges is called “cohomology” where we use “co” because it is “dual.” Stoke’s theorem makes this connection. This allows one to use calculus to study and classify surfaces. Just a little multilinear algebra and we have the connection!

Key Concepts from this Section

- **cross product:** (page 695) Given two column vectors u and w in \mathbb{R}^3 , create a 3×3 matrix A with any other column vector q so that $A = \begin{pmatrix} u & v & q \end{pmatrix}$. Then, we define the cross product between u and v as:

$$u \times v = c_q$$

where c_q is the vector of signed cofactors for the column q . It is the same no matter what the entries in q are.

- **theorem 6.5.1 :** (page 696) The cross product is orthogonal to each of the vectors involved.

$$(u \times v) \perp u \quad (u \times v) \perp v$$

- **theorem 6.5.2 anticommutativity of the cross product:** (page 697)

$$u \times v = -v \times u.$$

- **cross product by wedge product:** (page 697) We can equivalently express the cross product in terms of the wedge product \wedge :

$$u \times v = (dy \wedge dz(u, v), dz \wedge dx(u, v), dx \wedge dy(u, v))$$

- **theorem 6.5.3 :** (page 698) The cross product is a bilinear transformation.

- **theorem 6.5.4 bilinear properties of the cross product:** (page 698)

- $u \times (v + w) = u \times v + u \times w$
- $u \times (kv) = k \cdot (u \times v)$

- **theorem 6.5.5 zero cross product:** (page 698) Let $u \in \mathbb{R}^3$. Then:

$$u \times u = (0, 0, 0)$$

- **theorem 6.5.6 :** (page 698) The volume of a parallelepiped in \mathbb{R}^3 with vector w coming off of a base formed by vectors u and v is given by the absolute value of $(u \times v) \bullet w$.

- **area of a parallelogram:** (page 700) The area of a parallelogram formed by two vectors $u, v \in \mathbb{R}^3$ is given by:

$$\sqrt{(dy \wedge dz(u, v))^2 + (dx \wedge dz(u, v))^2 + (dx \wedge dy(u, v))^2}$$

where since we are squaring, we do not worry about the order of wedging.

- **area of a parallelogram in \mathbb{R}^4 :** (page 700) The area of a parallelogram formed by two vectors $u, v \in \mathbb{R}^4$ where coordinates are given by (x, y, z, w) is given by:

$$\sqrt{(dy \wedge dz(u, v))^2 + (dx \wedge dz(u, v))^2 + (dx \wedge dy(u, v))^2 + (dx \wedge dw(u, v))^2 + (dy \wedge dw(u, v))^2 + (dz \wedge dw(u, v))^2}$$

- **n -form:** (page 703) We call a wedge product expression like $x^2 dx + xy dy$ a 1-form, an expression like $z^3 dx \wedge dz - y dy \wedge dz$ a 2-form, an expression like $(6z + x) dy \wedge dz \wedge dx$ a 3-form and so forth.

- **integral of a $n - form$ over a n -dimensional region:** (page 704) Create a mesh of n -dimensional parallelograms (parallelepipeds) over your region. The n -form gives a rule for how to get a number from each piece of the mesh. If the sums of these numbers get closer and closer to a number as we make the mesh finer and finer, we call that number the integral of the n -form over the region.

- **integral of a constant n -form:** (page 704) We say that a n -form is constant if it looks something like $1 \cdot dx \wedge dy$ (this is an example of a 2-form) where the expression in front “1” is just a constant. Any parallelogram mesh approximation to an integral *in this case* is *exact!* We are actually finding the integral itself when we use the approximation technique.

- **finding approximate surface area:** (page 708) To find surface area, start with the 2-form:

$$\sqrt{(dy \wedge dz(u, v))^2 + (dx \wedge dz(u, v))^2 + (dx \wedge dy(u, v))^2}$$

Use derivatives to relate dz to dx and dy and simplify to a 2-form that looks like:

$$(expression) \cdot dx \wedge dy(u, v)$$

Then, divide the shadow of the surface on the xy -plane into rectangles (or parallelograms) and plug these into the 2-form. Lastly, add up the results.

- **how to change coordinates in an n -form:** (page 709) Just rewrite the d variable's in terms of the others by using derivatives. Then use the wedge product between these.
- **jacobian matrix:** (page 711) The Jacobian matrix of a change of coordinates function is simply the first derivative matrix of that change of coordinates function.
- **theorem 6.5.7 :** (page 711) To change coordinates of an n -form from $da_1 \wedge da_2 \wedge \cdots \wedge da_n$ to $db_1 \wedge db_2 \wedge \cdots \wedge db_n$, take the change of coordinates function g from the *new coordinates* (b_1, \dots, b_n) to the *old coordinates* (a_1, \dots, a_n) . Let J be the Jacobian (first derivative matrix) of g . Then:

$$da_1 \wedge da_2 \wedge \cdots \wedge da_n = \det(J) \cdot db_1 \wedge db_2 \wedge \cdots \wedge db_n$$

- **an m -form that evaluates like a $(m - 1)$ -form:** (page 717) Let w be a variable corresponding to a standard basis vector e_r so that $e_r \perp \langle \underbrace{u_1, \dots, u_{m-1}}_{\text{makes a "parallelepiped"}}, \rangle$. If m is odd, we assume that (u_1, \dots, u_{m-1}) is positively oriented (in a volume/area sense) for $+e_r$ coming off the it as a base. We assume that it is negatively oriented (in a volume/area sense) with $+e_r$ coming off the base if m is even. Suppose that σ is a $(m - 1)$ -form with respect to variables corresponding to e_1, \dots, e_{r-1} . Then:

$$\sigma(u_1, \dots, u_{m-1}) = dw \wedge \sigma(u_1, \dots, u_{m-1}, (-1)^{m+1} e_r)$$

- **generalized stoke's theorem:** (page 718) This is the technique we use for integrating through the interior instead of on the boundary of a *closed region*. Specifically, if we are integrating in the xy -plane, on the boundary we integrate things like $f dx$ or $f dy$. In both cases, just replace f with $Df \bullet (dx, dy) \wedge$ which is the same thing as $(f_x dx + f_y dy) \wedge$. Then integrate the result on the interior. (*Notice what is extra: we have both $f_x dx$ and $f_y dy$ wedged in front. But one of these goes away in the wedge product!*)

If we are integrating in \mathbb{R}^3 , on the boundary we integrate things like $f dx \wedge dy$ or $f dz \wedge dx$ or $f dy \wedge dz$. In all of these cases, just replace f with $Df \bullet (dx, dy, dz) \wedge$ which is the same thing as $(f_x dx + f_y dy + f_z dz) \wedge$. Then integrate the result on the interior.

6.5.8 Exercises

Cross Products

Compute the following cross products:

1. $(-2, 0, 0) \times (-1, 2, 0)$

2. $(1, 1, -1) \times (1, 2, 2)$

3. $(2, 2, 0) \times (2, 0, 0)$

4. $(-1, -2, 0) \times (-1, 2, 2)$

5. $(-1, 2, -2) \times (-2, -1, -2)$

6. $(0, -2, 1) \times (-1, 0, -1)$

7. $(-1, 2, 2) \times (1, 0, 1)$

8. $(0, -2, -2) \times (-2, 0, -2)$

9. $(0, -1, 0) \times (-1, 0, -1)$

10. $(-2, 1, 1) \times (0, -1, 2)$

Oriented Area

For each of the following, find the *oriented* area of the parallelogram formed by using the indicated base vector and vector off of the base.

11. Base: $(0, -2)$

12. Base: $(1, -1)$

Off Base: $(-1, 0)$

Off Base: $(2, 1)$

13. Base: $(0, 2)$

14. Base: $(-2, 0)$

Off Base: $(-1, -1)$

Off Base: $(2, 2)$

15. Base: $(-1, 2)$

16. Base: $(-1, 0)$

Off Base: $(1, -1)$

Off Base: $(2, 2)$

17. Base: $(-2, 2)$

Off Base: $(1, 1)$

18. Base: $(-1, 2)$

Off Base: $(1, -2)$

19. Base: $(0, 1)$

Off Base: $(-2, -1)$

20. Base: $(0, 1)$

Off Base: $(-1, -2)$

Oriented Volume

For each of the following, find the *oriented* volume of the parallelepiped formed.

21. Base: $\underbrace{(0, 0, 2)}_{\text{parallelogram base}}, (1, -2, -2)$

Off Base: $(1, 2, -2)$

22. Base: $\underbrace{(-2, 0, -1)}_{\text{parallelogram base}}, (0, 2, 1)$

Off Base: $(-2, 2, 1)$

23. Base: $\underbrace{(-1, 0, 1)}_{\text{parallelogram base}}, (0, 1, -1)$

Off Base: $(0, 2, 2)$

24. Base: $\underbrace{(0, -1, -1)}_{\text{parallelogram base}}, (1, -2, 2)$

Off Base: $(-1, 1, 1)$

25. Base: $\underbrace{(1, 0, 0)}_{\text{parallelogram base}}, (2, -2, -1)$

Off Base: $(0, -1, 0)$

26. Base: $\underbrace{(-2, -1, -2)}_{\text{parallelogram base}}, (-2, 0, 0)$

Off Base: $(2, 1, -1)$

27. Base: $\underbrace{(1, 0, 0)}_{\text{parallelogram base}}, (-1, 0, 1)$

Off Base: $(-2, 0, 0)$

28. Base: $\underbrace{(2, 1, 1)}_{\text{parallelogram base}}, (1, -2, -2)$

Off Base: $(0, -2, -2)$

29. Base: $\underbrace{(0, -2, 0)}_{\text{parallelogram base}}, (-1, -2, -2)$

Off Base: $(-2, -2, -1)$

30. Base: $\underbrace{(0, 2, 2)}_{\text{parallelogram base}}, (-2, -1, 0)$

Off Base: $(-1, 0, 0)$

Surface Area from 2-forms

Find a 2-form that can be used to find or approximate surface area for the following surfaces.

31. $z = x^3y + 2xy$

32. $z = -5y^4 + 2xy$

33. $z = -7y^4 + 4xy$

34. $z = x^3y + 4xy$

35. $z = 2x - 3y$

36. $z = x + y$

37. $z = -8y^4 + 4xy$

38. $z = x + 2y$

39. $z = x^3y + xy$

40. $z = 3x + y$

Changing Coordinates

Find the expression $f(t, w)$ such that $dx \wedge dy = f(t, w) \cdot dt \wedge dw$.

41. $x = t^3$

42. $x = t^3$

$y = w$

$y = w + 1$

43. $x = t^3 - tw$

44. $x = t + 1$

$y = t + w$

$y = w + \sin(t)$

45. $x = t^3 - tw$

46. $x = t - w$

$y = t + w$

$y = t + w$

47. $x = t^3$

48. $x = t^3 - tw$

$y = w + 1$

$y = t + w$

49. $x = t^3 + 1$

$$y = w^3 + \sin(t)$$

50. $x = t^3$

$$y = w^3$$

Stoke's Theorem

Change the given 2-form into an 3-form that allows one to integrate on an interior instead of a boundary surface.

51. $4xydx \wedge dy + 4zdx \wedge dz + 4ydy \wedge dz$

53. $(-2x + z)dx \wedge dy + (4x^3z + 4xy)dx \wedge dz + (2x + 4y)dy \wedge dz$

55. $2ydx \wedge dy + (3y + 2z)dx \wedge dz + (3x^3z + 2xy)dy \wedge dz$

57. $(2y + z)dx \wedge dy + xyzdx \wedge dz + (-x + z)dy \wedge dz$

52. $(x^3z + xy)dx \wedge dy + ydx \wedge dz + (y + z)dy \wedge dz$

54. $xyzdx \wedge dy + (2x^3z + 4xy)dx \wedge dz + (x + 4y)dy \wedge dz$

56. $(y + 4z)dx \wedge dy + (3x + 4y)dx \wedge dz + (4x^3z + 4xy)dy \wedge dz$

58. $2ydx \wedge dy + zdx \wedge dz + xyzdy \wedge dz$

Change the given 1-form into an 2-form that allows one to integrate through an interior instead of on a boundary path.

59. $(4y^2 + x)dx + (4xy + x)dy$

61. $3x^2dx + 3xydy$

60. $2xydx + 2xdy$

62. $xdx + xydy$

63. $3ydx + (3xy + x)dy$

64. $2y^2dy$

65. $(4y^2 + 2x)dx + 2xydy$

66. $2x^2dx + (3y^2 + 2x)dy$

67. $2ydx + xdy$

68. $(4y^2 + x)dx + (x + 3y)dy$

Proof Practice

69. Prove that given a vector $u \in \mathbb{R}^3$ that $u \times u = (0, 0, 0)$.

70. Use properties of the cross product to prove that for vectors $a, b \in \mathbb{R}^3$,

$$a \times (a + b) + b \times (a + b) = (0, 0, 0)$$

71. Use properties of the cross product to prove that for vectors $a, b \in \mathbb{R}^3$,

$$(a \times (a - b) + b \times (a)) \bullet (a + b) = 0$$

72. Prove that the volume of a parallelepiped in \mathbb{R}^3 with vector w coming off of a base formed by vectors u and v is given by the absolute value of $(u \times v) \bullet w$.

73. Prove that a sum of bilinear transformations with the same input is again a bilinear transformation.

74. Application of wedge product to complex calculus: One of the exercises of the last section introduced the idea of Cauchy Riemann Equations. Prove that if a function $f(x, y) = (u(x, y), v(x, y))$ satisfies these equations: $u_x = v_y$, $u_y = -v_x$, then when $(u + v \cdot i) \cdot (dx + i \cdot dy)$ is integrated around a simple closed loop enclosing a region where the function $f(x, y)$ and its derivatives are defined and continuous, that result will be 0. Use the *Generalized Stoke's Theorem*.

Commentary on the last exercise: This shows that if a function of a complex variable $f(z)$ admits a power series representation over a region of the complex plane in which a closed loop C lies, then the integral $\int_C f(z) dz$ comes out to 0. This idea can be used to change paths of integration away from real numbers into the complex plane—and this can actually simplify computations!

If we integrate along any path beginning from a point $z_0 \in \mathbb{C}$ and ending at $z \in \mathbb{C}$ in the complex plane in a region where $f(z)$ is continuous and has continuous complex derivatives, then this last exercise leads to the fact that *which path we take does not matter*. Any variation in path can be found by “adding a loop to the path.” Thus, we have a function F given by $z \mapsto \int_{z_0}^z f(c) dc$ where we use $c \in \mathbb{C}$ since z represents a bound of integration. The first derivative of this function will be $f(z)$ itself. The antiderivative F actually coincides with the power series antiderivative. So, if we restrict ourselves to a good domain, *all path integrals* from $z = a$ to $z = b$ can be computed by $F(b) - F(a)$ where the complex antiderivative $F(z)$ can be found in the same way we find antiderivatives of functions of a real variable.

6.5.9 Solutions

1. $(0, 0, -4)$

2. $(4, -3, 1)$

3. $(0, 0, -4)$

4. $(-4, 2, -4)$

5. $(-6, 2, 5)$

6. $(2, -1, -2)$

7. $(2, 3, -2)$

8. $(4, 4, -4)$

9. $(1, 0, -1)$

10. $(3, 4, 2)$

11. -2

12. 3

13. 2

14. -4

15. -1

16. -2

17. -4

18. 0

19. 2

20. 1

21. 8

22. -4

23. -4

24. 4

25. -1

26. 6

27. 0**28.** 0**29.** -6**30.** -2

31. $\sqrt{(3x^2y + 2y)^2 + (x^3 + 2x)^2 + 1} dx \wedge dy$

32. $\sqrt{(2y)^2 + (-20y^3 + 2x)^2 + 1} dx \wedge dy$

33. $\sqrt{(4y)^2 + (-28y^3 + 4x)^2 + 1} dx \wedge dy$

34. $\sqrt{(3x^2y + 4y)^2 + (x^3 + 4x)^2 + 1} dx \wedge dy$

35. $\sqrt{(2)^2 + (-3)^2 + 1} dx \wedge dy$

36. $\sqrt{(1)^2 + (1)^2 + 1} dx \wedge dy$

37. $\sqrt{(4y)^2 + (-32y^3 + 4x)^2 + 1} dx \wedge dy$

38. $\sqrt{(1)^2 + (2)^2 + 1} dx \wedge dy$

39. $\sqrt{(3x^2y + y)^2 + (x^3 + x)^2 + 1} dx \wedge dy$

40. $\sqrt{(3)^2 + (1)^2 + 1} dx \wedge dy$

41. $3t^2 \cdot dt \wedge dw$

42. $3t^2 \cdot dt \wedge dw$

43. $3t^2 + t - w \cdot dt \wedge dw$

44. $1 \cdot dt \wedge dw$

45. $3t^2 + t - w \cdot dt \wedge dw$

46. $2 \cdot dt \wedge dw$

47. $3t^2 \cdot dt \wedge dw$

48. $3t^2 + t - w \cdot dt \wedge dw$

49. $9t^2w^2 \cdot dt \wedge dw$

50. $9t^2w^2 \cdot dt \wedge dw$

51. 0

52. $(x^3 - 1) dx \wedge dy \wedge dz$

53. $(-4x + 3) dx \wedge dy \wedge dz$

54. $(xy - 4x + 1) dx \wedge dy \wedge dz$

55. $(9x^2z + 2y - 3) dx \wedge dy \wedge dz$

56. $(12x^2z + 4y) dx \wedge dy \wedge dz$

57. $-x z dx \wedge dy \wedge dz$

58. $y z dx \wedge dy \wedge dz$

59. $(-4y + 1) dx \wedge dy$

60. $(-2x + 2) dx \wedge dy$

61. $3y dx \wedge dy$

62. $y dx \wedge dy$

63. $(3y - 2) dx \wedge dy$

64. 0

65. $-6y dx \wedge dy$

66. $2dx \wedge dy$

67. $-dx \wedge dy$

68. $(-8y + 1) dx \wedge dy$

69. Just think of the cofactor function for the first column of a matrix where the other two columns are the same. The output of such a function is always 0 (a zero determinant). Hence, $e_1 \mapsto 0$, $e_2 \mapsto 0$ and $e_3 \mapsto 0$. Hence, the cofactor function matrix is $\begin{pmatrix} 0 & 0 & 0 \end{pmatrix}$ which tells us that the cross product is $(0, 0, 0)$.

70. One could simply distribute the \times to see:

$$\underbrace{a \times a}_{=0} + a \times b + \underbrace{b \times a}_{=-a \times b} + \underbrace{b \times b}_{=0}$$

Or, one could *undistribute* the $(a + b)$ on the right to have:

$$(a + b) \times (a + b) = (0, 0, 0).$$

71. This expression becomes:

$$\begin{aligned} & \underbrace{(a \times a - a \times b + b \times a)}_{=0} \bullet (a + b) \\ &= (-2a \times b) \bullet (a + b) \end{aligned}$$

Notice that $(a + b) \in (a \times b)^\perp$. Therefore, this dot product evaluates to 0.

72. All this dot product is doing is plugging in the vector w as a column into the cofactor function row matrix. That is, it just computes the determinant of a matrix with columns $\begin{pmatrix} u & v & w \end{pmatrix}$ which gives precisely what we want.

73. We just need to prove that the sum is linear in each component. That is, let f and g be two bilinear transformations. Then,

$$(f + g)(u, v) = f(u, v) + g(u, v)$$

To check if it is linear in the second component, we could compute:

$$\begin{aligned} (f + g)(u, v + k \cdot w) &= f(u, v + k \cdot w) + g(u, v + k \cdot w) \\ &= f(u, v) + k \cdot f(u, w) + g(u, v) + k \cdot g(u, w) = (f(u, v) + g(u, v)) + k \cdot (f(u, w) + g(u, w)) \\ &= (f + g)(u, v) + k \cdot (f + g)(u, w) \end{aligned}$$

Checking the first component is similar.

74. We change the integral along the loop to an integral over the interior region (area) inside of the loop. First, we multiply:

$$(u + v \cdot i) \cdot (dx + i \cdot dy) = udx + (udy) \cdot i + (vdx) \cdot i - vdy = (udx - vdy) + (udy + vdx) \cdot i$$

Now, we change this to something we can integrate over a region using the Generalized Stoke's Theorem keeping the real and the complex parts distinct:

$$((u_x dx + u_y dy) \wedge dx - (v_x dx + v_y dy) \wedge dy) + ((u_x dx + u_y dy) \wedge dy + (v_x dx + v_y dy) \wedge dx) \cdot i$$

When you switch $dy \wedge dx$ to $-dx \wedge dy$ remember the negative. And remember that $dx \wedge dx = dy \wedge dy = 0$

$$(-u_y dx \wedge dy - v_x dx \wedge dy) + (u_x dx \wedge dy - v_y dx \wedge dy) \cdot i$$

Now replacing u_y with $-v_x$ and u_x with v_y from the Cauchy Riemann equations, we have:

$$(v_x dx \wedge dy - v_x dx \wedge dy) + (v_y dx \wedge dy - v_y dx \wedge dy) \cdot i = 0$$

In other words, when we integrate 0 over the interior, we get the same result as integrating on the closed loop. The result is just 0.

Chapter 6 Selected Review Questions

Section 6.1

Can you write permutations in disjoint cycle notation?

1. $(1\ 3)(4\ 5)(1\ 4\ 3\ 5\ 2)(2\ 4\ 3\ 5)$ 2. $(1\ 5\ 3)(2\ 4)(1\ 2)(3\ 5\ 4)(1\ 2)(3\ 4\ 5)$

Can you determine if permutations are even or odd?

3. $(1\ 5\ 3\ 4\ 2)(1\ 5)(3\ 4)(1\ 4\ 3)(2\ 5)$ 4. $(1\ 5\ 4\ 2\ 3)(3\ 5)(1\ 5\ 4\ 2\ 3)$

5. $(1\ 3\ 4)(2\ 5)(1\ 5\ 3\ 2)(3\ 4)$ 6. $(1\ 2\ 4\ 5)(2\ 3\ 5\ 4)(1\ 2\ 4\ 3\ 5)$

Section 6.2

Can you compute determinants by using a strategic use of sliding and cofactors?

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

8.
$$\begin{pmatrix} 0 & -2 & -1 \\ -1 & -2 & -2 \\ 1 & 1 & 0 \end{pmatrix}$$

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

10.
$$\begin{pmatrix} 2 & -1 & 1 & -1 \\ -1 & -1 & 2 & -1 \\ -2 & -1 & 0 & 1 \\ 1 & 0 & 0 & 2 \end{pmatrix}$$

Can you use six pairs of determinants of 2×2 submatrices to find the determinant of a 4×4 matrix?

11. $\begin{pmatrix} 2 & -2 & 1 & 2 \\ 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 \end{pmatrix}$

12. $\begin{pmatrix} -1 & 1 & 2 & -1 \\ 2 & 0 & -1 & 0 \\ 0 & 0 & -2 & 0 \\ -1 & 2 & 0 & 0 \end{pmatrix}$

Can you identify determinants of elementary matrices and consider how determinants work across products and inverses? Show how you use these ideas to find the determinant.

13. $\begin{pmatrix} -1 & -2 & -1 \\ 0 & 2 & -2 \\ 2 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1}$

14. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} \begin{pmatrix} 2 & -2 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ -2 & -1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} -1 & 1 & -1 \\ -1 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}^{-1}$

Section 6.3

Can you find specific cofactors for a given matrix?

15. Find C_{11} for $\begin{pmatrix} 1 & 2 & 0 & -1 \\ 2 & -1 & -2 & -2 \\ 2 & -1 & -1 & 0 \\ -1 & 0 & 1 & -1 \end{pmatrix}$

16. Find C_{32} for $\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & -1 & -2 & 2 \\ -1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}$

Can you find inverses of matrices using the cofactor method?

17. $\begin{pmatrix} -2 & 0 & -2 \\ -1 & 0 & 0 \\ 2 & 1 & -1 \end{pmatrix}$

18. $\begin{pmatrix} 1 & -2 & -1 \\ -1 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix}$

Can you use Cramer's rule to find a specific variable value in the solution?

19. Find the value of x :

$$\begin{array}{rcl} x + 2y + z & = & 0 \\ 2x + y + 2z & = & 0 \\ -2x - y + 2z & = & -4 \end{array}$$

20. Find the value of y :

$$\begin{array}{rcl} x - y + 2z & = & -5 \\ -x - 2y & = & 0 \\ -2x + 2y - z & = & 7 \end{array}$$

Section 6.4

Can you use the four defining properties of a determinant in the text to calculate the determinant of a matrix?

21.
$$\begin{pmatrix} -2 & 0 & 0 & 0 \\ -2 & 0 & -2 & 1 \\ 0 & 0 & 0 & -1 \\ 1 & 1 & 2 & 2 \end{pmatrix}$$

22.
$$\begin{pmatrix} -2 & 0 & 1 & -2 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Can you evaluate trilinear transformations?

- (a) Find the domain and the codomain of the trilinear transformation T .
- (b) Evaluate $T(v_1, v_2, v_3)$.

23.
$$\underbrace{\begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} -1 & -2 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}}_{\text{level 2}}$$

$\underbrace{(0, 2, 2)}_{v_1}, \underbrace{(-1, 0)}_{v_2}, \underbrace{(2, -2)}_{v_3}$

24.
$$\underbrace{\begin{pmatrix} 0 & -2 \\ 2 & -2 \\ -1 & 1 \end{pmatrix}}_{\text{level 1}}, \underbrace{\begin{pmatrix} -2 & 1 \\ 0 & -2 \\ 0 & 0 \end{pmatrix}}_{\text{level 2}}$$

$\underbrace{(-2, -2, 1)}_{v_1}, \underbrace{(2, -2)}_{v_2}, \underbrace{(-1, -2)}_{v_3}$

Can you use either *tensors* or the *fast bilinear evaluation technique* to perform the matrix multiplications?

25.
$$\begin{pmatrix} 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 2 & -2 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \end{pmatrix}$$

26.
$$\begin{pmatrix} 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 2 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$$

Can you represent multivariable polynomials with multilinear transformations? For each of the following multivariable polynomials $f(x, y)$:

- (a) find a linear transformation L expressed as a row matrix,
- (b) a bilinear transformation B expressed as a 2×2 matrix,
- (c) and a trilinear transformation T expressed as matrix levels....

...such that:

$$f(x, y) = f(0, 0) + \underbrace{T(v)}_{\text{linear part}} + \underbrace{B(v, v)}_{\text{bilinear part}} + \underbrace{T(v, v, v)}_{\text{trilinear part}} \quad \text{and} \quad v = (x, y)$$

27. $f(x, y) = -x^2y + 2y^3 - x^2 - 2y + 2$

28. $f(x, y) = x^2y - 2xy^2 + y^3 - 2y$

Can you evaluate a wedge product at vector inputs?

29. $dy \wedge dz((-1, -1, -2), (-1, 0, -2))$

30. $dx \wedge dy((0, 2, -1), (-2, 0, -1))$

Section 6.5

Can you find the *oriented* area of a parallelogram formed by using a base vector and vector off of the base?

31. Base: $(0, -2)$

32. Base: $(1, -1)$

Off Base: $(-1, 0)$

Off Base: $(2, 1)$

Can you find the *oriented* volume of a parallelepiped?

33. Base: $\underbrace{(0, 0, 2)}_{\text{parallelogram base}}, (1, -2, -2)$

Off Base: $(1, 2, -2)$

34. Base: $\underbrace{(-2, 0, -1)}_{\text{parallelogram base}}, (0, 2, 1)$

Off Base: $(-2, 2, 1)$

Solutions/Hints

1. $(1 \ 5 \ 3 \ 2)$

2. $(1 \ 5 \ 3)(2 \ 4)$

3. odd

4. odd

5. odd

6. even

7. -2

8. 3

9. -9

10. 16

11. -2

12. 8

13. -10

14. 4

15. 3

16. 4

17. $\frac{1}{2} \begin{pmatrix} 0 & -2 & 0 \\ -1 & 6 & 2 \\ -1 & 2 & 0 \end{pmatrix}$

18. $-\frac{1}{2} \begin{pmatrix} -4 & -2 & -4 \\ 0 & 0 & -1 \\ -2 & -2 & -2 \end{pmatrix}$

19. $x = -\frac{1}{12} \det \begin{pmatrix} 0 & 2 & 1 \\ 0 & 1 & 2 \\ -4 & -1 & 2 \end{pmatrix} = 1$

20. $y = -\frac{1}{9} \det \begin{pmatrix} 1 & -5 & 2 \\ -1 & 0 & 0 \\ -2 & 7 & -1 \end{pmatrix} = 1$

21. -4

22. 2

23. Solutions by part:

(a) $T : \mathbb{R}^3 \times \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) -4

24. Solutions by part:

(a) $T : \mathbb{R}^3 \times \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

(b) 20

25. -8 **26.** -2 **27.** Solutions by part:

(a) $(0, -2)$

(b) $\frac{1}{2} \begin{pmatrix} -2 & 0 \\ 0 & 0 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \begin{pmatrix} 0 & -2 \\ -2 & 0 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \begin{pmatrix} -2 & 0 \\ 0 & 12 \end{pmatrix}}_{\text{level 2}}$

28. Solutions by part:

(a) $(0, -2)$

(b) $\frac{1}{2} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(c) $\underbrace{\frac{1}{6} \begin{pmatrix} 0 & 2 \\ 2 & -4 \end{pmatrix}}_{\text{level 1}}, \underbrace{\frac{1}{6} \begin{pmatrix} 2 & -4 \\ -4 & 6 \end{pmatrix}}_{\text{level 2}}$

29. 2 **30.** 4 **31.** -2 **32.** 3 **33.** 8 **34.** -4

Matrices as Scalars

7

Matrix Scalars and Zero Scalars

7.1

7.1.1 A Scalar as a Matrix	743
7.1.2 Representations of the Zero Matrix	745
7.1.3 Polynomial Scalars That Act Like Zero	747
7.1.4 Generalized Synthetic Division	750
7.1.5 Counting Paths	755
7.1.6 Recursive Sequences	757
7.1.7 Exercises	763
7.1.8 Solutions	770

Questions to Guide Your Study:

- *What is a scalar matrix and what kind of function of column vectors does it describe?*
- *How can any square matrix be described by a scalar matrix? How do you multiply with matrices and vectors with matrix scalar “ x ” entries?*
- *How do you find a polynomial in terms of a matrix action “ x ” that behaves like zero?*
- *How can you use such a polynomial to simplify raising a matrix to a high power?*
- *How does generalized synthetic division help?*
- *How does this process help us think about recursive sequences?*
- *What is a systems of equation technique with a zero scalar polynomial that also helps with finding high powers of a matrix?*

7.1.1 A Scalar as a Matrix

When a scalar like 4 acts on a vector $(2, 1)$ it multiplies to each vector entry:

$$4 \cdot (2, 1) = (4 \cdot 2, 4 \cdot 1) = (8, 4).$$

This *action* itself can be thought in terms of a *matrix function*:

$$\underbrace{\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}}_{4} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 8 \\ 4 \end{pmatrix}$$

Scalar Matrix

A square $n \times n$ matrix like

$$k \cdot \text{id}_{\mathbb{R}^n} = \begin{pmatrix} k & 0 & \cdots & 0 \\ 0 & k & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & k \end{pmatrix}$$

is called a *scalar matrix*. It behaves like a scalar k as a function on vectors. This is true in both a row and a column interpretation. The effect is to send a vector v to kv .

A lot can actually be learned about a matrix if we simply *pretend that it is a scalar matrix*. For instance, let's take the matrix

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

Suppose that x itself as a symbol is a scalar so that

$$x \cdot (1, -1, 2) = (x, -x, 2x)$$

That is, x is *behaving* like the scalar matrix

$$x \cdot \text{id}_{\mathbb{R}^3} = \begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix}$$

Yet, we would like this scalar matrix action to be consistent with the other matrix action of x .

$$x \cdot (1, -1, 2) = \underbrace{\begin{pmatrix} 0 & 0 & -1 \\ 1 & -1 & -1 \\ 1 & 0 & -2 \end{pmatrix}}_x \cdot \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \\ -3 \end{pmatrix}$$

This tells us that the vector $(x, -x, 2x)$ is the same as $(-2, 0, 3)$:

$$(x, -x, 2x) = (-2, 0, 3)$$

That is, x is a *funny* scalar. A vector which has an entry with it can be rewritten as a vector that has no x at all! Let's look at this another way—rewrite $(x, -x, 2x)$ as:

$$x \cdot (1, 0, 0) - x \cdot (0, 1, 0) + 2x \cdot (0, 0, 1)$$

Notice that $x \cdot (1, 0, 0)$ is just the first column of the matrix x , $-x \cdot (0, 1, 0)$ is just the negative of the second column of the matrix x , and that $2x \cdot (0, 0, 1)$ is just double the third column of the matrix x . So, we have:

$$x \cdot (1, 0, 0) = (0, 1, 1) \quad -x \cdot (0, 1, 0) = (0, 1, 0) \quad 2x \cdot (0, 0, 1) = (-2, -2, -4)$$

Adding these together, we get $(-2, 0, -3)$.



Example 1. Letting x represent the same matrix as above, let's determine what vector $(x^2 + 1, x - 2, 2x^2 + 2)$ represents. We break this up as:

$$\underbrace{x^2 \cdot (1, 0, 0) + (1, 0, 0)}_{(x^2+1,0,0)} + \underbrace{x \cdot (0, 1, 0) - 2 \cdot (0, 1, 0)}_{(0,x-2,0)} + \underbrace{2x^2 \cdot (0, 0, 1) + 2 \cdot (0, 0, 1)}_{(0,0,2x^2+2)}$$

Notice that $x^2 \cdot (1, 0, 0)$ is just the first column of the matrix x^2 which we can compute by plugging in the first column of the matrix x into x according to a column interpretation. That is,

$$x^2 \cdot (1, 0, 0) = x \cdot (0, 1, 1) = (-1, -2, -2).$$

Likewise,

$$x^2 \cdot (0, 0, 1) = x \cdot (-1, -1, -2) = (2, 2, 3).$$

Putting the pieces together:

$$\underbrace{(-1, -2, -2) + (1, 0, 0)}_{(x^2+1, 0, 0)} + \underbrace{(0, -1, 0) - 2 \cdot (0, 1, 0)}_{(0, x-2, 0)} + \underbrace{2 \cdot (2, 2, 3) + 2 \cdot (0, 0, 1)}_{(0, 0, 2x^2+2)} \\ (0, -2, -2) + (0, -3, 0) + (4, 4, 8) = (4, -1, 6).$$

Therefore,

$$(x^2 + 1, x - 2, 2x^2 + 2) = (4, -1, 6).$$

A 3-tuple of polynomials like $(2x + x^4, x^3 - x + 1, 7 + x) \in \mathbb{R}[x]^3$ is equivalent to a 3-tuple of real numbers in \mathbb{R}^3 under the assumption that the scalar matrix

$$x \cdot \text{id}_{\mathbb{R}^3} = \begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix}$$

behaves the same as

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

Theorem 7.1.1

Let A be a square $n \times n$ matrix and let x represent the action of A as a scalar. The assumption that the scalar x behaves like A turns $\mathbb{R}[x]^n$ into \mathbb{R}^n .

7.1.2 Representations of the Zero Matrix

Suppose that x represents the same matrix action as in our discussion above. Then,

$$x \cdot (1, 0, 0) = (x, 0, 0) = (0, 1, 1)$$

That is, the first column of both matrix representations is the same! The same is true for all columns:

$$\left(\begin{array}{ccc} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{array} \right) = \left(\begin{array}{ccc} 0 & 0 & -1 \\ 1 & -1 & -1 \\ 1 & 0 & -2 \end{array} \right)$$

$$\begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 0 \\ x \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ x \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -2 \end{pmatrix}$$

The column vectors are the same! *But the entries are not!*

Matrix Action Principle

Suppose that a matrix A represents a function according to a column interpretation. If a matrix B does the same thing, then each column of A is equal to the corresponding column of B . *The entries of the columns may not correspond!*

Consider the matrix function determined by following subtraction:

$$\underbrace{\begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix}}_{x \cdot \text{id}} - \underbrace{\begin{pmatrix} 0 & 0 & -1 \\ 1 & -1 & -1 \\ 1 & 0 & -2 \end{pmatrix}}_A = \underbrace{\begin{pmatrix} x & 0 & 1 \\ -1 & x+1 & 1 \\ -1 & 0 & x+2 \end{pmatrix}}_{x \cdot \text{id} - A}$$

The reader should be convinced that this matrix function should always output the 0-vector in \mathbb{R}^3 since both matrices in the subtraction give the same action. That is, this matrix is equivalent *by columns* (not entries!) to the 0-matrix:

$$\begin{pmatrix} x & 0 & 1 \\ -1 & x+1 & 1 \\ -1 & 0 & x+2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Example 2. Let x represent the matrix $\begin{pmatrix} 1 & 2 \\ 3 & -4 \end{pmatrix}$. Then

$$\begin{pmatrix} x-1 & -2 \\ -3 & x+4 \end{pmatrix}$$

represents the zero matrix. For instance, consider the matrix multiplication:

$$\begin{pmatrix} x-1 & -2 \\ -3 & x+4 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 5 \end{pmatrix} = \begin{pmatrix} x-11 \\ 5x+17 \end{pmatrix}$$

Let's verify that $(x-11, 5x+23)$ is the zero vector since it comes from multiplying the zero matrix to a column vector.

$$(x-11, 5x+23) = x \cdot (1, 0) + 5x \cdot (0, 1) + (-11, 17)$$

$$= (1, 3) + (10, -20) + (-11, 17) = (0, 0)$$

just as expected.

7.1.3 Polynomial Scalars That Act Like Zero



Video

We just saw an example of a matrix with polynomial entries that acts like zero. Yet what about a polynomial itself (other than zero) that acts as a zero scalar? Such polynomials have many uses if we understand what matrix the variable x represents. To get us started, let's look at an example. Suppose that we let the variable x represent the matrix:

$$x = \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}$$

Now the matrix

$$\begin{pmatrix} x-1 & -1 \\ -1 & x-3 \end{pmatrix}$$

acts as the zero matrix. Let's compute the determinant of this matrix:

$$(x-1) \cdot (x-3) - (-1)(-1) = x^2 - 4x + 2$$

Is this determinant zero? We know that the matrix it comes from represents the zero function...is this enough? Let's check to see if this polynomial is a zero scalar:

$$\underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}}_{x^2}^2 - 4 \cdot \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}}_{-4x} + 2 \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{+2}$$

Notice that we are thinking of $+2$ as being the scalar matrix

$$2 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

Constants in Polynomials as Scalar Matrices

Any constant in a polynomial scalar where x represents a matrix is treated itself as a scalar matrix.

Let's run the matrix computation itself right now and see what we get:

$$\begin{aligned}
 & \underbrace{\left(\begin{array}{cc} 1 & 1 \\ 1 & 3 \end{array} \right)^2}_{x^2} - 4 \cdot \underbrace{\left(\begin{array}{cc} 1 & 1 \\ 1 & 3 \end{array} \right)}_{-4x} + 2 \cdot \underbrace{\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right)}_{+2} \\
 &= \underbrace{\left(\begin{array}{cc} 2 & 4 \\ 4 & 10 \end{array} \right)}_{x^2} + \underbrace{\left(\begin{array}{cc} -4 & -4 \\ -4 & -12 \end{array} \right)}_{-4x} + \underbrace{\left(\begin{array}{cc} 2 & 0 \\ 0 & 2 \end{array} \right)}_{+2} \\
 &= \left(\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array} \right)
 \end{aligned}$$

Notice that we get the zero matrix! This means that scalar multiplication by $x^2 - 4x + 2$ is the same as matrix multiplication by the zero matrix. That is, $x^2 - 4x + 2$ is the same as the zero scalar.

Is such a determinant always a zero scalar? We will see that it is when we learn about minimal polynomials.

Yet realize that the *entries* of the zero matrix and this other matrix *are not equal*—their columns are. *Therefore, we cannot simply assume their determinants are equal.* There is some work to do to make this precise. This is done in the section on minimal polynomials.

Characteristic Polynomial

The characteristic polynomial of a $n \times n$ square matrix A is the determinant of the matrix $x \cdot \text{id}_{\mathbb{R}^n} - A$. This determinant is a polynomial.

Theorem 7.1.2

Let x represent the action of a square matrix A as a scalar. Then, the characteristic polynomial of this matrix is scalar that behaves like zero.

Proof. This is only a sketch that looks forward to what we will do in the section on *minimal polynomials* and is provided for completeness. *For a complete understanding of the proof, go to the section on minimal polynomials.* We will see in that section how we can do row and column sliding operations (only airdropping) with polynomial scalars to change the matrix $(x \cdot \text{id}_{\mathbb{R}^n} - A)$ to a diagonal matrix D . We will see that this diagonal matrix D *again represents the zero matrix*. The determinant of D and $(x \cdot \text{id}_{\mathbb{R}^n} - A)$ *are the same since airdropping does not change the determinant*—simply the product of the diagonal of D . This is also the

characteristic polynomial $p(x)$ of the matrix A . Now make a scalar matrix out of $p(x)$:

$$K = \begin{pmatrix} p(x) & 0 & \cdots & 0 \\ 0 & p(x) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p(x) \end{pmatrix}$$

Using the idea that *diagonal* matrices simply multiply together at their entries *and every diagonal entry of D is a factor of $p(x)$* :

$$K = \underbrace{D}_{\text{zero matrix}} \cdot (\text{another diagonal matrix})$$

Therefore, K also represents the zero function! That is, the scalar $p(x)$ that defines K is a zero scalar. \square

So the polynomial we found $x^2 - 4x + 2$ is the characteristic polynomial of the matrix we began with and so is a zero scalar by this theorem just as we verified.

Yet how is this useful? Here is one beginning application. But we will see others. What if we wanted to raise the matrix x to an exponent—say, x^5 ? Then, we think if we divide the polynomial x^5 by the polynomial $x^2 - 4x + 2$, we get:

$$x^5 = \underbrace{\text{quotient} \cdot (x^2 - 4x + 2)}_{=0} + \text{remainder}$$

That is, x^5 can be calculated simply by computing the matrix given by the polynomial remainder. Consider:

$$\begin{array}{r} & x^3 + 4x^2 + 14x + 48 \\ \hline x^2 - 4x + 2) & x^5 \\ & -x^5 + 4x^4 - 2x^3 \\ \hline & 4x^4 - 2x^3 \\ & -4x^4 + 16x^3 - 8x^2 \\ \hline & 14x^3 - 8x^2 \\ & -14x^3 + 56x^2 - 28x \\ \hline & 48x^2 - 28x \\ & -48x^2 + 192x - 96 \\ \hline & 164x - 96 \end{array}$$

Therefore, the matrix given by the remainder $164x - 96$ is the same as the matrix x^5 :

$$\begin{aligned} \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}}_{x^5}^5 &= 164 \cdot \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}}_{164x} - \underbrace{\begin{pmatrix} 96 & 0 \\ 0 & 96 \end{pmatrix}}_{-96} \\ &= \begin{pmatrix} 164 & 164 \\ 164 & 492 \end{pmatrix} - \begin{pmatrix} 96 & 0 \\ 0 & 96 \end{pmatrix} = \begin{pmatrix} 68 & 164 \\ 164 & 396 \end{pmatrix} \end{aligned}$$

We have just calculated matrix x^5 and we never even multiplied two matrices together! What we needed simply was to know to divide by the polynomial $x^2 - 4x + 2$. What was special about this polynomial? We knew that it was a zero scalar!

7.1.4 Generalized Synthetic Division

To simplify the division process and to be able to easily spot patterns with powers of matrices, we can go right to something called *generalized synthetic division* which works when we divide by any polynomial whose leading coefficient is 1 [2]. (This is better than what can be done with the standard synthetic division process!)

Let's run through an example:

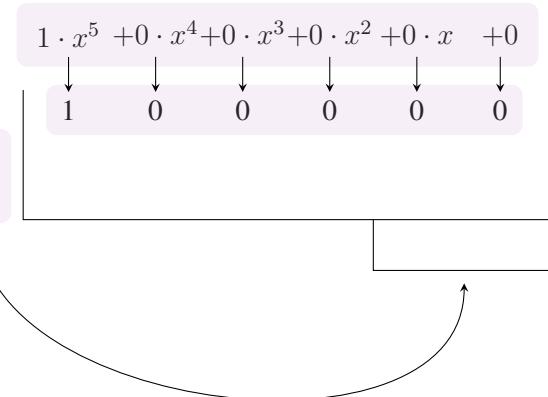
Step 1:

This leading
coefficient is 1
so process will
work.



$$1 \cdot x^2 - 4x + 2$$

Negate *these*
two coefficients.



Step 2:

$$\begin{array}{r} 4 \\ -2 \\ \hline 1 & 0 & 0 & 0 & 0 \\ | & drop \\ 1 & & & & \end{array}$$

Step 3:

$$\left| \begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 4 & -2 & & & & \\ -2 & & & & & \\ \hline 1 & & & & & \end{array} \right|$$

A diagram showing a row operation on a matrix. A pink box labeled "multiply" has arrows pointing from the scalar 4 to the first column and from the scalar -2 to the second column. A pink arrow labeled "add" points from the second row to the third row.

Step 4:

$$\left| \begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 4 & -2 & & & & \\ \hline 1 & 4 & & & & \end{array} \right|$$

A diagram showing a row operation on a matrix. A pink box labeled "add" has an arrow pointing from the second row to the third row.

Step 5:

$$\left| \begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 4 & -2 & & & & \\ -2 & & & & & \\ \hline 1 & 4 & & & & \end{array} \right|$$

A diagram showing a row operation on a matrix. A pink box labeled "multiply" has arrows pointing from the scalar 4 to the first column and from the scalar -2 to the second column. A pink arrow labeled "add" points from the second row to the third row.

Step 6:

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 4 & 4 & 16 & add \\ -2 & & -2 & -8 \\ \hline 1 & 4 & 14 & & & \end{array} \right]$$

Step 7:

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 4 & 4 & 16 & 56 \\ -2 & & -2 & -8 & -28 \\ \hline 1 & 4 & 14 & & & \end{array} \right]$$

multiply

Step 8:

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 4 & 4 & 16 & 56 & add \\ -2 & & -2 & -8 & -28 \\ \hline 1 & 4 & 14 & 48 & & \end{array} \right]$$

Step 9:

$$\begin{array}{r} 4 \\ -2 \end{array} \left| \begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 0 \\ & 4 & 16 & 56 & 192 & \\ & & -2 & -8 & -28 & -96 \\ \hline 1 & 4 & 14 & 48 & & \end{array} \right.$$

multiply

Step 10:

$$\begin{array}{r} 4 \\ -2 \end{array} \left| \begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 0 \\ & 4 & 16 & 56 & 192 & \\ & & -2 & -8 & -28 & -96 \\ \hline 1 & 4 & 14 & 48 & & \end{array} \right. \quad \begin{array}{l} add \\ \downarrow \\ 164 \quad -96 \\ \hline 164x - 96 \end{array}$$

remainder

Notice that this is exactly what we got as the remainder of this same division in the previous subsection.

Example 3. Let's use this technique to find

$$\left(\begin{array}{cc} 0 & -1 \\ 1 & -1 \end{array} \right)^6$$

We take the determinant of

$$\left(\begin{array}{cc} x & 1 \\ -1 & x+1 \end{array} \right)$$

and find that the characteristic polynomial is $x^2 + x + 1$.

Now, we perform generalized synthetic division dividing $x^2 + x + 1$ into x^6 :

$$\begin{array}{c} \left[\begin{array}{cccccc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & & & & & & \\ -1 & & & & & & \\ \hline 1 & -1 & 0 & 1 & -1 & & \\ & & & & & 0 & 1 \\ & & & & & & \\ \end{array} \right] \\ 0x + 1 \\ \text{remainder} \end{array}$$

Notice that the remainder is simply 1 as a scalar. Turned into a matrix, this is simply the scalar matrix

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

Therefore:

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^6 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Example 4. Notice in the previous example that the last line of the generalized synthetic division process is patterned. Continuing this pattern:

$$\underbrace{1 \ -1 \ 0}_{\text{1}} \ \underbrace{1 \ -1 \ 0}_{\text{2}} \ \underbrace{1 \ -1 \ 0}_{\text{3}} \ \underbrace{1 \ -1 \ 0}_{\text{4}} \dots$$

If we changed the power from x^6 to x^{23} , we could just think about where we would land in this pattern. Then we would know what the matrix to the 23rd power would be! Notice that for x^6 the bottom line is 7 positions long and the pattern block $\underbrace{1 \ -1 \ 0}_{\text{1}}$ is 3 positions long. Therefore, the last two positions of the last line come from the ending 0 in the pattern block and the beginning 1 of another.

Now, for x^{23} , we have 24 positions to consider. Now, let's think of dividing 24 positions into pattern blocks of size 3. Notice that when we divide 23 by 3 we get a remainder of 0. This tells us that the pattern blocks completely fill out the bottom line. The last two positions of the line will look like $-1 \ 0$ which represents $-x$. Therefore:

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^{23} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$$

which is just the negative of the matrix itself.

Example 5. Continuing the last two examples, suppose that we wish to compute

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^{100}$$

We know that there will be 101 positions on the bottom line and that 101 is 2 past 99 which is completely filled with pattern blocks each of size 3. Therefore, we take the first two positions of a pattern block: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ which represents $x - 1$. In terms of matrices, this is:

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^{100} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & -2 \end{pmatrix}$$

Theorem 7.1.3

The characteristic polynomial *always* has a leading coefficient of 1 so that the generalized synthetic division technique always works!

Proof. This is left as an exercise to the reader. Think about how a determinant is formed as a sum of permuted diagonal products. \square

Example 6. Extra: *synthetic division for any polynomial division* comes from extending our generalized synthetic algorithm as follows. Suppose that we would like to divide $6x^4 - 7x^3 - 2x^2 + 5x + 1$ by $2x^2 - 3x + 1$. Since the divisor has leading coefficient “2,” we create a wavy $\div 2$ line along the bottom line *until the remainder*. Any time we cross that line to drop a number or put a sum, we *first divide by 2*. We proceed as follows:

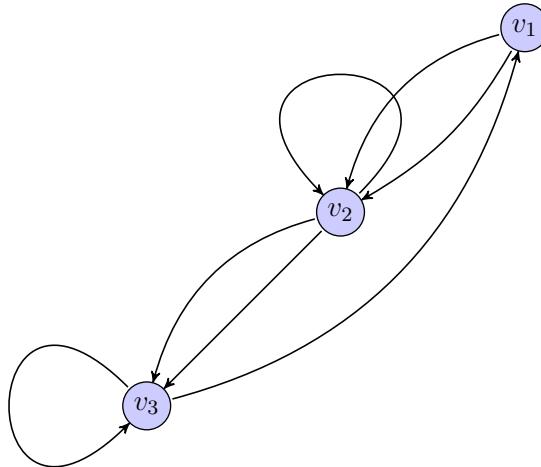
$$\begin{array}{r|ccccc} & 6 & -7 & -2 & 5 & 1 \\ 3 & & 9 & 3 & -3 & \\ -1 & & & -3 & -1 & 1 \\ \hline \div 2 & 3 & 1 & -1 & 1 & 2 \end{array}$$

More video examples:



7.1.5 Counting Paths

Earlier in the text we talked about what an adjacency matrix of a digraph is. We saw that the n th power of this adjacency matrix tells us how many paths that are n -edges long go from one vertex to another. For instance, suppose that we have the following digraph:



Its adjacency matrix is:

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

Suppose we compute:

$$A^5 = \begin{pmatrix} 12 & 26 & 32 \\ 16 & 25 & 42 \\ 13 & 16 & 25 \end{pmatrix}$$

Let's look at the first row. The “12” tells us that there are 12 paths that are 5 edges long that start at vertex 1 and go to vertex 1 since the “12” is in the first row and first column. The “26” tells us that there are 26 paths that are 5 edges long that start at vertex 1 and go to vertex 2 since the “26” is in the first row (signifying that we start at vertex 1) and the second column (signifying that we end at vertex 2). Likewise, the “32” tells us that there are 32 paths of length 5 that start at vertex 1 and end at vertex 3.

Example 7. Suppose that the matrix

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

represents an adjacency matrix on a graph with two vertices. Let's figure out how many paths there are from vertex 2 to vertex 1 of length 6. To do so, we need to compute A^6 . First, we find that the characteristic polynomial is:

$$\det \begin{pmatrix} x & -1 \\ -2 & x-1 \end{pmatrix} = x^2 - x - 2$$

Next, we divide x^6 by $x^2 - x - 2$ using generalized synthetic division:

$$\begin{array}{r}
 & \begin{array}{ccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 1 & 3 & 5 & 11 \\ & 2 & & 2 & 6 & 10 & 22 \\ & 1 & 1 & 3 & 5 & 11 & 21 & 22 \\ & & & & & & 21x + 22 \\ & & & & & & \text{remainder} \end{array} \\
 \begin{array}{c} 1 \\ 2 \end{array} &
 \end{array}$$

$$A^6 = 21 \cdot \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} + 22 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 22 & 21 \\ 42 & 43 \end{pmatrix}$$

Since our paths start at vertex 2, we go to the second row. Since our paths end at vertex 1 we go to column 1. The entry reads as “42.” Therefore, there are 42 paths that are six edges long that start at vertex 2 and end at vertex 1.

Counting Number of Paths

Let A be an adjacency matrix for a digraph. The (i, j) entry of the matrix A^n tells us how many paths that are n edges long start at vertex i and end at vertex j .

7.1.6 Recursive Sequences



Earlier in the text we learned how to come up with a formula for a_n if it represents a sequence a_0, a_1, a_2, \dots defined so $a_0 = 1$ and $a_1 = 3$ and $a_{n+2} = 2 \cdot a_n + a_{n+1}$. This formula involved a matrix power. We found that

$$a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

Let's find the characteristic polynomial of

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

and then use it to determine how to compute A^n .

$$\det \begin{pmatrix} x & -1 \\ -2 & x-1 \end{pmatrix} = x^2 - x - 2$$

What is different this time is that the exponent n is arbitrary instead of fixed. We could try to find a pattern in the generalized synthetic division process as we have before. But the pattern is usually not readily apparent. Usually there are no repeating blocks. So instead, we use another strategy. We are looking for the remainder when we divide x^n by $x^2 - x - 2$. The remainder always has degree *strictly less than* what we are dividing by.

We are currently dividing by $x^2 - x - 2$ which has degree 2. Hence, the remainder will be of the form $ax + b$. So:

$$x^n = (\text{quotient}) \cdot (x^2 - x - 2) + \underbrace{ax + b}_{\text{remainder}}$$

Now in reality, with x representing the matrix A , $(x^2 - x - 2) = 0$, so our equation reads as: $x^n = ax + b$. Yet, to get information about the scalars a and b , we consider the expanded equation and consider scalar values of x (*instead of matrix values*) that *again* give us the equality $x^n = ax + b$. To do so, we factor $(x^2 - x - 2)$ to see:

$$x^n = (\text{quotient}) \cdot \underbrace{(x - 2)(x + 1)}_{x^2 - x - 2} + ax + b.$$

The scalar values $x = 2$ and $x = -1$ give us the equality $x^2 - x - 2 = 0$ and therefore the equality $x^n = ax + b$. Substituting these in one at a time for x , we obtain:

$$x = 2 : \quad 2^n = 0 + a \cdot 2 + b.$$

$$x = -1 : \quad (-1)^n = 0 + a \cdot (-1) + b.$$

So, we have a system of equations:

$$\begin{aligned} 2a + b &= 2^n \\ -a + b &= (-1)^n \end{aligned}$$

Subtracting the second equation from the first, we have:

$$3a = 2^n - (-1)^n$$

$$a = \frac{2^n - (-1)^n}{3}$$

Now, using $-a + b = (-1)^n$, we have:

$$b = a + (-1)^n = \frac{2^n - (-1)^n}{3} + (-1)^n$$

We will use these calculations in a minute. But first, let's go back to the matrix product :

$$a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}}_{A^n = x^n = ax + b}^n \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

We rewrite $ax + b$ as a matrix and replace A^n by it:

$$ax + b = a \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}}_x + \underbrace{\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}}_b$$

$$a_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \left(\underbrace{\begin{pmatrix} 0 & a \\ 2a & a \end{pmatrix}}_{ax} + \underbrace{\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}}_b \right) \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

Realize that multiplying on the left by $\begin{pmatrix} 1 & 0 \end{pmatrix}$ via a row interpretation just picks out the first row of a matrix. Also, matrix multiplication distributes. Hence, distributing $\begin{pmatrix} 1 & 0 \end{pmatrix}$ into the parentheses, we get:

$$a_n = \left(\begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 0 & a \\ 2a & a \end{pmatrix}}_{ax} + \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}}_b \right) \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

$$a_n = \left(\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \right) \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} b & a \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix} = b + 3a$$

$$a_n = b + 3a = \underbrace{(a + (-1)^n)}_b + 3a = 4a + (-1)^n = 4 \cdot \frac{2^n - (-1)^n}{3} + (-1)^n, \quad n \geq 2$$

Notice that this formula is not a recursion. Rather, it is written as an expression that you can just plug n into.

Theorem 7.1.4

Suppose that $a_{n+2} = r \cdot a_n + t \cdot a_{n+1}$. Then, the characteristic polynomial of

$$A = \begin{pmatrix} 0 & 1 \\ r & t \end{pmatrix}$$

is $x^2 - tx - r$. Find the remainder $ax + b$ from dividing x^n by $x^2 - tx - r$. Then,

$$a_n = b \cdot a_0 + a \cdot a_1 \quad n \geq 2$$

How to Find the Remainder without Dividing

Above we saw an example when the characteristic polynomial $p(x)$ had distinct roots r_1 and r_2 so that it factored as $p(x) = (x - r_1) \cdot (x - r_2)$. In this case, we can use a system of equations to find the remainder when we divide x^n by $p(x)$:

$$\begin{aligned} r_1^n &= a \cdot r_1 + b \\ r_2^n &= a \cdot r_2 + b \end{aligned}$$

Example 8. Suppose that $a_{n+2} = 3 \cdot a_n + 2a_{n+1}$ with $a_0 = 1$ and $a_1 = 1$. Then take the characteristic polynomial $x^2 - 2x - 3 = (x - 3)(x + 1)$ and divide it into x^n to get a remainder $ax + b$. We know that the equality $x^n = ax + b$ also holds not only when x is a matrix, but when it is the scalar 3 or the scalar -1 . This allows us to find the scalars a and b by considering the system of equations:

$$\begin{aligned} 3^n &= 3a + b \\ (-1)^n &= -a + b \end{aligned}$$

Subtracting the second equation from the first, we get:

$$3^n - (-1)^n = 4a \quad a = \frac{3^n - (-1)^n}{4}$$

We also know that $b = (-1)^n + a$. Therefore,

$$a_n = \underbrace{((-1)^n + a)}_b \cdot \underbrace{a_0}_1 + a \cdot \underbrace{a_1}_1 = (-1)^n + 2a$$

$$a_n = (-1)^n + 2 \cdot \underbrace{\frac{3^n - (-1)^n}{4}}_a$$

Notice that using this formula, $a_2 = 5$ and also using the recursion, $a_2 = 3 \cdot \underbrace{1}_{a_0} + 2 \cdot \underbrace{1}_{a_1} = 5$.

Example 9. For those who have seen Taylor series (calculus II). Suppose now that $a_{n+2} = -a_n + 2a_{n+1}$ and $a_0 = 1$ and $a_1 = 1$. Then the characteristic polynomial is $x^2 - 2x + 1 = (x - 1)^2$. Notice that we cannot get two different scalar values for x that make $x^2 - 2x + 1 = 0$ and subsequently $x^n = ax + b$. So we do not get two equations which we would need to determine the scalars a and b . Hence, we resort to another technique.

We find the Taylor series expansion of $f(x) = x^n$ with center $x = 1$ (the one scalar that works). We get:

$$f(x) = f(1) + f'(1)(x - 1) + \underbrace{\frac{f''(1)}{2!}(x - 1)^2 + \frac{f'''(1)}{3!}(x - 1)^3 + \dots}_{(x-1)^2=x^2-2x+1 \text{ is a factor of}}$$

Since $x^2 - 2x + 1 = 0$, we have:

$$f(x) = f(1) + f'(1)(x - 1)$$

Using $f'(x) = nx^{n-1}$:

$$\underbrace{x^n}_{f(x)} = \underbrace{(1)^n}_{f(1)} + \underbrace{n \cdot (1)^{n-1}}_{f'(1)} \cdot (x - 1)$$

$$x^n = 1 + n(x - 1) = \underbrace{n}_a x + \underbrace{(1 - n)}_b$$

Therefore, with $a = n$ and $b = 1 - n$, we have

$$a_n = (1 - n) \cdot \underbrace{1}_{a_0} + n \cdot \underbrace{0}_{a_1} = 1 - n, \quad n \geq 2$$

Key Concepts from this Section

- **scalar matrix:** (page 743) A square $n \times n$ matrix like

$$k \cdot \text{id}_{\mathbb{R}^n} = \begin{pmatrix} k & 0 & \cdots & 0 \\ 0 & k & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & k \end{pmatrix}$$

is called a *scalar matrix*. It behaves like a scalar k as a function on vectors. This is true in both a row and a column interpretation. The effect is to send a vector v to kv .

- **theorem 7.1.1 :** (page 745) Let A be a square $n \times n$ matrix and let x represent the action of A as a scalar. The assumption that the scalar x behaves like A turns $\mathbb{R}[x]^n$ into \mathbb{R}^n .
- **matrix action principle:** (page 746) Suppose that a matrix A represents a function according to a column interpretation. If a matrix B does the same thing, then each column of A is equal to the corresponding column of B . *The entries of the columns may not correspond!*
- **constants in polynomials as scalar matrices:** (page 747) Any constant in a polynomial scalar where x represents a matrix is treated itself as a scalar matrix.

- **characteristic polynomial:** (page 748) The characteristic polynomial of a $n \times n$ square matrix A is the determinant of the matrix $x \cdot \text{id}_{\mathbb{R}^n} - A$. This determinant is a polynomial.
- **theorem 7.1.2 :** (page 748) Let x represent the action of a square matrix A as a scalar. Then, the characteristic polynomial of this matrix is scalar that behaves like zero.
- **theorem 7.1.3 :** (page 755) The characteristic polynomial *always* has a leading coefficient of 1 so that the generalized synthetic division technique always works!
- **synthetic division for any polynomial division:** (page 755) See the example in the text.
- **counting number of paths:** (page 757) Let A be an adjacency matrix for a digraph. The (i, j) entry of the matrix A^n tells us how many paths that are n edges long start at vertex i and end at vertex j .
- **theorem 7.1.4 :** (page 759) Suppose that $a_{n+2} = r \cdot a_n + t \cdot a_{n+1}$. Then, the characteristic polynomial of

$$A = \begin{pmatrix} 0 & 1 \\ r & t \end{pmatrix}$$

is $x^2 - tx - r$. Find the remainder $ax + b$ from dividing x^n by $x^2 - tx - r$. Then,

$$a_n = b \cdot a_0 + a \cdot a_1 \quad n \geq 2$$

- **how to find the remainder without dividing:** (page 759) Above we saw an example when the characteristic polynomial $p(x)$ had distinct roots r_1 and r_2 so that it factored as $p(x) = (x - r_1) \cdot (x - r_2)$. In this case, we can use a system of equations to find the remainder when we divide x^n by $p(x)$:

$$\begin{aligned} r_1^n &= a \cdot r_1 + b \\ r_2^n &= a \cdot r_2 + b \end{aligned}$$

7.1.7 Exercises

Rewriting a Vector with Polynomial Entries

Rewrite the vector v as a vector in \mathbb{R}^3 without polynomial entries if x is given by the indicated matrix.

1. $(-x^2 + 1, x^2, 2)$

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

2. $(-x + 2, -x, x + 1)$

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

3. $(-x^2 - 1, 2x^2, 2x + 1)$

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

4. $(x, 2x + 1, x^2 - x + 2)$

$$x = \begin{pmatrix} -1 & 1 & 1 \\ -1 & 1 & -1 \\ 2 & -1 & 2 \end{pmatrix}$$

5. $(2x^2 - 1, 2x^2 + 1, x^2 + 1)$

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

6. $(2x^2 + 2, 2x^2 - x - 1, 2x^2 + x - 1)$

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

7. $(-x^2 + 2x + 2, -x^2 + x, x^2 + 2x + 1)$

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

8. $(-x^2 + 2x, x^2 + 2x, -x^2 + 2x - 1)$

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

9. $(x - 1, x^2 + x + 1, -1)$

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

10. $(2x^2, x^2 + x - 1, 2x)$

$$x = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

Matrices to a Power

Use the characteristic polynomial and generalized synthetic division to find the following matrix powers.

11. $\begin{pmatrix} 0 & 2 \\ 1 & -1 \end{pmatrix}^7$

12. $\begin{pmatrix} 0 & -2 \\ 1 & -1 \end{pmatrix}^7$

13. $\begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}^5$

14. $\begin{pmatrix} 0 & -3 \\ 1 & 2 \end{pmatrix}^6$

15. $\begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}^5$

16. $\begin{pmatrix} 0 & -3 \\ 1 & -1 \end{pmatrix}^6$

17. $\begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}^5$

18. $\begin{pmatrix} 0 & -3 \\ 1 & -2 \end{pmatrix}^6$

19. $\begin{pmatrix} 0 & 3 \\ 1 & -1 \end{pmatrix}^6$

20. $\begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}^6$

21. $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^7$

22. $\begin{pmatrix} 0 & 3 \\ 1 & -2 \end{pmatrix}^5$

23. $\begin{pmatrix} 0 & -2 \\ 1 & 1 \end{pmatrix}^5$

24. $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^6$

25. $\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}^7$

26. $\begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}^5$

Practice with Generalized Synthetic Division

Use the generalized synthetic division technique to perform the following polynomial divisions.

27. Divide $2x^5 - x^4 - 6x^3 - 3x^2 + 6x + 4$
by $x^2 - x - 2$

29. Divide $3x^5 + 5x^4 + 6x^3 + x^2 + 3x - 4$
by $x^2 + x + 1$

31. Divide $2x^5 + x^4 - x^3 - 2x^2 + 2x$
by x^2

33. Divide $3x^5 + x^4 + 4x^3 - x^2 + 5x - 1$
by $x^2 + 1$

35. Divide $2x^5 - 3x^4 - x^3 + x^2 + 7x - 4$
by $x^2 - 2x + 1$

28. Divide $2x^5 - 4x^4 + x^3 + 2x^2 + 3x - 1$
by $x^2 - 2x + 1$

30. Divide $2x^5 - 3x^3 - 3x^2 + x - 1$
by $x^2 - x - 1$

32. Divide $3x^5 + 4x^4 - 3x^3 - x^2 - 2x + 3$
by $x^2 + x - 2$

34. Divide $3x^5 - 2x^4 + x^2 + 3x + 2$
by x^2

36. Divide $3x^5 + 2x^4 + 4x^3 + 4x$
by $x^2 + 1$

Use the synthetic division technique for any polynomial division to complete the following.

37. Divide $6x^5 + 7x^4 + x^3 + 6x^2 + 6x - 5$
by $3x^2 + 2x - 2$

39. Divide $12x^5 + 14x^4 - 4x^3 - 10x^2 - 2x + 6$
by $3x^2 + 2x - 2$

41. Divide $6x^5 + x^4 - 6x^3 - 7x^2 + 2x + 3$
by $2x^2 - x - 2$

43. Divide $8x^5 - 4x^4 + 6x^3 + 4x^2 + 3x + 1$
by $2x^2 - 2x + 2$

45. Divide $8x^5 + 8x^4 + 4x^3 - 4x^2 + 1$
by $2x^2 + 2x + 2$

38. Divide $6x^5 + x^4 - 12x^3 - 2x^2 + 8x$
by $3x^2 + 2x - 2$

40. Divide $4x^5 - 3x^3 + x^2 - 3$
by $2x^2 - x - 2$

42. Divide $12x^5 + 14x^4 + 8x^3 - 2x^2 + x + 2$
by $4x^2 + 2x$

44. Divide $4x^5 + 6x^4 + 8x^3 + 8x^2 + 8x + 6$
by $2x^2 + 2x + 2$

46. Divide $8x^5 - 4x^4 - 8x^3 + 2x^2 + 6x + 1$
by $2x^2 - x - 1$

Counting Paths

Use a matrix power and generalized synthetic division to find the number of paths fit the given criteria.

47. $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

paths of length 5 from vertex 1 to vertex
1

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

paths of length 6 from vertex 2 to vertex
1

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

paths of length 5 from vertex 1 to vertex
1

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

paths of length 5 from vertex 2 to vertex
2

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

paths of length 5 from vertex 1 to vertex
1

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

paths of length 7 from vertex 1 to vertex
1

Recursive Sequences

Find the remainder $ax + b$ of dividing x^n by an appropriate polynomial using a system of equations in order to find a simple nonrecursive formula for a_n

53. $a_{n+2} = 2 \cdot a_n + (-1) \cdot a_{n+1}$

$$a_0 = 2, \quad a_1 = -2$$

54. $a_{n+2} = 6 \cdot a_n + (1) \cdot a_{n+1}$

$$a_0 = -1, \quad a_1 = 2$$

55. $a_{n+2} = -6 \cdot a_n + (-5) \cdot a_{n+1}$

$$a_0 = 0, \quad a_1 = 1$$

56. $a_{n+2} = 3 \cdot a_n + (2) \cdot a_{n+1}$

$$a_0 = -2, \quad a_1 = -1$$

57. $a_{n+2} = -3 \cdot a_n + (4) \cdot a_{n+1}$

$$a_0 = -1, \quad a_1 = -2$$

58. $a_{n+2} = 6 \cdot a_n + (-1) \cdot a_{n+1}$

$$a_0 = 1, \quad a_1 = -2$$

59. $a_{n+2} = 0 \cdot a_n + (3) \cdot a_{n+1}$

$$a_0 = 1, \quad a_1 = 0$$

60. $a_{n+2} = -3 \cdot a_n + (-4) \cdot a_{n+1}$

$$a_0 = 1, \quad a_1 = -2$$

61. $a_{n+2} = 0 \cdot a_n + (-1) \cdot a_{n+1}$

$$a_0 = -2, \quad a_1 = 2$$

62. $a_{n+2} = 6 \cdot a_n + (-1) \cdot a_{n+1}$

$$a_0 = 2, \quad a_1 = 1$$

63. $a_{n+2} = 3 \cdot a_n + (2) \cdot a_{n+1}$

$$a_0 = -1, \quad a_1 = 2$$

64. $a_{n+2} = 3 \cdot a_n + (2) \cdot a_{n+1}$

$$a_0 = 0, \quad a_1 = -1$$

Do the same as above for the following except use a Taylor expansion technique—the appropriate polynomial divisor has a repeated root.

65. $a_{n+2} = -4 \cdot a_n + (-4) \cdot a_{n+1}$

$$a_0 = -2, \quad a_1 = 0$$

66. $a_{n+2} = -9 \cdot a_n + (-6) \cdot a_{n+1}$

$$a_0 = -2, \quad a_1 = 0$$

67. $a_{n+2} = -1 \cdot a_n + (-2) \cdot a_{n+1}$

$$a_0 = -2, \quad a_1 = 1$$

68. $a_{n+2} = -4 \cdot a_n + (-4) \cdot a_{n+1}$

$$a_0 = 1, \quad a_1 = 2$$

69. $a_{n+2} = -9 \cdot a_n + (6) \cdot a_{n+1}$

$$a_0 = 1, \quad a_1 = 2$$

70. $a_{n+2} = -1 \cdot a_n + (-2) \cdot a_{n+1}$

$$a_0 = -2, \quad a_1 = 2$$

71. $a_{n+2} = -4 \cdot a_n + (4) \cdot a_{n+1}$

$$a_0 = -1, \quad a_1 = -2$$

72. $a_{n+2} = -9 \cdot a_n + (6) \cdot a_{n+1}$

$$a_0 = 2, \quad a_1 = 1$$

73. $a_{n+2} = -4 \cdot a_n + (-4) \cdot a_{n+1}$

$$a_0 = 0, \quad a_1 = 2$$

74. $a_{n+2} = -4 \cdot a_n + (-4) \cdot a_{n+1}$

$$a_0 = 0, \quad a_1 = 1$$

75. $a_{n+2} = -9 \cdot a_n + (-6) \cdot a_{n+1}$

$$a_0 = 2, \quad a_1 = 1$$

76. $a_{n+2} = -9 \cdot a_n + (-6) \cdot a_{n+1}$

$$a_0 = 0, \quad a_1 = -1$$

An Exploration with Pythagorean Triples

77. Primitive Pythagorean Triples: If you can find a right triangle whose sides are all positive integer lengths, you have found a Pythagorean triple. A couple common examples are $(3, 4, 5)$ and $(5, 12, 13)$. You could multiply these by a number and get others (by similarity of triangles): $2 \cdot (3, 4, 5) = (6, 12, 10)$ or $4 \cdot (5, 12, 13) = (20, 48, 52)$. But these new triples would not be considered primitive since the integers share common factors. We will explore a way that *all* primitive Pythagorean triples can be obtained through a series of questions:

- (a) Prove that any symmetric 2×2 matrix $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ whose range has dimension 1 and $a, b, c > 0$, follows the following rules:

- $c = \frac{b}{a} \cdot b$ Hint: the rows are multiples of each other (why?) and a was multiplied by something to get b .
- $b^2 + (\frac{a-c}{2})^2 = (\frac{a+c}{2})^2$
- $A = \begin{pmatrix} (\sqrt{a})^2 & \sqrt{a}\sqrt{\frac{b^2}{a}} \\ \sqrt{a}\sqrt{\frac{b^2}{a}} & \left(\sqrt{\frac{b^2}{a}}\right)^2 \end{pmatrix} = \begin{pmatrix} \sqrt{a} & \\ \sqrt{a} & \sqrt{\frac{b^2}{a}} \end{pmatrix} \cdot \begin{pmatrix} \sqrt{a} & \\ \sqrt{\frac{b^2}{a}} & \end{pmatrix}$

- (b) Notice that Pythagorean triples are therefore represented by a column vector of length 2. For instance, $\begin{pmatrix} 3 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 \end{pmatrix} = \begin{pmatrix} 9 & 3 \\ 3 & 1 \end{pmatrix}$ represents the Pythagorean triple found with 3, then from the diagonal entries: $\frac{9-1}{2} = 4$ and $\frac{9+1}{2} = 5$. In order to keep an integer Pythagorean triple, we need that both diagonal entries are odd or both are even. We can maintain this idea on $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$ if we multiply it with matrices like the following whose multiplication represent row operations:

$$\begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 2k & 1 \end{pmatrix}$$

For instance, if we compute:

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix} \quad R_1 + 2 \cdot R_2 \mapsto R_1$$

$$\begin{pmatrix} 5 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 5 & 1 \end{pmatrix} = \begin{pmatrix} 25 & 5 \\ 5 & 1 \end{pmatrix}$$

Notice that we get a Pythagorean triple $(5, 12, 13)$ by taking half of the sum 26 and difference 24 of the diagonal entries. We therefore have discovered a new Pythagorean triple that is primitive from our original one. By applying similar row operations to $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$ of both forms, it can be shown that one actually finds *all* primitive Pythagorean triples! Remember though that matrix multiplication (as composition) is not commutative.

Your Exercise: Use matrix powers (by hand) to discover a new primitive Pythagorean triple from:

$$\left(\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right)^8 \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

Remember that the power *does not distribute over the multiplication since the multiplication itself is not commutative*. You are allowed to use technology—except you should at least show what steps you would make for the matrix powers part. Try to do the matrix powers part as much as you can by hand. However, these numbers get quite large in the end (this particular Pythagorean triple is in the trillions—and yet you really can get the matrix power with “small” numbers if you use strategy).

7.1.8 Solutions

1. $(0, 1, 2)$

2. $(4, -2, 3)$

3. $(-4, 4, -2)$

4. $(0, -1, 7)$

5. $(5, 3, 6)$

6. $(10, 23, 4)$

7. $(1, -2, 3)$

8. $(5, -1, -4)$

9. $(-3, 0, -1)$

10. $(3, 3, 9)$

11. Characteristic Polynomial:

$$x^2 + x - 2$$

Remainder:

$$43x - 42$$

Matrix power:

$$\begin{pmatrix} -42 & 86 \\ 43 & -85 \end{pmatrix}$$

12. Characteristic Polynomial:

$$x^2 + x + 2$$

Remainder:

$$7x + 10$$

Matrix power:

$$\begin{pmatrix} 10 & -14 \\ 7 & 3 \end{pmatrix}$$

13. Characteristic Polynomial:

$$x^2 - x - 2$$

Remainder:

$$11x + 10$$

Matrix power:

$$\begin{pmatrix} 10 & 22 \\ 11 & 21 \end{pmatrix}$$

14. Characteristic Polynomial:

$$x^2 - 2x + 3$$

Remainder:

$$-10x + 33$$

Matrix power:

$$\begin{pmatrix} 33 & 30 \\ -10 & 13 \end{pmatrix}$$

15. Characteristic Polynomial:

$$x^2 - 2x - 2$$

Remainder:

$$44x + 32$$

Matrix power:

$$\begin{pmatrix} 32 & 88 \\ 44 & 120 \end{pmatrix}$$

16. Characteristic Polynomial:

$$x^2 + x + 3$$

Remainder:

$$-16x - 3$$

Matrix power:

$$\begin{pmatrix} -3 & 48 \\ -16 & 13 \end{pmatrix}$$

17. Characteristic Polynomial:

$$x^2 - 3x + 2$$

Remainder:

$$31x - 30$$

Matrix power:

$$\begin{pmatrix} -30 & -62 \\ 31 & 63 \end{pmatrix}$$

18. Characteristic Polynomial:

$$x^2 + 2x + 3$$

Remainder:

$$10x + 33$$

Matrix power:

$$\begin{pmatrix} 33 & -30 \\ 10 & 13 \end{pmatrix}$$

19. Characteristic Polynomial:

$$x^2 + x - 3$$

Remainder:

$$-40x + 57$$

Matrix power:

$$\begin{pmatrix} 57 & -120 \\ -40 & 97 \end{pmatrix}$$

20. Characteristic Polynomial:

$$x^2 + 2x + 1$$

Remainder:

$$-6x - 5$$

Matrix power:

$$\begin{pmatrix} -5 & 6 \\ -6 & 7 \end{pmatrix}$$

21. Characteristic Polynomial:

$$x^2 - x + 1$$

Remainder:

$$x$$

Matrix power:

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

22. Characteristic Polynomial:

$$x^2 + 2x - 3$$

Remainder:

$$61x - 60$$

Matrix power:

$$\begin{pmatrix} -60 & 183 \\ 61 & -182 \end{pmatrix}$$

23. Characteristic Polynomial:

$$x^2 - x + 2$$

Remainder:

$$-x + 6$$

Matrix power:

$$\begin{pmatrix} 6 & 2 \\ -1 & 5 \end{pmatrix}$$

24. Characteristic Polynomial:

$$x^2 - x - 1$$

Remainder:

$$8x + 5$$

Matrix power:

$$\begin{pmatrix} 5 & 8 \\ 8 & 13 \end{pmatrix}$$

25. Characteristic Polynomial:

$$x^2 + x - 1$$

Remainder:

$$13x - 8$$

Matrix power:

$$\begin{pmatrix} -8 & 13 \\ 13 & -21 \end{pmatrix}$$

26. Characteristic Polynomial:

$$x^2 - 3x + 1$$

Remainder:

$$55x - 21$$

Matrix power:

$$\begin{pmatrix} -21 & -55 \\ 55 & 144 \end{pmatrix}$$

27. quotient:

$$2x^3 + x^2 - x - 2$$

Remainder:

$$2x$$

28. quotient:

$$2x^3 - x$$

Remainder:

$$4x - 1$$

29. quotient:

$$3x^3 + 2x^2 + x - 2$$

Remainder:

$$4x - 2$$

30. quotient:

$$2x^3 + 2x^2 + x$$

Remainder:

$$2x - 1$$

31. quotient:

$$2x^3 + x^2 - x - 2$$

Remainder:

$$2x$$

32. quotient:

$$3x^3 + x^2 + 2x - 1$$

Remainder:

$$3x + 1$$

33. quotient:

$$3x^3 + x^2 + x - 2$$

Remainder:

$$4x + 1$$

34. quotient:

$$3x^3 - 2x^2 + 1$$

Remainder:

$$3x + 2$$

35. quotient:

$$2x^3 + x^2 - x - 2$$

Remainder:

$$4x - 2$$

36. quotient:

$$3x^3 + 2x^2 + x - 2$$

Remainder:

$$3x + 2$$

37. quotient:

$$2x^3 + x^2 + x + 2$$

Remainder:

$$4x - 1$$

38. quotient:

$$2x^3 - x^2 - 2x$$

Remainder:

$$4x$$

39. quotient:

$$4x^3 + 2x^2 - 2$$

Remainder:

$$2x + 2$$

40. quotient:

$$2x^3 + x^2 + x + 2$$

Remainder:

$$4x + 1$$

41. quotient:

$$3x^3 + 2x^2 + x - 1$$

Remainder:

$$3x + 1$$

42. quotient:

$$3x^3 + 2x^2 + x - 1$$

Remainder:

$$3x + 2$$

43. quotient:

$$4x^3 + 2x^2 + x + 1$$

Remainder:

$$3x - 1$$

44. quotient:

$$2x^3 + x^2 + x + 2$$

Remainder:

$$2x + 2$$

45. quotient:

$$4x^3 - 2x$$

Remainder:

$$4x + 1$$

46. quotient:

$$4x^3 - 2x$$

Remainder:

$$4x + 1$$

47. 3**48.** 40**49.** 12**50.** 21**51.** 135**52.** 360

53. $a_n = \left(\frac{4}{3} (-2)^n + \frac{2}{3}\right)$

54. $a_n = (-(-2)^n)$

55. $a_n = ((-2)^n - (-3)^n)$

56. $a_n = \left(-\frac{3}{4} \cdot 3^n - \frac{5}{4} (-1)^n\right)$

57. $a_n = \left(-\frac{1}{2} \cdot 3^n - \frac{1}{2}\right)$

58. $a_n = \left(\frac{1}{5} \cdot 2^n + \frac{4}{5} (-3)^n\right)$

59. $a_n = (0^n)$

60. $a_n = \left(\frac{1}{2} (-1)^n + \frac{1}{2} (-3)^n\right)$

61. $a_n = (-2)(-1)^n$

62. $a_n = \left(\frac{7}{5} \cdot 2^n + \frac{3}{5}\right)(-3)^n$

63. $a_n = \left(\frac{1}{4} \cdot 3^n - \frac{5}{4}\right)(-1)^n$

64. $a_n = \left(-\frac{1}{4} \cdot 3^n + \frac{1}{4}\right)(-1)^n$

65. $a_n = 2(-2)^n(n-1)$

66. $a_n = 2(-3)^n(n-1)$

67. $a_n = 2(-1)^n(n-1) + (-1)^{n-1}n$

68. $a_n = -(-2)^n(n-1) + 2(-2)^{n-1}n$

69. $a_n = -3^n(n-1) + 2 \cdot 3^{n-1}n$

70. $a_n = 2(-1)^n(n-1) + 2(-1)^{n-1}n$

71. $a_n = 2^n(n-1) - 2 \cdot 2^{n-1}n$

72. $a_n = -2 \cdot 3^n(n-1) + 3^{n-1}n$

73. $a_n = 2(-2)^{n-1}n$

74. $a_n = (-2)^{n-1}n$

75. $a_n = -2(-3)^n(n-1) + (-3)^{n-1}n$

76. $a_n = -(-3)^{n-1}n$

77. Solutions/hints by part:

(a) Notice that one row is just multiplied by $\frac{b}{a}$ to get the other row. The rest in this part is just computation.

(b) We want to compute A^8 for

$$A = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$$

Then, $\det(A - x) = x^2 - 6x + 1$. Notice that this does not have nice roots. Nevertheless, we can use polynomial division! But let's do this strategically. We know that $x^2 \equiv 6x - 1 \pmod{x^2 - 6x + 1}$. Hence, we want to know what $(6x - 1)^4$ is mod $x^2 - 6x + 1$. Let's just look at $(6x - 1)^2$. This is $36x^2 - 12x + 1$. We know that $36x^2 - 12x + 1 = (36 \cdot 6 - 12) \cdot x - 35 + 36(x^2 - 6x + 1)$. Hence,

$$x^4 \equiv (6x - 1)^2 \equiv 204x - 35$$

Now,

$$(204x - 35)^2 = 41616x^2 - 14280x - 1225$$

We need to compute what this is mod $x^2 - 6x + 1$ and the result will be the same as the remainder when we divide x^8 by $x^2 - 6x + 1$. Only this time, the division is simpler. The remainder is $235416x - 42841$.

Hence, we compute:

$$235416 \cdot \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} - 42841 \cdot \text{Id} = \begin{pmatrix} 1134239 & 470832 \\ 470832 & 192575 \end{pmatrix}$$

Remember that our goal is to compute

$$A^8 \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3873549 \\ 1605071 \end{pmatrix}$$

Now we compute:

$$\begin{pmatrix} 3873549 \\ 1605071 \end{pmatrix} \cdot \begin{pmatrix} 3873549 & 1605071 \end{pmatrix} = \begin{pmatrix} 15004381855401 & 6217321166979 \\ 6217321166979 & 2576252915041 \end{pmatrix}$$

Hence, our Pythagorean triple is 6217321166979, 6214064470180, 8790317385221. Checking:

$$6217321166979^2 + 6214064470180^2 = 8790317385221^2$$

Using technology, one can check that the gcd of these numbers is 1. That is, we found a *primitive* Pythagorean triple in the trillions!

Characteristic Polynomial by Central Submatrices

7.2

7.2.1 Finding Coefficients	776
7.2.2 Relating Characteristic Polynomials	783
7.2.3 Studying the Orthonormal Columns	791
7.2.4 An Optional Calculus Proof	796
7.2.5 Counting Spanning Trees	800
7.2.6 Trace and Similarity	806
7.2.7 An Extra Group Map Example	813
7.2.8 Conjugacy and Similarity	816
7.2.9 Exercises	821
7.2.10 Solutions	825

Questions to Guide Your Study:

- *How can we find a characteristic polynomial by using determinants of submatrices?*
- *How are the characteristic polynomials of $B^T B$ and BB^T related for a matrix B ?*
- *How can we use this relationship to quickly find the area of a parallelogram between two vectors that live in \mathbb{R}^n for $n \geq 3$?*
- *How can we use this relationship to quickly find the number of spanning trees in a digraph?*
- *How can comparing traces help us know if two matrices in a group act the same upon a change of perspective?*

7.2.1 Finding Coefficients



We are going to look at another way that we can compute the characteristic polynomial of a matrix. Let's consider the matrix:

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

Now look at:

$$x \cdot \text{id} - A = \begin{pmatrix} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{pmatrix}$$

The characteristic polynomial is the determinant of this matrix $x \text{id} - A$. Recall that the determinant is the sum of signed permuted diagonals. In all the diagonals, only one gives a fourth degree polynomial: the identity do-nothing permutation diagonal indicated above: $(x-1)(x-1)(x-2)(x-2)$ which has a leading term of x^4 . In fact:

The leading term of the characteristic polynomial of a $n \times n$ matrix is always x^n .

So far so good. In our present example, let's see how we could determine the coefficient of x^3 from thinking of permuted diagonals. Notice that the x^3 term *also* comes from this one identity permutation diagonal since 3 of the factors *have to be on the diagonal*. This forces the other factor to be along the diagonal as well. Here are the four situations of distributing down the identity permutation diagonal where **we cross out factors from which we pull an x and circle the entry from which we will take a constant**:

$$\left(\begin{array}{cccc} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{array} \right) \quad \left(\begin{array}{cccc} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{array} \right)$$

$(-1) \cdot x \cdot x \cdot x$ $x \cdot (-1) \cdot x \cdot x$

$$\left(\begin{array}{cccc} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{array} \right) \quad \left(\begin{array}{cccc} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{array} \right)$$

$x \cdot x \cdot (-2) \cdot x$ $x \cdot x \cdot x \cdot (-2)$

Adding these up, we get:

$$-x^3 - x^3 - 2x^3 - 2x^3 = -(1 + 1 + 2 + 2) = -(\text{Sum of diagonal entries of } A)x^3 = -6x^3$$

That is, the coefficient of x^3 is just -1 multiplied to the sum of the diagonal entries of A :

$$\begin{pmatrix} & & 2 & 0 & 1 \\ 1 & & & & \\ & 2 & & & \\ & & 1 & & \\ & 0 & & 1 & 1 \\ & & & 1 & \\ 0 & & & & \\ & 1 & & 2 & 1 \\ & & 0 & & \\ 1 & & & & \\ & 2 & & 2 & 2 \end{pmatrix}$$

Trace

The trace of a matrix A , denoted as $\text{tr}(A)$, is the sum of the entries down its diagonal from top left to bottom right.

The coefficient of x^{n-1} in the characteristic polynomial for a $n \times n$ matrix is always $-\text{tr}(A)$.

Next, to find the coefficient of x^2 , we consider all ways of pulling an x from two of the factors in

$$(x - 1)(x - 1)(x - 2)(x - 2)$$

and two constants from the matrix so that our product is a permuted diagonal. Since we choose two factors on the diagonal. What is left to choose from is a ***central submatrix***—i.e. it is a submatrix which is centered

on the diagonal. When a factor like $x - 1$ is in this central submatrix, we choose the constant -1 . Here is an illustration:

$$\begin{pmatrix} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{pmatrix}$$

$$x^2 \cdot \det \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix} = x^2 \cdot \det \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{pmatrix}$$

$$x^2 \cdot \det \begin{pmatrix} -1 & 0 \\ -1 & -2 \end{pmatrix} = x^2 \cdot \det \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{pmatrix}$$

$$x^2 \cdot \det \begin{pmatrix} -1 & -1 \\ -2 & -2 \end{pmatrix} = x^2 \cdot \det \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$$

$$\begin{pmatrix} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{pmatrix}$$

$$x^2 \cdot \det \begin{pmatrix} -1 & -1 \\ 0 & -2 \end{pmatrix} = x^2 \cdot \det \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$$

$$\begin{array}{c}
 \left(\begin{array}{cccc}
 x-1 & -2 & 0 & -1 \\
 0 & \boxed{x-1} & -1 & \boxed{-1} \\
 -1 & 0 & x-2 & -1 \\
 -2 & \boxed{-1} & -2 & \boxed{x-2}
 \end{array} \right) \quad \left(\begin{array}{cccc}
 x-1 & -2 & 0 & -1 \\
 0 & x-1 & -1 & -1 \\
 -1 & 0 & x-2 & -1 \\
 -2 & -1 & -2 & x-2
 \end{array} \right) \\
 x^2 \cdot \det \begin{pmatrix} -1 & -1 \\ -1 & -2 \end{pmatrix} = x^2 \cdot \det \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \\
 x^2 \cdot \det \begin{pmatrix} -2 & -1 \\ -2 & -2 \end{pmatrix} = x^2 \cdot \det \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}
 \end{array}$$

To get the sum of permuted diagonals coming from this setup is equivalent to finding the determinant of the central submatrix (because it is central the signs we need are the same!) Notice that the constants are all the opposite sign of what they are in A . This means that the corresponding central matrices of A have had two rows multiplied by -1 so that the determinant has been multiplied by -1 . Hence, we simply take the sum of the determinants of the 6 corresponding central submatrices of A :

$$\begin{aligned}
 & \det \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} + \det \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} + \det \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} \\
 & + \det \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} + \det \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} + \det \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} \\
 & = 1 + 2 + 0 + 2 + 1 + 2 = 8.
 \end{aligned}$$

Therefore the coefficient of x^2 will be $+8$.

Next, to find the coefficient of x , we need to choose only one x at a time from the diagonal and then take the determinant of a central submatrix of A —**yet we will change the sign of the determinant of the submatrix of A** . This is because in $x \cdot \text{id} - A$, we have multiplied three rows of that central submatrix by -1 .

$$\begin{pmatrix} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{pmatrix}$$

$$x \cdot \det \begin{pmatrix} -1 & -2 & 0 \\ 0 & -1 & -1 \\ -1 & 0 & -2 \end{pmatrix} = -x \cdot \det \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 2 \end{pmatrix}$$

$$\begin{pmatrix} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{pmatrix}$$

$$x \cdot \det \begin{pmatrix} -1 & -2 & -1 \\ 0 & -1 & -1 \\ -2 & -1 & -2 \end{pmatrix} = -x \cdot \det \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 2 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{pmatrix}$$

$$x \cdot \det \begin{pmatrix} -1 & 0 & -1 \\ -1 & -2 & -1 \\ -2 & -2 & -2 \end{pmatrix} = -x \cdot \det \begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & 1 \\ 2 & 2 & 2 \end{pmatrix}$$

$$\begin{pmatrix} x-1 & -2 & 0 & -1 \\ 0 & x-1 & -1 & -1 \\ -1 & 0 & x-2 & -1 \\ -2 & -1 & -2 & x-2 \end{pmatrix}$$

$$x \cdot \det \begin{pmatrix} -1 & -1 & -1 \\ 0 & -2 & -1 \\ -1 & -2 & -2 \end{pmatrix} = -x \cdot \det \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 1 & 2 & 2 \end{pmatrix}$$

So the coefficient of x is:

$$\underbrace{-\det \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 2 \end{pmatrix} - \det \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 2 & 1 & 2 \end{pmatrix} - \det \begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & 1 \\ 2 & 2 & 2 \end{pmatrix} - \det \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 1 & 2 & 2 \end{pmatrix}}_{-4-3-0-1} = -8$$

Lastly, the determinant of $-A$ itself ignoring the x 's is the constant term. Since $-A$ means we have made four rows negative, we have multiplied the determinant of A by $(-1)^4 = +1$. Hence, the constant term of the

characteristic polynomial is simply the determinant of A which is 2. Therefore the characteristic polynomial of our matrix A is $x^4 - 6x^3 + 8x^2 - 8x + 2$.

The constant term of the characteristic polynomial of an $n \times n$ matrix A is always $(-1)^n \det(A)$.

Example 1. Let's find the characteristic polynomial of

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

Since it is a 2×2 matrix, the leading term is x^2 . The coefficient of x is just the opposite sign of the trace: $-(2 + 3) = 5$ and the constant term is just the determinant of the matrix: $2 \cdot 3 - 4 \cdot 1 = 2$. Hence, the characteristic polynomial is:

$$x^2 - 5x + 2.$$

Characteristic Polynomial of a 2×2 matrix

Let A be a 2×2 matrix. Then the characteristic polynomial is $x^2 - \text{tr}(A)x + \det(A)$

Example 2. Let's find the characteristic polynomial of $\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix}$. The leading term is x^3 . Then since the trace is $1 + 1 + 1 = 3$, the next term is $-3x^2$. There are three central 2×2 submatrices. Add up these determinants:

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

Hence, the next term is $+3x$. We take the negative of the determinant of the 3×3 matrix to get the constant term. Since the determinant is -1 , the constant term will be $+1$. Therefore, the characteristic polynomial of this matrix is $x^3 - 3x^2 + 3x + 1$.

Theorem 7.2.1

The coefficient of x^k in the characteristic polynomial of a $n \times n$ matrix A is $(-1)^{n-k}$ multiplied to the sum of determinants of all the $(n - k) \times (n - k)$ *central* submatrices.

7.2.2 Relating Characteristic Polynomials



Suppose that we have a matrix

$$B = \begin{pmatrix} 1 & 2 \\ 1 & 3 \\ 1 & 4 \end{pmatrix}$$

and that we compute

$$B^T B = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 3 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 9 \\ 9 & 29 \end{pmatrix}$$

and

$$BB^T = \begin{pmatrix} 1 & 2 \\ 1 & 3 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 7 & 9 \\ 7 & 10 & 13 \\ 9 & 13 & 17 \end{pmatrix}$$

You can check that the characteristic polynomial of $B^T B$ is $x^2 - 32x + 6$ and that the characteristic polynomial of BB^T is $x^3 - 32x + 6x$. *Wait!* They have the same ordered list of nonzero coefficients! The number 6 is the determinant of $B^T B$ and it is also the sum of determinants of 2×2 central submatrices of $B^T B$. This idea actually has some neat consequences and applications. But before we get there, let's see why such an idea is true generally. One important idea that we will use is something called:

Similarity

We say that two $n \times n$ matrices A and B are similar, denoted as $A \sim B$ if and only if there is an invertible $n \times n$ matrix C so that $A = CBC^{-1}$.

It should be clear that $A \sim B$ implies $B \sim A$ and vice versa so that the idea is symmetric. Now, here is an important result about the characteristic polynomials of two matrices which are similar:

Theorem 7.2.2

Suppose that A and B are two $n \times n$ matrices such that $A = CBC^{-1}$ for an invertible $n \times n$ matrix C (i.e. A and B are similar), then A and B have the same characteristic polynomial.

Proof. First, we know that CMC^{-1} and M have the same determinant for any $n \times n$ matrix M since:

$$\det(CMC^{-1}) = \underline{\det(C)} \det(M) \underline{\det(C^{-1})} = \det(M)$$

So, consider $M = x \text{id} - B$ and $CMC^{-1} = C(x \text{id} - B)C^{-1}$. These have the same determinant. Let's simplify

$$CMC^{-1} = C(x \text{ id} - B)C^{-1};$$

$$C(x \text{ id} - B)C^{-1} = \underbrace{Cx \text{ id} C^{-1}}_{xCC^{-1}} - \underbrace{CBC^{-1}}_A = x \text{ id} - CBC^{-1}$$

Wait! The determinant of M is the characteristic polynomial of B and the determinant of CMC^{-1} is the characteristic polynomial of A . Therefore, the two characteristic polynomials are the same. \square

Theorem 7.2.3

Given a $n \times k$ matrix B where $n \geq k$, then:

$$x^{n-k} \cdot (\text{Characteristic Polynomial of } B^T B) = \text{Characteristic Polynomial of } BB^T$$

Proof. Let $M = \begin{pmatrix} B & 0 \end{pmatrix}$ be an $n \times n$ matrix where B is a block and 0 refers to a block of 0's. Then, via block multiplication:

$$M^T M = \begin{pmatrix} B^T \\ 0 \end{pmatrix} \cdot \begin{pmatrix} B & 0 \end{pmatrix} = \begin{pmatrix} B^T B & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} k \times k \text{ block} & k \times (n-k) \text{ block} \\ (n-k) \times k \text{ block} & (n-k) \times (n-k) \text{ block} \end{pmatrix}$$

$$MM^T = \begin{pmatrix} B & 0 \end{pmatrix} \cdot \begin{pmatrix} B^T \\ 0 \end{pmatrix} = BB^T$$

If $n = k$, then M would be B and M^T would be B^T . We now will compare $M^T M$ and MM^T and this will lead to our desired result. First, let's put M into Smith normal form using a row operations matrix R and a column operations matrix C :

$$RMC = \begin{pmatrix} \text{id} & 0 \\ 0 & 0 \end{pmatrix}$$

where id is an identity block and the 0's are 0 blocks. *Note: If the Smith normal form of M is simply the identity matrix, the proof that follows would become easier—we would be able to ignore all of the blocks other than the top right one. One can check that the result would still hold.* Then:

$$M = R^{-1} \begin{pmatrix} \text{id} & 0 \\ 0 & 0 \end{pmatrix} C^{-1}$$

Let's also express M^T in terms of *this same* C and R . First let's multiply out $C^{-1}M^TR^{-1}$ and let's write it

according to the same block sizes as the Smith normal form matrix $\begin{pmatrix} \text{id} & 0 \\ 0 & 0 \end{pmatrix}$ we found for M . Thus we write:

$$C^{-1}M^TR^{-1} = \begin{pmatrix} D & E \\ F & G \end{pmatrix}$$

where we have given labels D , E , F , and G to the blocks. Then, we have:

$$M^T = C \begin{pmatrix} D & E \\ F & G \end{pmatrix} R.$$

This rewriting of M and M^T will allow us to compare their products M^TM and MM^T better. We have:

$$\begin{aligned} MM^T &= R^{-1} \underbrace{\begin{pmatrix} \text{id} & 0 \\ 0 & 0 \end{pmatrix}}_M C \underbrace{\begin{pmatrix} D & E \\ F & G \end{pmatrix}}_{M^T} R \\ &= R^{-1} \begin{pmatrix} D & E \\ 0 & 0 \end{pmatrix} R \end{aligned}$$

Also:

$$\begin{aligned} M^TM &= C \underbrace{\begin{pmatrix} D & E \\ F & G \end{pmatrix}}_{M^T} R \underbrace{\begin{pmatrix} \text{id} & 0 \\ 0 & 0 \end{pmatrix}}_M C^{-1} \\ &= C \begin{pmatrix} D & 0 \\ F & 0 \end{pmatrix} C^{-1}. \end{aligned}$$

Now let's compare the matrices

$$Q = \begin{pmatrix} D & 0 \\ F & 0 \end{pmatrix} \quad P = \begin{pmatrix} D & E \\ 0 & 0 \end{pmatrix}$$

One very important key observation is that *the only* central submatrices of both Q and P that have nonzero determinant are central submatrices of the block D itself. This is because all others will either have a row or a column of zeros. Thus, by our technique for computing characteristic polynomials, we know that both of these matrices *must have the same characteristic polynomial!* Yet, $Q \sim M^TM$ and $P \sim MM^T$. Therefore, M^TM and MM^T have the same characteristic polynomials. Now remember that

$$M^TM = \begin{pmatrix} B^TB & 0 \\ 0 & 0 \end{pmatrix} \quad MM^T = BB^T$$

so that:

$$\text{characteristic polynomial of } BB^T = \text{characteristic polynomial of } M^T M$$

$$= \det(x \text{id}_{k \times k} - B^T B) = \det \begin{pmatrix} x \text{id}_{k \times k} - B^T B & 0 \\ 0 & x \text{id}_{(n-k) \times (n-k)} \end{pmatrix} = x^{n-k} \cdot (\text{characteristic polynomial of } B^T B).$$

This last equality follows since the determinant of a block diagonal matrix is simply the product of the determinants of the blocks. \square

So...we have proven our above observation that the characteristic polynomials of BB^T and $B^T B$ should always coordinate! In our example earlier we had a 3×2 matrix B given by:

$$B = \begin{pmatrix} 1 & 2 \\ 1 & 3 \\ 1 & 4 \end{pmatrix}$$

So our result tells us with $n = 3$ and $k = 2$ that

$$x^1 \cdot \underbrace{(\text{Characteristic Polynomial of } B^T B)}_{x^2 - 32x + 6} = \underbrace{\text{Characteristic Polynomial of } BB^T}_{x^3 - 32x^2 + 6x}$$

which is exactly as we had calculated.

The “6” in the characteristic polynomial of $B^T B$ as the coefficient of $x^{2-2} = x^0$ is

$$(-1)^2 \cdot \det B^T B.$$

In contrast, the “6” in the characteristic polynomial of BB^T as the coefficient of $x^{3-2} = x^1$ is

$$(-1)^2 \cdot (\text{Sum of determinants of } 2 \times 2 \text{ central submatrices of } BB^T).$$

This shows us that:

$$\det(B^T B) = (\text{Sum of determinants of } 2 \times 2 \text{ central submatrices of } BB^T)$$

Indeed, generally we have:

Corollary 7.2.4

Suppose that B is a $n \times k$ matrix with $n \geq k$. Then:

$$\det(B^T B) = (\text{Sum of determinants of } k \times k \text{ central submatrices of } BB^T)$$

Proof. This follows from our last theorem that relates characteristic polynomials. The constant term of the characteristic polynomial of $B^T B$ is $(-1)^k \det(B^T B)$. The coefficient of x^{n-k} in the characteristic polynomial of BB^T is product of $(-1)^k$ and the sum of $k \times k$ central submatrices of BB^T . These two coefficients are the same. \square

Let's consider the central 2×2 submatrices of

$$BB^T = \begin{pmatrix} 5 & 7 & 9 \\ 7 & 10 & 13 \\ 9 & 13 & 17 \end{pmatrix}$$

and how they arise as a block of B multiplied to a block of B^T

$$\left(\begin{array}{ccc|c} 5 & 7 & & 9 \\ 7 & 10 & & 13 \\ 9 & 13 & & 7 \end{array} \right) \text{ comes from } \left(\begin{array}{cc|c} 1 & 2 & \\ 1 & 3 & \\ \hline 1 & 4 & \end{array} \right) \cdot \left(\begin{array}{cc|c} 1 & 1 & 1 \\ 2 & 3 & 4 \end{array} \right)$$

$$\left(\begin{array}{ccc|c} 5 & & 9 & \\ & 7 & & 13 \\ 9 & & 7 & \end{array} \right) \text{ comes from } \left(\begin{array}{cc|c} 1 & 2 & \\ & 3 & \\ \hline 1 & 4 & \end{array} \right) \cdot \left(\begin{array}{c|cc} 1 & 1 & 1 \\ 2 & & 3 \\ \hline & 1 & 4 \end{array} \right)$$

$$\begin{pmatrix} 5 & 7 & 9 \\ 7 & \boxed{10} & 13 \\ 9 & 13 & 7 \end{pmatrix} \text{ comes from } \begin{pmatrix} 1 & 2 \\ \hline 1 & 3 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$$

Notice that the corresponding blocks are just transposes of each other! That is, each 2×2 central submatrix of BB^T in our current example is a product JJ^T where J is a 2×2 submatrix of B .

In fact, this correspondence between central 2×2 submatrices JJ^T of BB^T and 2×2 submatrices J of B is a *bijective correspondence*.

This tells us that every central submatrix of BB^T can be thought of as JJ^T where J is just a submatrix of B . Now, remember that we were taking determinants of these central submatrices and adding them together to get coefficients. In particular:

$$\det(JJ^T) = \det(J) \cdot \det(J^T) = \det(J)^2$$

Wait! We saw something like this in section 6.5. If u represents the first column of B and v represents the second column, then a sum of squares of determinants of 2×2 submatrices arises when we compute:

$$\sqrt{(dy \wedge dz(u, v))^2 + (dx \wedge dz(u, v))^2 + (dx \wedge dy(u, v))^2}$$

This gives the positive *area* of the parallelogram formed with v extending off of the base of u (since we are looking for positive area, it does not matter which vantage point we take to look at the parallelogram—we just take the absolute value of the area). Remember that $dy \wedge dz(u, v)$ computes the area of the orthogonal projection of the parallelogram onto the yz -plane. This is computed via a determinant of a 2×2 submatrix:

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

That is, the term $6x$ in the characteristic polynomial of BB^T is the sum of the squares of the areas of the

projections of the parallelogram onto the different planes. It is the square of the area of the parallelogram! But this is fascinating: *we did not have to find this sum of squares!* We can just compute $\det(B^T B)$ instead:

$$\det \underbrace{\begin{pmatrix} 3 & 9 \\ 9 & 29 \end{pmatrix}}_{B^T B} = (\text{square of the area of the parallelogram})$$

That is, the parallelogram has an area of $\sqrt{6}$.

Our current example generalizes—to get the coefficient of x^{n-k} in the characteristic polynomial of BB^T , instead of looking at a sum of determinants of central submatrices of BB^T , we look at a sum of squares of determinants of submatrices of B . This coefficient is also the constant term of $B^T B$ which is just $\det(B^T B)$

Theorem 7.2.5 Cauchy-Binet Formula (Special Case)

Suppose that $k \leq n$. The sum of squares of the determinants of the $k \times k$ submatrices of a $n \times k$ matrix B is equal to $\det(B^T B)$

Corollary 7.2.6 Parallelograms in Three Dimensions

The area of a two-dimensional parallelogram formed by vectors $u, v \in \mathbb{R}^3$ can be found by taking the square root of the determinant of $B^T B$ where $B = \begin{pmatrix} u & v \end{pmatrix}$ is formed by the columns u and v .

Example 3. Let's find the positive area of the parallelogram formed between the vectors $u = (1, 3, 4)$ and $v = (3, -1, 1)$. We should get the same result if we put the vector u before v or if we put v before u since we are looking for the positive area. If we put u before v , we express it in the matrix of columns:

$$B = \begin{pmatrix} 1 & 3 \\ 3 & -1 \\ 4 & 1 \end{pmatrix}$$

Now, compute:

$$\det B^T B = \det \begin{pmatrix} 26 & 4 \\ 4 & 11 \end{pmatrix} = 270$$

Hence, the area is: $\sqrt{270} = 3\sqrt{30} \approx 16.43$. This calculation can be very fast if we realize that

$$B^T B = \begin{pmatrix} u \bullet u & u \bullet v \\ u \bullet v & v \bullet v \end{pmatrix}$$

So we just take three dot products, a quick 2×2 determinant and take a square root!

The above ideas easily generalize. Even if we were in *four* dimensions and we had two vectors u and v forming a two-dimensional parallelogram, the sum of the squares of the areal projections would still be equal to the square of the determinant of $B^T B$ where $B = \begin{pmatrix} u & v \end{pmatrix}$. Now here is the question:

Is the sum of the squares of the areal projections really equal to the square of the area if we are in higher dimensions?

Maybe we should define the notion of area in higher dimensions. If we simply defined it as the square root of the sum of squares of area projections, then there would be no question. Yet suppose that we defined area as being the determinant of:

$$\begin{pmatrix} u & v & \underbrace{\text{Two column unit vectors that are orthogonal to each other and the base}}_{\text{extra appended columns}} \end{pmatrix}$$

where the base is the parallelogram formed by u and v . This would coincide with a volume: a *four*-dimensional volume. Orthogonality off the base means we just multiply the lengths off of the base which are both 1. This is analogous to a situation in three dimensions. Suppose we have a box formed with orthogonal sides on the x , y and z axes. Suppose that on the x axis we have a length of 3, but on the other axes we have length 1. Thinking of x axis as length, y as width and z as height, the volume of this box would then be $(\text{length}) \cdot (\text{width}) \cdot (\text{height}) = 3 \cdot 1 \cdot 1$. That is, the volume of the box has the same numerical value as the length of edge on the x axis: we are just multiplying by 1's in our volume calculation.

So, if we want a nice relationship like this between high dimensional volume which we define by a determinant and between two-dimensional area, perhaps we should define area in this way. If we did, we could write our matrix whose determinant computes a four-dimensional volume which is also an area in blocks as follows:

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

where B is made from column vectors u and v and C is made of two columns which give us an orthonormal basis for $\langle u, v \rangle^\perp$ which we can obtain via Gram Schmidt. Then,

$$\det(A)^2 = \det(A^T) \cdot \det(A) = \det(A^T A) = \det \left(\begin{pmatrix} B^T \\ C^T \end{pmatrix} \cdot \begin{pmatrix} B & C \end{pmatrix} \right)$$

$$= \det \begin{pmatrix} B^T B & B^T C \\ C^T B & C^T C \end{pmatrix}$$

Since the columns of C are orthonormal, $C^T C = \text{id}_{2 \times 2}$. Since the columns of C are orthogonal to the columns of B , $C^T B$ is a zero matrix. Hence, we are taking the determinant of a block diagonal matrix which is found by multiplying the determinants of the diagonal blocks:

$$= \det \begin{pmatrix} B^T B & 0's \\ 0's & \text{id}_{2 \times 2} \end{pmatrix} = \det(B^T B) \cdot \det(\text{id}_{2 \times 2}) = \det(B^T B)$$

Yet we know that this last determinant is the sum of the squares of the areal projections. This means a couple things:

- The two potential definitions of two-dimensional area in higher dimensions coincide.
- It does not matter what orthonormal basis we choose for $\langle u, v \rangle^\perp$ to make C : *the determinant of $(B \ C)$ will always be the same.*

We have the following:

Corollary 7.2.7 Parallelograms in n Dimensions

The area of a two-dimensional parallelogram formed by vectors $u, v \in \mathbb{R}^n$ where $n \geq 2$ can be found by taking the square root of the determinant of $B^T B$ where $B = \begin{pmatrix} u & v \end{pmatrix}$ is formed by the columns u and v .

7.2.3 Studying the Orthonormal Columns

The orthonormal columns C that we appended to B in the reading above *are interesting themselves*. The determinant of the matrix $(B \ C)$ gives a volume that is numerically the same as area of the parallelogram formed by the columns of B . This determinant can be found by pairing determinants of submatrices of B with determinants of submatrices of C . This pairing is a “dot product” between two lists. One list is from B and one list is from C . Think of these lists as vectors. When the entries of these vectors are ordered correctly, the two vectors are *parallel* and the one from C is a *unit vector*. The amazing thing is that no matter how we choose the columns C according to our criteria, *this parallel unit vector idea holds!*

In section 6.2 we discussed a method for computing the determinant of a 4×4 matrix using only 2×2 submatrices. Applying that technique here, we pair signed determinants of 2×2 submatrices of B with 2×2 submatrices of C that appear kitty-corner to the one they are paired with. That is, we are taking a dot product $b \bullet c$ between a vector b whose entries are the six signed 2×2 submatrices of B and a vector c whose entries

are the corresponding determinants of kitty corner 2×2 submatrices of C . We already know that

$$b \bullet b = (\text{sum of squares of areal projections}) = (\text{square of the area of the parallelogram})$$

But we also know that

$$\underbrace{|b \bullet c|}_{\text{absolute value}} = (\text{area of parallelogram}) = \sqrt{b \bullet b} = |b|$$

First realize that $b, c \in \mathbb{R}^6$ and have nothing to do with \mathbb{R}^4 : they just represent lists of six things. This relationship that we currently have *could potentially come about if* $c = \pm \frac{1}{\sqrt{b \bullet b}} \cdot b$ which is the same as $= \frac{1}{|b|}$

saying that c is a unit vector parallel to b . That is,

$$\underbrace{|b \bullet c|}_{\text{absolute value}} = \left| b \bullet \underbrace{\pm \frac{1}{\sqrt{b \bullet b}} \cdot b}_c \right| = \left| \frac{b \bullet b}{\sqrt{b \bullet b}} \right| = \sqrt{b \bullet b} = |b|$$

If $|c| = 1$, then the
projection length of b in
the direction c is $b \bullet c$.

But how likely is this? This idea proposes that using *any* orthonormal basis of $\langle u, v \rangle^\perp$ for the columns of C would *always* yield the same vector c up to \pm . *It actually does!* Let's see an example!

Example 4. Suppose that $u = (1, 2, 0, 1)$ and $v = (0, 1, 1, 1)$. Then, we can find a basis for $\langle u, v \rangle^\perp$ by using our fast column technique for finding the basis of the kernel of

$$\begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

We first find the reduced row echelon form:

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

The last two columns are nonpivot columns and change into a basis $\{(2, -1, 1, 0), (1, -1, 0, 1)\}$ for $\langle u, v \rangle^\perp$.

Applying Gram Schmidt starting with the vector $(1, -1, 0, 1)$, we change $(2, -1, 1, 0)$ to:

$$(2, -1, 1, 0) - \frac{(2, -1, 1, 0) \bullet (1, -1, 0, 1)}{(1, -1, 0, 1) \bullet (1, -1, 0, 1)}(1, -1, 0, 1) = (2, -1, 1, 0) - (1, -1, 0, 1) = (1, 0, 1, -1)$$

Now change the vectors $(1, -1, 0, 1)$ and $(1, 0, 1, -1)$ to be unit vectors so that we have the following orthonormal basis for $\langle u, v \rangle^\perp$:

$$\left\{ \frac{1}{\sqrt{3}}(1, -1, 0, 1), \frac{1}{\sqrt{3}}(1, 0, 1, -1) \right\}$$

So

$$C = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 \\ -1 & 0 \\ 0 & 1 \\ 1 & -1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$$

So, the area of our parallelogram is equal to the absolute value of $\det(B \ C)$. The two columns of C are multiplied by $\frac{1}{\sqrt{3}}$. We can factor these out of the determinant since determinants are multilinear:

$$\text{Area} = \left| \frac{1}{\sqrt{3}} \cdot \frac{1}{\sqrt{3}} \det \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 1 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} \right| = \left| \frac{1}{3}(-9) \right| = 3$$

We can double check that

$$B^T B = \begin{pmatrix} u \bullet u & u \bullet v \\ u \bullet v & v \bullet v \end{pmatrix} = \begin{pmatrix} 6 & 3 \\ 3 & 3 \end{pmatrix}$$

The determinant of this matrix is 9 so that the area of the parallelogram is $\sqrt{9} = 3$ just as found using our new alternate method. Now to our question about the behavior of the determinants of the 2×2 submatrices of C . If we put them into a vector c as we discussed above so that the entries of c correspond to signed determinants of what is kitty-corner from b , is it true that $c = \pm \frac{1}{|b|} \cdot b$? We consider the 4×4 determinant technique using this kitty corner pairing:

+ 0 apart \Rightarrow even

$$\left(\begin{array}{cc|cc} 1 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 2 & 1 & -\frac{1}{\sqrt{3}} & 0 \\ \hline 0 & 1 & 0 & \frac{1}{\sqrt{3}} \\ 1 & 1 & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} \end{array} \right)$$

$$(1) \cdot \left(-\frac{1}{3}\right)$$

- 1 apart \Rightarrow odd

$$\left(\begin{array}{cc|cc} 1 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 2 & 1 & -\frac{1}{\sqrt{3}} & 0 \\ \hline 0 & 1 & 0 & \frac{1}{\sqrt{3}} \\ 1 & 1 & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} \end{array} \right)$$

$$(-1) \cdot \left(\frac{1}{3}\right)$$

+ 2 apart \Rightarrow even

$$\left(\begin{array}{cc|cc} 1 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 2 & 1 & -\frac{1}{\sqrt{3}} & 0 \\ \hline 0 & 1 & 0 & \frac{1}{\sqrt{3}} \\ \hline 1 & 1 & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} \end{array} \right)$$

$$(1) \cdot \left(-\frac{1}{3}\right)$$

+ 0 apart \Rightarrow even

$$\left(\begin{array}{cc|cc} 1 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 2 & 1 & -\frac{1}{\sqrt{3}} & 0 \\ \hline 0 & 1 & 0 & \frac{1}{\sqrt{3}} \\ \hline 1 & 1 & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} \end{array} \right)$$

$$(2) \cdot \left(-\frac{2}{3}\right)$$

- 1 apart \Rightarrow odd

$$\left(\begin{array}{cc|cc} 1 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 2 & 1 & -\frac{1}{\sqrt{3}} & 0 \\ \hline 0 & 1 & 0 & \frac{1}{\sqrt{3}} \\ \hline 1 & 1 & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} \end{array} \right)$$

$$(-1) \cdot \left(\frac{1}{3}\right)$$

+ 0 apart \Rightarrow even

$$\left(\begin{array}{cc|cc} 1 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 2 & 1 & -\frac{1}{\sqrt{3}} & 0 \\ \hline 0 & 1 & 0 & \frac{1}{\sqrt{3}} \\ \hline 1 & 1 & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} \end{array} \right)$$

$$(-1) \cdot \left(\frac{1}{3}\right)$$

Notice something fascinating:

$$b = (1, -1, 1, 2, -1, -1) \quad c = \left(-\frac{1}{3}, \frac{1}{3}, -\frac{1}{3}, -\frac{2}{3}, \frac{1}{3}, \frac{1}{3} \right) = -\frac{1}{3}b = -\frac{1}{|b|}b$$

just as conjectured!

How can this be? Let's think about C for a minute. We know that $C^T C = \text{id}_{2 \times 2}$ which has determinant 1. Remember that $\det(C^T C)$ is the same as the sum of the determinants of the central 2×2 submatrices of CC^T which is the same as the sum of squares of the determinants of the 2×2 submatrices of C . That is, the sum of the squares of the entries of c is 1. So, if $c = (t_1, t_2, t_3, t_4, t_5, t_6)$, then $t_1^2 + t_2^2 + t_3^2 + t_4^2 + t_5^2 + t_6^2 = 1$. That is, c is a unit vector in \mathbb{R}^6 .

Theorem 7.2.8

If C is a $n \times k$ matrix with orthonormal columns where $k \leq n$, then the list of determinants of $k \times k$ submatrices (in any order) is a unit vector.

It turns out that among the unit vectors of \mathbb{R}^6 , there is one and only one unit vector h such that $b \bullet h = |b|$. In fact, this h is the unique unit vector such that $b \bullet h$ is greater than $b \bullet w$ for any other unit vector $w \in \mathbb{R}^6$. This tells us that since $|b \bullet c| = |b|$ that $c = \pm h$.

How is this? Consider for *fixed* b :

$$(b - w) \bullet (b - w) = b \bullet b - 2b \bullet w + w \bullet w$$

$$2b \bullet w = \underbrace{b \bullet b}_{\text{fixed}} + \underbrace{w \bullet w}_{=1, w \text{ is a unit vector}} - (b - w) \bullet (b - w)$$

This equation shows that $2b \bullet w$ is maximized precisely when $(b - w) \bullet (b - w) = |b - w|^2$ is minimized—which is the same as when $|b - w|$ is minimized. In a picture, one can see that this minimization happens precisely when w is in line with b —and there is only one way to do this:



Since w is a unit vector in the same direction as b , $b \bullet w$ is the projection length of b onto its own direction—that is, $b \bullet w$ is $|b|$ (the length of b).

Theorem 7.2.9

The list of corresponding determinants of submatrices of C which are kitty-corner to the determinants of the submatrices of B form a vector which is equal to

$$\frac{1}{|b|} \cdot b$$

where b is the list of corresponding determinants of kitty-corner submatrices of B .

7.2.4 An Optional Calculus Proof

Another way to see that $w = \frac{1}{|b|}b$ uniquely maximizes $b \bullet w$ while w is a unit vector is to use calculus. *We include this proof here as an example of the use of the characteristic polynomial and of things still yet to come.* To keep things simple and yet still instructive, let's examine the question if b and w were in \mathbb{R}^3 . Let $b = (q, r, t)$ and $w = (x, y, z)$. Then, we are trying to find a maximum for the function $f(x, y, z) = (q \ r \ t) \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ subject

to the constraint that $x^2 + y^2 + z^2 = 1$ (i.e. that w is a unit vector). We can think of taking f and composing it with $g(x, y) = (x, y, z(x, y))$ where z depends on x and y according to the equation $x^2 + y^2 + z^2 = 1$. It is true that if we were to solve for z , we would have a choice of $z = \pm\sqrt{1 - x^2 - y^2}$. But at least *locally* a choice has been made. Therefore, this description is ok for the sake of derivatives *which just look up close*. We take the derivative of $f \circ g(x, y)$ and look where it is instantaneously the zero matrix $(0 \ 0)$. This would give a critical point. We do this via the *chain rule* which says that composition of functions corresponds to matrix multiplication of derivative matrices:

$$D(f \circ g) : \underbrace{\begin{pmatrix} q & r & t \end{pmatrix}}_{Df} \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ z_x & z_y \end{pmatrix}}_{Dg} = (0 \ 0)$$

where z_x is the partial derivative of z as a function of x .

Likewise, we could also think of a function $G(x, y, z) = x^2 + y^2 + z^2$ which we also want to restrict to $x^2 + y^2 + z^2 = 1$. We can do this by $G \circ g$ yet again. We know that this restriction fixes the output of G to be 1 so that we should expect $D(G \circ g) = (0 \ 0)$ as well. We have:

$$D(G \circ g) : \underbrace{\begin{pmatrix} 2x & 2y & 2z \end{pmatrix}}_{DG} \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ z_x & z_y \end{pmatrix}}_{Dg} = (0 \ 0)$$

You should be able to verify that our matrix equations can be stated as saying that we would like to find (x, y, z) so that both $DG : (2x, 2y, 2z)$ and $Df : (q, r, t)$ are orthogonal to the plane $\langle(1, 0, z_x), (0, 1, z_y)\rangle$. In other words, they need to be *in the same one-dimensional subspace* and be scalar multiples of each other. That is, (x, y, z) which is half of $DG : (2x, 2y, 2z)$ should be directly in line with the vector (q, r, t) . This exact same idea tells us that when we were working in \mathbb{R}^6 that for w to maximize or minimize $|b \bullet w|$ while being a unit vector, it is absolutely necessary for w to be lined up and parallel with b . We have forced:

$$(x, y, z) = \pm \frac{(q, r, t)}{|(q, r, t)|}$$

(Note for those with experience in multivariable calculus: this method is another perspective of Lagrange multipliers—yet it is better because here we can verify if the critical point actually gives us a maximum or a minimum!)

We go further and test to see if choosing $(x, y, z) = \frac{(q, r, t)}{|(q, r, t)|}$ (with +) actually is a maximum. This coincides in $f \circ g$ with setting $(x, y) = \frac{(q, r)}{|(q, r, t)|}$. In the multivariable Taylor series expansion of $f \circ g$ centered at $(x, y) = \frac{(q, r)}{|(q, r, t)|}$, since the first derivative is $\begin{pmatrix} 0 & 0 \end{pmatrix}$ at this point, the bilinear part locally leads the way in approximating how $f \circ g$ changes as we move away from $\frac{(q, r)}{|(q, r, t)|}$. It is true that we focused on Taylor series centered at $(0, 0)$ in section 6.4. But, if we replace $f \circ g(x, y)$ with $h(x, y) = f \circ g\left(x + \frac{q}{|(q, r, t)|}, y + \frac{r}{|(q, r, t)|}\right)$, then centering h at $(0, 0)$ gives us the same information and derivatives as we would have centering $f \circ g(x, y)$ at $(x, y) = \frac{(q, r)}{|(q, r, t)|}$.

The bilinear part of the Taylor expansion of $f \circ g$ centered at $\frac{(q, r)}{|(q, r, t)|}$ is:

$$\frac{1}{2} D_{\frac{(q, r)}{|(q, r, t)|}}^2 (f \circ g) (v, v) \quad v = (x, y) - \frac{(q, r)}{|(q, r, t)|}$$

Notice how the vector input v into the bilinear form is the difference $(x, y) - \frac{(q, r)}{|(q, r, t)|}$. *The input vector always refers to how much we have shifted from our center.* We desire:

$$\frac{1}{2} D_{\frac{(q, r)}{|(q, r, t)|}}^2 (f \circ g) (v, v) < 0$$

. This would tell us that as (x, y) moves away from $\frac{(q, r)}{|(q, r, t)|}$ that $f \circ g(x, y)$ changes negatively—that is, decreases—as long as we have moved very slightly away from $\frac{(q, r)}{|(q, r, t)|}$. Thus, we would be ensured that the result would be a maximum. This is the same idea in single variable calculus when a negative value of the second derivative confirms that a critical point yield a maximum value of the function.

Now the second derivative, being bilinear, can be represented by a plain old matrix that can be written as a two-dimensional array of numbers. In fact, it is a *symmetric* matrix. When we study symmetric matrices and

look at optimization examples in just a few sections we will see that checking to see if $D^2_{\frac{(q,r)}{|(q,r,t)|}}(f \circ g)(v, v) < 0$ is the same as applying a technique called *Descartes rule of signs* to the *characteristic polynomial* of $D^2_{\frac{(q,r)}{|(q,r,t)|}}$. We will go over this technique later. Since this second derivative is given as a 2×2 matrix, its characteristic polynomial can be written as $x^2 + a_1x + a_0$. We will see that we just need $x^2 + a_1x + a_0$ to have two negative real roots. That they are real will follow from symmetry of the matrix—we prove this in a later section! That they are negative happens from this *Descartes rule of signs* which asserts that we need $a_1 > 0$ and $a_0 > 0$. Now let our second derivative matrix be denoted as A . Then $a_1 = -\text{tr}(A)$ and $a_0 = \det(A)$. So we know what we need to check. We just need to know what A looks like.

It would help if we knew z_x and z_y . To find these as expressions in x and y , we use

$$D(G \circ g) : \underbrace{\begin{pmatrix} 2x & 2y & 2z \end{pmatrix}}_{DG} \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ z_x & z_y \end{pmatrix}}_{Dg} = \begin{pmatrix} 0 & 0 \end{pmatrix}$$

since this equation keeps (x, y) variable and holds true for any (x, y) so that $x^2 + y^2 + z^2 = 1$. We compute:

$$\underbrace{\begin{pmatrix} 2x & 2y & 2z \end{pmatrix}}_{DG} \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ z_x & z_y \end{pmatrix}}_{Dg} = \begin{pmatrix} 2x + (2z)(z_x) & 2y + (2x)(z_y) \end{pmatrix}$$

We know that this is $\begin{pmatrix} 0 & 0 \end{pmatrix}$. So, we require:

$$\begin{aligned} 2x + (2z)(z_x) &= 0 & 2y + (2x)(z_y) &= 0 \\ z_x &= -\frac{x}{z} & z_y &= -\frac{y}{z} \end{aligned}$$

where we think of z as being a function of x and y . This description of z_x and z_y is enough to get the second derivative matrix of $f \circ g$. We compute:

$$D(f \circ g) : \underbrace{\begin{pmatrix} q & r & t \end{pmatrix}}_{Df} \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ z_x & z_y \end{pmatrix}}_{Dg} = \begin{pmatrix} q + tz_x & r + tz_y \end{pmatrix} = \begin{pmatrix} q - \frac{tx}{z} & r - \frac{ty}{z} \end{pmatrix}$$

Remember that q , r , and t are constants. Notice that to take the partial derivative of $\frac{x}{z}$ with respect to x , we simply need to apply a quotient rule remembering that z is not a constant, but is a function of x and y :

$$\frac{x}{z} \rightarrow \frac{z - xz_x}{z^2} = \frac{z - x \cdot \left(-\frac{x}{z}\right)}{z^2} = \frac{-z^2 - x^2}{z^3}$$

Using ideas like this, we compute the second derivative matrix as:

$$D^2(f \circ g) : t \cdot \begin{pmatrix} \frac{-z^2-x^2}{z^3} & \frac{-xy}{z^3} \\ \frac{-xy}{z^3} & \frac{-z^2-y^2}{z^3} \end{pmatrix}$$

Now, plugging in $(x, y, z) = \frac{(q, r, t)}{|(q, r, t)|}$ to this matrix and simplifying yields:

$$A = \frac{|(q, r, t)|}{t^2} \cdot \underbrace{\begin{pmatrix} -t^2 - q^2 & -qr \\ -qr & -t^2 - r^2 \end{pmatrix}}_B$$

Since $\det(A) = \frac{|(q, r, t)|^2}{t^4} \det(B)$ (two columns have been rescaled) and $\text{tr}(A) = \frac{|(q, r, t)|}{t^2} \cdot \text{tr}(B)$, it suffices to check if $\det(B) > 0$ and $\text{tr}(B) < 0$. That would ensure that $a_1 > 0$ and $a_0 > 0$ as desired. Clearly,

$$\text{tr}(B) = -t^2 - q^2 - t^2 - r^2 < 0$$

if we assume that our vector $b = (q, r, t) \neq (0, 0, 0)$. We have

$$\det(B) = (-t^2 - q^2)(-t^2 - r^2) - q^2r^2 = t^4 + 2q^2t^2 > 0$$

again if $b \neq (0, 0, 0)$. This is just as desired. Hence, choosing $w = \frac{1}{|b|}b$ really does maximize the dot product $b \bullet w$ if w is a unit vector if we are working in \mathbb{R}^3 .

Let $w = -\frac{1}{|b|}b$. Then, w gives a minimum value for $b \bullet w = -|b|$. This is because $(-b) \bullet w = +|b|$ so that w maximizes the dot product $(-b) \bullet (w)$.

If we are working in higher dimensions, we can use similar ideas—the largest difference really is that our characteristic polynomial has more terms to check since we would be working with a $(n-1) \times (n-1)$ matrix for the second derivative.

Theorem 7.2.10

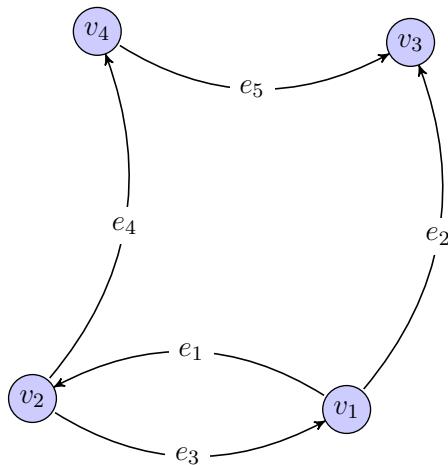
Let $b \in \mathbb{R}^n$. The vector $w = +\frac{1}{|b|}b$ gives the unique maximum and $w = -\frac{1}{|b|}b$ gives the unique minimum of $b \bullet w$ where w is a unit vector in \mathbb{R}^n .

7.2.5 Counting Spanning Trees

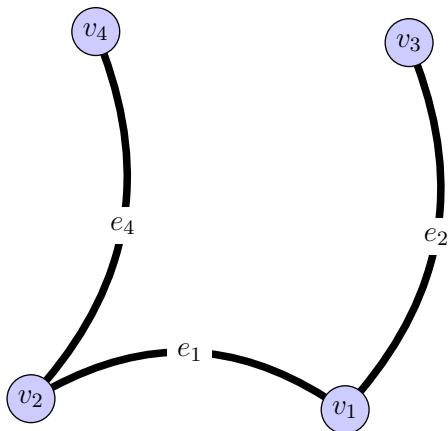
Spanning Tree

A spanning tree is a part of a digraph which is made up of all the vertices of that digraph, and a **minimal amount of edges** (*ignoring direction*) to ensure connectivity. That is, there is an edge path *ignoring direction* in the spanning tree from one vertex to any other. We get rid of as many extra edges that we can so that there still is a path. But if we were to remove any edge from the spanning tree at all, we would break the spanning tree into two pieces not connected to each other.

Example 5. Consider the following digraph:



A possible spanning tree is:



Theorem 7.2.11

The number of edges in a spanning tree of a digraph with n vertices is $n - 1$.

Proof. Each new edge needs to rope in one new vertex to ensure minimal connection. Since we start with one vertex and no edge as we build the tree, we will always have one less edge than vertex. \square

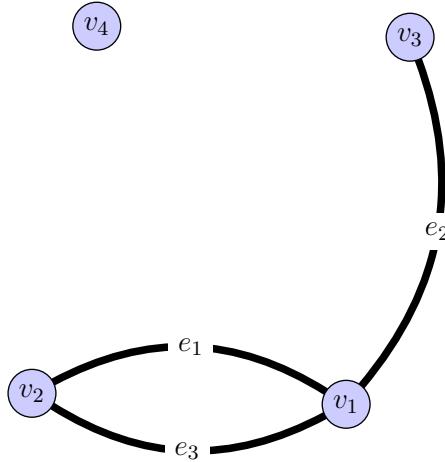
Question

How many different spanning trees are there in a digraph?

Our work in this section helps answer this question! Let's consider the incidence matrix in our above example:

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

A spanning tree consists of three edges. A spanning tree is represented by a 4×3 submatrix of A (i.e. we have chosen three columns). What has to be true about these columns? We want every vertex to be reached. As we build with our three edges we simply need that each edge visits a new vertex. So, three edges do not make up a spanning tree if and only if there is an edge whose vertices match vertices we have already seen before. Consider for instance:



A cycle was created when we reused vertices. In fact, whenever we have a cycle of edges like $e_1 + e_3$ and we apply the incidence map

$$\underbrace{y_2 - y_1}_{e_1} + \underbrace{y_1 - y_2}_{e_3},$$

we get a linear combination of the columns which equals the zero vector. Even consider the larger cycle $e_1 + e_4 + e_5 - e_2$ where we subtract the edge e_2 to reverse its direction to actually see a directed cycle. The result of the incidence map in this case is again the zero vector:

$$\underbrace{y_2 - y_1}_{e_1} + \underbrace{y_2 - y_4}_{e_4} + \underbrace{y_4 - y_3}_{e_5} + \underbrace{y_1 - y_3}_{-e_2}.$$

On the other hand, if each edge goes to a new row to put a 1 or a -1 , we are adding pivots to a reduced row echelon form—so the resulting columns are linearly independent.

Theorem 7.2.12

A collection of $n - 1$ edges in a digraph of n vertices make up a spanning tree if and only if the $n - 1$ columns corresponding to the edges in the incidence matrix are linearly independent.

Also, notice that if we remove one row of the incidence matrix, we automatically know how to fill it out from the rest of the matrix. Let's try it! The bottom three rows of the incidence matrix we are considering are:

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

Remove top row from A

We know that for any nonzero column there must be exactly one $+1$ entry and one -1 entry. Knowing this tells us that the first and second columns are missing a -1 . The third column is missing a 1 and the fourth and fifth columns are not missing anything. Putting what is missing if anything into the first row we recover that row as $(-1 \ -1 \ 1 \ 0 \ 0)$ as desired. This means we do not change linear independence or dependence of columns by removing one row of the incidence matrix. So, let's just keep that top row removed. *Note that B has more columns than rows which is contrast to earlier examples in this section where B had more rows than columns.*

Now, notice that $(-1)^3 \det(BB^T)$ is the constant coefficient of the characteristic polynomial of BB^T . But it is also the coefficient of $x^{5-3} = x^2$ in the characteristic polynomial of B^TB . This is also the product of $(-1)^3$ and the sum of the squares of the determinants of the 3×3 submatrices of B .

The 3×3 submatrices of B will either have a determinant of ± 1 or 0.

Let's explain why. If the columns are dependent and do not make up a tree, then the determinant must be 0. On the other hand, a nonzero determinant indicates linear independence—which means that the 3×3 matrix corresponds to a spanning tree! So, let's suppose that we have one of these 3×3 submatrices that correspond to a spanning tree. In order to use the fact that we are holding a spanning tree in our hands, let's go back and add in the missing row so we have a 4×3 matrix. Yet, let's move this “usually hidden row” down to the bottom. What we have now is an incidence matrix of a spanning tree where we have labeled the first vertex as last. For

instance, we could take:

$$\underbrace{\begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}}_{3 \times 3 \text{ submatrix}} \rightarrow \underbrace{\begin{pmatrix} -1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}} \rightarrow \underbrace{\begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \\ -1 & 0 & 0 \end{pmatrix}}$$

Put hidden row back to have an incidence matrix of the spanning tree.

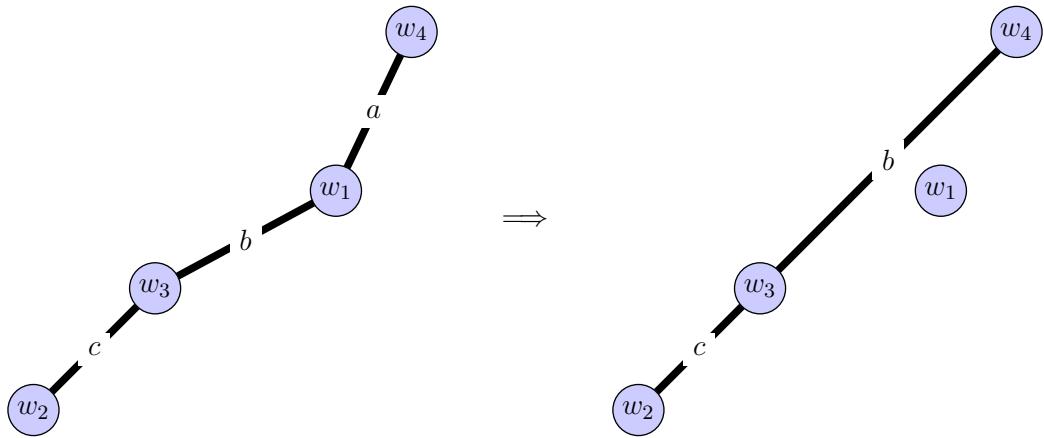
Move inserted row to the bottom to have an incidence matrix of the spanning tree with vertices reordered.

We are going to consider an inductive process through row and column operations that have visual representations of how to see that our original 3×3 matrix *must* have a determinant ± 1 generally and not just in this case. We proceed as follows to get a 1 in the upper right corner with 0's to the right and below:

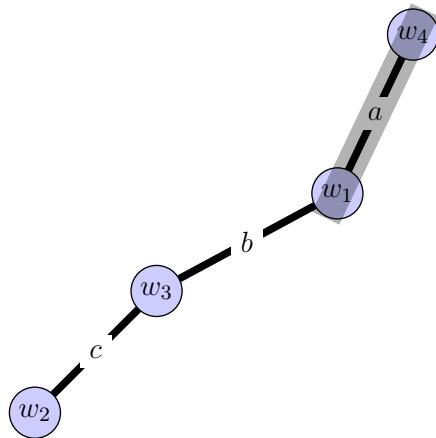
$$\begin{pmatrix} 1 & -1 & 0 \\ 0 & +1 \cdot (1) & 0 & +1 \cdot (-1) & 1 & +1 \cdot (0) \\ 0 & 1 & -1 \\ -1 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} (+1 \cdot (1)) & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

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

In our current setup, let w_1 be the vertex corresponding to the first row, let w_2 represent the vertex for the second row, etc. Visually, this is what has happened:



Any one edge connection that was coming from w_1 as now been moved to coming from w_4 . That is, it is like w_1 and w_4 and the edge between them has been thought of as a single point:



This process cannot produce a cycle. The result is a spanning tree for the three remaining vertices. We can see an incidence matrix for this spanning tree among these remaining vertices in the following submatrix:

$$\begin{array}{c} w_1 \\ w_2 \\ w_3 \\ w_4 \end{array} \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & -1 & 0 \end{array} \right)$$

Now, we repeat such a process in this submatrix since *it is again the incidence matrix of a spanning tree just as we had at the beginning*. That is, we inductively continue until our 3×4 matrix looks like:

$$\begin{array}{c} w_1 \\ w_2 \\ w_3 \\ w_4 \end{array} \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ * & * & * \end{array} \right)$$

where the $*$'s refer to the current state of the *hidden* row. *We only act on the hidden bottom row—it never airdrops upward.* All the processes we have used have only changed the determinant of the top part of our original 4×3 shown below by multiplying by ± 1 :

$$\begin{array}{c} w_1 \\ w_2 \\ w_3 \\ w_4 \end{array} \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & -1 & 0 \end{array} \right)$$

Hence,

$$\det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} = \pm \det(\text{id}_{3 \times 3}) = \pm 1$$

This is the determinant of our 3×3 submatrix of B that referred to a spanning tree. In a similar way, each spanning tree corresponds bijectively to a 3×3 submatrix of B with determinant ± 1 .

Therefore, the sum of squares of determinants of 3×3 submatrices of B counts how many choices of 3 columns have a nonzero determinant since we are just adding a 1 each time. That is, *we have counted the number of spanning trees!* Yet, instead of adding the sum of squares of determinants, let's just take the determinant of BB^T to find how many spanning trees there are!

$$\det(BB^T) = \begin{pmatrix} 1 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} = 7$$

Therefore, there are exactly seven spanning trees for our digraph. **Can you find them all?**

Counting Spanning Trees

To count the number of spanning trees of a digraph, remove a row from the incidence matrix to get a matrix B . Then compute $\det(BB^T)$.

7.2.6 Trace and Similarity

Recall that two square matrices A and B are similar, denoted as $A \sim B$ if A and B are just a change of basis away from each other. That is, there is some unpretending matrix U such that $A = U^{-1}BU$. We have seen in this section that:

If $A \sim B$, then the characteristic polynomial of A is the same as the characteristic polynomial of B .

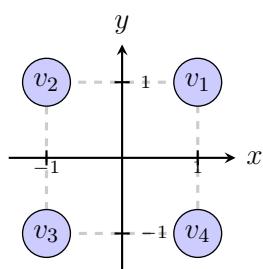
In particular, since the trace of the matrix picks out a coefficient of the characteristic polynomial:

Theorem 7.2.13

If $A \sim B$, then $\text{tr}(A) = \text{tr}(B)$

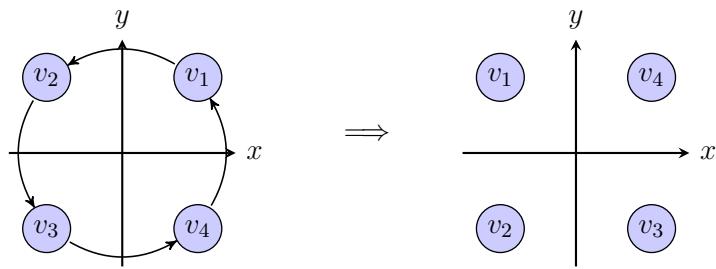
We will apply this idea to *multiplicative groups* of matrices. When we say “multiplicative group” we mean a collection of square $n \times n$ matrices G such that if $A, B \in G$, then $A \cdot B \in G$. We also mean that if $A \in G$, then $A^{-1} \in G$. In particular, this tells us that $\text{id}_{n \times n} \in G$.

We will consider a group of matrices G which helps us model the symmetries of a square



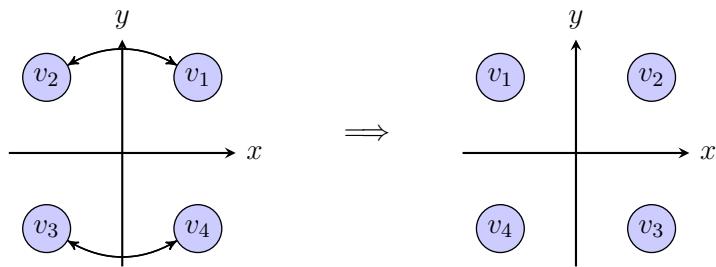
Consider the counterclockwise rotation of vertices given in a column interpretation by a matrix

$$r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$



Also consider reflecting the vertices across the y -axis given in a column interpretation by the matrix

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



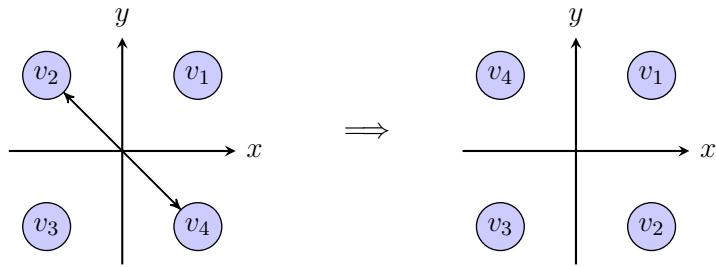
Both of these actions on the vertices of the square are called symmetries because after each one, we still see four vertices in the same places. Their labels have been rearranged however.

Symmetry of a Square

The process of rearranging the labels of the four vertices while leaving four vertices in the same places.

A symmetry of a square is a permutation—a self bijection—between the labels of the vertices. Composing two of these together can be accomplished via matrix multiplication. For instance applying the symmetry r and then s can be thought of as the matrix product $s \cdot r$ where in a column interpretation we think: “first the function r and then the function s .”

$$sr = \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}}_s \cdot \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



We get the following matrix group D_8 :

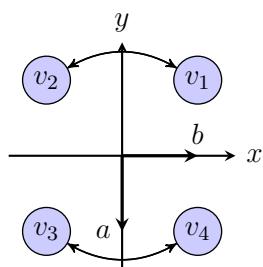
Dihedral Group of order 8

$$\text{id}_{2 \times 2} \quad r \quad r^2 \quad r^3 \quad s \quad sr \quad sr^2 \quad sr^3$$

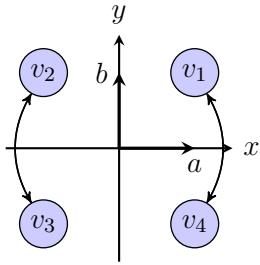
We can even form a multiplication table for this group of symmetries as follows:

.	id	s	$s \cdot r^2$	r^2	$s \cdot r$	r	r^3	$s \cdot r^3$
id	id	s	$s \cdot r^2$	r^2	$s \cdot r$	r	r^3	$s \cdot r^3$
s	s	id	r^2	$s \cdot r^2$	r	$s \cdot r$	$s \cdot r^3$	r^3
$s \cdot r^2$	$s \cdot r^2$	r^2	id	s	r^3	$s \cdot r^3$	$s \cdot r$	r
r^2	r^2	$s \cdot r^2$	s	id	$s \cdot r^3$	r^3	r	$s \cdot r$
$s \cdot r$	$s \cdot r$	r^3	r	$s \cdot r^3$	id	$s \cdot r^2$	s	r^2
r	r	$s \cdot r^3$	$s \cdot r$	r^3	s	r^2	id	$s \cdot r^2$
r^3	r^3	$s \cdot r$	$s \cdot r^3$	r	$s \cdot r^2$	id	r^2	s
$s \cdot r^3$	$s \cdot r^3$	r	r^3	$s \cdot r$	r^2	s	$s \cdot r^2$	id

Let's suppose that we would like to view the symmetry s in terms of the basis $\{a, b\}$ where $a = (0, -1)$ and $b = (1, 0)$:



So now *when we pretend* that a is pointing in the direction of e_1 and b is pointing in the direction of e_2 , we have:



This last visual is actually given by the matrix

$$sr^2 = \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}}_s \cdot \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{r^2}^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The unpretending matrix is

$$U = \begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = r^{-1} = r^3$$

When two group elements are related by an unpretending matrix which is also a group element, we say the two elements are conjugate.

Conjugate Group Elements

Two group elements A and B in a multiplicative matrix group are called *conjugate* if $A \sim B$ and the unpretending matrix U such that $A = U^{-1}BU$ is also one of the group elements.

We can check:

$$\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{U^{-1}=r} \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}}_s \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}_{U=r^3} = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_{sr^2}$$

Some symmetries look the same with just a change of perspective. The trace can help us identify when this cannot happen since if $\text{tr}(A) \neq \text{tr}(B)$, then $A \not\sim B$.

Example 6. Let's see if there is ever a change of perspective (i.e. change of basis) such that s would look like r^2 . We simply compare traces:

$$\text{tr} \left(\underbrace{\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}}_s \right) = 0 \quad \text{tr} \left(\underbrace{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}}_{r^2} \right) = -2$$

Since these are different, $s \not\sim r^2$.

Example 7. Notice that we already discovered that $sr^2 \sim s$. So we should expect their traces to be the same. We compare:

$$\text{tr} \left(\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_{sr^2} \right) = 0 \quad \text{tr} \left(\underbrace{\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}}_s \right) = 0$$

But we cannot just off of the trace alone always detect if two matrices are similar or not. But if we combine the trace with something else, we may be able to.

Multiplicative group map

A function $f : D \rightarrow C$ where D and C are multiplicative groups is called a *multiplicative group map* if $f(A \cdot B) = f(A) \cdot f(B)$. *Multiplication in the domain becomes multiplication in the codomain.*

Theorem 7.2.14

Let g be a group multiplicative map, then if $\text{tr} \circ g(A) \neq \text{tr} \circ g(B)$, we know that $A \not\sim B$.

Proof. Suppose that $A = U^{-1}BU$. Then $g(A) = g(U^{-1})g(B)g(U)$. If $g(U^{-1})$ happened to be the inverse of $g(U)$, we could say then that $g(A) \sim g(B)$. First, realize that $g(U) = g(U \cdot \text{id}) = g(U) \cdot g(\text{id})$. Since $g(U)$ lives in a group (the codomain of g), it has an inverse so that we can multiply it on the left as follows:

$$\underbrace{g(U)^{-1} \cdot g(U)}_{\text{id}} = \underbrace{g(U)^{-1} \cdot g(U)}_{\text{id}} \cdot g(\text{id})$$

so that $g(\text{id}) = \text{id}$. Consequently,

$$\text{id} = g(\text{id}) = g(\underbrace{UU^{-1}}_{\text{id}}) = g(U) \cdot g(U^{-1})$$

which confirms that $g(U^{-1})$ really is $g(U)^{-1}$. So we have shown that if $A \sim B$, then $g(A) \sim g(B)$ which means that $\text{tr} \circ g(A) = \text{tr} \circ g(B)$. So if $\text{tr} \circ g(A) \neq \text{tr} \circ g(B)$, we could not possibly have $A \sim B$ because that would imply $\text{tr} \circ g(A) = \text{tr} \circ g(B)$ which would be a contradiction.

□

Example 8. Notice that:

$$\text{tr} \left(\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_r \right) = 0 \quad \text{tr} \left(\underbrace{\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}}_s \right) = 0$$

Yet even though their traces are the same, $s \not\sim r$. We use a multiplicative group map to see this. We let $g : D_8 \rightarrow \{\text{id}_{2 \times 2}, -\text{id}_{2 \times 2}\}$ be defined by sending everything in the subgroup $H = \{\text{id}, r, r^2, r^3\}$ to $\text{id}_{2 \times 2}$ and everything in the (coset—i.e. a multiplication shift of H by s on the left) $s \cdot H = \{s, sr, sr^2, sr^3\}$ to $-\text{id}_{2 \times 2}$. Then,

$$\text{tr}(g(r)) = \text{tr}(\text{id}_{2 \times 2}) = 2$$

$$\text{tr}(g(s)) = \text{tr}(-\text{id}_{2 \times 2}) = -2$$

Therefore, $s \not\sim r$.

The study of classes of conjugate elements in groups via taking a trace and considering multiplicative group maps is a whole field of study of mathematics called representation and character theory which has numerous applications in physics, chemistry, differential equations, coding theory, etc.

Symmetric Groups

The set S_n is the collection of permutations on $\{1, 2, \dots, n\}$. This collection is made into a group via the operation of composition \circ .

Permutation Groups as Matrices

We can represent a permutation in S_n as a matrix by applying the permutation to the columns of the identity matrix. Multiplication between two of these permutation matrices corresponds exactly to the composition of the two permutations in S_n .

Example 9. The permutation $(1\ 2)(3\ 4)$ can be represented by the matrix

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

where we have switched the first two columns and the last two columns just like the cycle notation tells us.

Example 10. The permutation $(1\ 2\ 3\ 4)$ can be represented by the matrix

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

where we have replaced the first column with the second, the second with the third, the third with the fourth and the fourth with the first just as we would think $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 1$ from the cycle notation.

Example 11. The permutation $(1\ 2)(3)(4)$ can be represented by the matrix

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

Notice that the trace is 2. This number corresponds to the number of *fixed points* of the permutation. That is, the number of elements in $\{1, 2, 3, 4\}$ that are not reassigned in the permutation—such as “3” and “4.”

Trace of a permutation matrix

The trace of a permutation matrix counts the number of fixed points of the permutation

Theorem 7.2.15

Permutation matrices that have different numbers of fixed points are not similar.

But it is not true that two permutation matrices will be similar just if they have the same number of fixed points.

Another way we can try to tell if two permutation matrices are not similar is by using the following group map.

The Sign of a Permutation

We can map our permutation matrix A to the 1×1 matrix $(+1)$ if it represents an even permutation and (-1) if it represents an odd permutation.

To take the trace of a 1×1 matrix is to simply just take the number entry in the matrix. Therefore, if g is the sign of a permutation group map, $\text{tr} \circ g(A) = +1$ if A represents an even permutation and $\text{tr} \circ g(A) = -1$ if A represents an odd permutation.

Theorem 7.2.16

Two permutation matrices are not similar if one represents an odd permutation and the other an even permutation.

Example 12. The following two permutation matrices are not similar:

$$\underbrace{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{\text{odd: } (1 \ 2)(3)(4)} \not\sim \underbrace{\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}}_{\text{even: } (1 \ 2 \ 3 \ 4)}$$

7.2.7 An Extra Group Map Example

Example 13. We build an example of a multiplicative group map whose domain is the collection of permutation matrices describing S_4 . Simply, we change the basis of the matrix and then eliminate the last row and column. The specific change of basis that we will use ensures that eliminating the last row and column will give us a multiplicative map. We want to express our permutation matrices in terms of the basis

$$e_2 - e_1$$

$$e_3 - e_2$$

$$e_4 - e_3$$

$$e_4$$

The unpretending matrix and its inverse are:

$$U = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad U^{-1} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ -1 & -1 & -1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Notice the last row of 1's in U^{-1} . This can be determined by going through the signed cofactors in the last column of U . Specifically, the last row of U^{-1} can be written in terms of determinants of submatrices of U as:

$$\left(+ \det \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \right) - \det \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} + \det \begin{pmatrix} -1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \det \begin{pmatrix} -1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \right)$$

Each of these four submatrices are the result of removing one row and the last column of U . Entries in each submatrix's diagonal *above the removed row* are -1 's. Entries in the submatrix's diagonal *below the removed row* are -1 's. The nonzero off diagonal entries *below the removed row* can be taken out by a chain airdropping action from the bottom. The nonzero off diagonal entries *above the removed row* can be taken out by a chain airdropping action from the top. What we get is that each determinant is just the product of the diagonal entries.

As we move the removed row downward, the number of -1 's in the diagonal increases by 1 so that the determinants alternate between ± 1 . The cofactor position moving downward also causes an alternating in signs which cancels the \pm alternating pattern. Hence, the whole bottom row of U^{-1} before dividing by the determinant of U is either all 1's or all -1 's. In our case, it is all -1 's because the top right corner position of the 4×4 is a negative position for computing a cofactor—there is an odd number of adjacent switches to get to the diagonal.

Think about the determinant of U which is lower triangular (0's are above the diagonal so that the *lower portion* of the matrix has the only nonzero entries). Take a cofactor expansion on the top row. Only the diagonal entry gives us something and it has a positive sign since it is on the diagonal. Continue this inductively on what is left to see that the product of the diagonal of U is the determinant of U . There are three -1 's and one $+1$. So, the determinant of U is -1 . Dividing by this determinant produces a bottom row of all $+1$'s.

This same reasoning shows that if we made a 5×5 version of U or a 6×6 version or $m \times m$ matrix for larger m , we should also expect a row of 1's. This row of 1's is key.

If you multiply a row of 1's to a permutation matrix, it is the same as adding all of the rows together of that permutation matrix. This sum of rows is just a row of 1's since every column in a permutation matrix has exactly one "1" with the rest of the entries being 0.

This tells us that the bottom row of $U^{-1}p$ where p is a permutation matrix is all 1's. Then, in the product $(U^{-1}p) \cdot U$, the bottom row is now the sum of all of the rows of U . Because of how we construct U , the bottom row is always $(0 \ 0 \ 0 \ 1)$. For instance,

$$\underbrace{\begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}}_{U^{-1}} \cdot \underbrace{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}}_{\text{permutation: } (1 \ 2)(3 \ 4)} \cdot \underbrace{\begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}}_U = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Our matrix has blocks that look like:

$$\begin{pmatrix} a & b \\ 0's & 1 \end{pmatrix}$$

Notice that when we multiply two matrices with such a block pattern we get something like:

$$\begin{pmatrix} a & b \\ 0's & 1 \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0's & 1 \end{pmatrix} = \begin{pmatrix} ac & * \\ 0's & 1 \end{pmatrix}$$

This idea is important in showing that

$$g : p \mapsto \text{submatrix of } U^{-1}pU \text{ formed by removing last row and column}$$

is a multiplicative group map. We see how with an example. Let's see what $g(p \cdot q)$ comes from eliminating the last row and column from the following calculation:

$$\begin{aligned} U^{-1} \cdot p \cdot q \cdot U &= U^{-1} \cdot p \cdot \underbrace{U \cdot U^{-1}}_{\text{id}} \cdot q \cdot U \\ &= \underbrace{\left(\begin{array}{ccc|c} -1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & -1 \\ \hline 0 & 0 & 0 & 1 \end{array} \right)}_{U^{-1} \cdot p \cdot U} \cdot \underbrace{\left(\begin{array}{ccc|c} 0 & 0 & -1 & -1 \\ 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & -1 \\ \hline 0 & 0 & 0 & 1 \end{array} \right)}_{U^{-1} \cdot q \cdot U} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 1 & 0 & -1 & -1 \\ 1 & -1 & 0 & -1 \\ \hline 0 & 0 & 0 & 1 \end{array} \right) \end{aligned}$$

We can rewrite this as:

$$= \underbrace{\left(\begin{array}{c|c} g(p) & * \\ \hline 0's & 1 \end{array} \right)}_{U^{-1} \cdot p \cdot U} \cdot \underbrace{\left(\begin{array}{c|c} g(q) & \diamond \\ \hline 0's & 1 \end{array} \right)}_{U^{-1} \cdot q \cdot U} = \left(\begin{array}{c|c} g(p) \cdot g(q) & * \\ \hline 0's & 1 \end{array} \right)$$

So when we eliminate the last row and column we have $g(p) \cdot g(q)$. The process we went through was for finding $g(p \cdot q)$. Therefore,

$$g(p \cdot q) = g(p) \cdot g(q)$$

The reader is invited to see that $\text{tr} \circ g$ does not give any better way to tell if two permutation matrices A and B are not similar than just taking tr . *But we had a little practice thinking about changing bases, matrix block multiplication, cofactors and determinants—and even had a good example of a group map!*

7.2.8 Conjugacy and Similarity

Suppose that both A is a permutation matrix which can be expressed in cycle notation as $a = (1\ 2)(3\ 4\ 5)$. We can write this as:

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

Let g be a permutation function on the set $\{1, 2, 3, 4, 5\}$. Suppose that we want to think about the permutation

$$b = (g(1)\ g(2))(g(3)\ g(4)\ g(5))$$

is related to a .

- First, realize that A represents the permutation b with respect to the permuted basis

$$Y = \{e_{g(1)}, e_{g(2)}, e_{g(3)}, e_{g(4)}, e_{g(5)}\}$$

- Let U be the permutation matrix for g . It is also the unpretending matrix that takes us writing a vector in terms of the basis Y to the standard basis.
- If B is the permutation matrix for b , then:

$$A = U^{-1}BU$$

since A is the rewriting of B in terms of the basis Y .

- That is,

$$B = UAU^{-1} \quad b = gag^{-1}$$

We see that $A \sim B$ via a change of basis matrix U which itself is *also a permutation matrix*. All of these matrices represent elements of the symmetric group on 5 elements S_5 . Therefore, A and B are conjugate to each other. We could also say the group elements a and b in cycle notations are conjugate to each other and write $a \sim b$.

Conjugacy between Permutations

Let a be a permutation with a *disjoint* cycle notation. Then gag^{-1} has the exact same disjoint cycle notation except every number j is replaced by $g(j)$.

Cycle-Type

The cycle-type of a permutation expressed in *disjoint* cycle notation is the list of the cycle sizes occurring with repetition as needed.

Example 14. The cycle type of $(2\ 4\ 6)(1\ 3\ 5)(7\ 8)$ is 3–3–2.

Our discussion of a and b leads to the following theorem:

Theorem 7.2.17 Cycle Types and Conjugacy

Elements of a symmetric group S_n that share the same cycle-type are conjugate to each other.

Let's stress the necessity of the cycles being disjoint in our discussion with a bad example. Suppose that we wish to find a permutation g that conjugates one permutation into another whose “*non-disjoint* cycle-types” match:

$$\begin{array}{cccccc} (1 & & 5 & & 4 & & 6) \\ \downarrow g & & \downarrow g & & \downarrow g & & \downarrow g \\ (1 & & 2 & & 3 & & 4) & & (5 & & 4) \\ & & & & & & & \downarrow g \\ & & & & & & & (1 & & 4) \end{array}$$

We see that g tries to send 5 and 4 to two different things. This is *not well-defined*. Hence, the word *disjoint* is necessary in our discussion.

Example 15. Let's rewrite the permutation $(1\ 2\ 3\ 4)(1\ 5)(3\ 4\ 2)(4\ 3\ 2\ 1)$ quickly in disjoint cycle notation. Notice that we can think:

$$\underbrace{(1\ 2\ 3\ 4)}_g \underbrace{(1\ 5)(3\ 4\ 2)}_{g^{-1}} \underbrace{(4\ 3\ 2\ 1)}$$

where $(1\ 5)(3\ 4\ 2)$ is in disjoint cycle notation. Then we simply have:

$$(g(1)\ g(5))(g(3)\ g(4)\ g(2)) = (2\ 5)(4\ 1\ 3)$$

Key Concepts from this Section

- **trace:** (page 778) The trace of a matrix A , denoted as $\text{tr}(A)$, is the sum of the entries down its diagonal from top left to bottom right.
- **central submatrix:** (page 778) This is a submatrix which is centered on the diagonal.
- **characteristic polynomial of a 2×2 matrix:** (page 782) Let A be a 2×2 matrix. Then the characteristic polynomial is $x^2 - \text{tr}(A)x + \det(A)$

- **theorem 7.2.1 :** (page 782) The coefficient of x^k in the characteristic polynomial of a $n \times n$ matrix A is $(-1)^{n-k}$ multiplied to the sum of determinants of all the $(n - k) \times (n - k)$ *central* submatrices.
- **similarity:** (page 783) We say that two $n \times n$ matrices A and B are similar, notated as $A \sim B$ if and only if there is an invertible $n \times n$ matrix C so that $A = CBC^{-1}$.
- **theorem 7.2.2 :** (page 783) Suppose that A and B are two $n \times n$ matrices such that $A = CBC^{-1}$ for an invertible $n \times n$ matrix C (i.e. A and B are similar), then A and B have the same characteristic polynomial.
- **theorem 7.2.3 :** (page 784) Given a $n \times k$ matrix B where $n \geq k$, then:

$$x^{n-k} \cdot (\text{Characteristic Polynomial of } B^T B) = \text{Characteristic Polynomial of } BB^T$$

- **corollary 7.2.4 :** (page 786) Suppose that B is a $n \times k$ matrix with $n \geq k$. Then:

$$\det(B^T B) = (\text{Sum of determinants of } k \times k \text{ central submatrices of } BB^T)$$

- **theorem 7.2.5 cauchy-binet formula (special case):** (page 789) Suppose that $k \leq n$. The sum of squares of the determinants of the $k \times k$ submatrices of a $n \times k$ matrix B is equal to $\det(B^T B)$
- **corollary 7.2.6 parallelograms in three dimensions:** (page 789) The area of a two-dimensional parallelogram formed by vectors $u, v \in \mathbb{R}^3$ can be found by taking the square root of the determinant of $B^T B$ where $B = \begin{pmatrix} u & v \end{pmatrix}$ is formed by the columns u and v .
- **corollary 7.2.7 parallelograms in n dimensions:** (page 791) The area of a two-dimensional parallelogram formed by vectors $u, v \in \mathbb{R}^n$ where $n \geq 2$ can be found by taking the square root of the determinant of $B^T B$ where $B = \begin{pmatrix} u & v \end{pmatrix}$ is formed by the columns u and v .
- **theorem 7.2.8 :** (page 795) If C is a $n \times k$ matrix with orthonormal columns where $k \leq n$, then the list of determinants of $k \times k$ submatrices (in any order) is a unit vector.
- **theorem 7.2.9 :** (page 795) The list of corresponding determinants of submatrices of C which are kitty-corner to the determinants of the submatrices of B form a vector which is equal to

$$\frac{1}{|b|} \cdot b$$

where b is the list of corresponding determinants of kitty-corner submatrices of B .

- **theorem 7.2.10 :** (page 799) Let $b \in \mathbb{R}^n$. The vector $w = +\frac{1}{|b|}b$ gives the unique maximum and $w = -\frac{1}{|b|}b$ gives the unique minimum of $b \bullet w$ where w is a unit vector in \mathbb{R}^n .

- **spanning tree:** (page 800) A spanning tree is a part of a digraph which is made up of all the vertices of that digraph, and a **minimal amount of edges** (*ignoring direction*) to ensure connectivity. That is, there is an edge path ***ignoring direction*** in the spanning tree from one vertex to any other. We get rid of as many extra edges that we can so that there still is a path. But if we were to remove any edge from the spanning tree at all, we would break the spanning tree into two pieces not connected to each other.
- **theorem 7.2.11 :** (page 800) The number of edges in a spanning tree of a digraph with n vertices is $n - 1$.
- **theorem 7.2.12 :** (page 802) A collection of $n - 1$ edges in a digraph of n vertices make up a spanning tree if and only if the $n - 1$ columns corresponding to the edges in the incidence matrix are linearly independent.
- **counting spanning trees:** (page 806) To count the number of spanning trees of a digraph, remove a row from the incidence matrix to get a matrix B . Then compute $\det(BB^T)$.
- **theorem 7.2.13 :** (page 806) If $A \sim B$, then $\text{tr}(A) = \text{tr}(B)$
- **symmetry of a square:** (page 807) The process of rearranging the labels of the four vertices while leaving four vertices in the same places.
- **D_8 :** (page 808) This is notation for the dihedral group of order 8.
- **dihedral group of order 8:** (page 808)

$$\begin{array}{ccccccc} \text{id}_{2 \times 2} & r & r^2 & r^3 & s & sr & sr^2 & sr^3 \end{array}$$

- **conjugate group elements:** (page 809) Two group elements A and B in a multiplicative matrix group are called *conjugate* if $A \sim B$ and the unpretending matrix U such that $A = U^{-1}BU$ is also one of the group elements.
- **multiplicative group map:** (page 810) A function $f : D \rightarrow C$ where D and C are multiplicative groups is called a *multiplicative group map* if $f(A \cdot B) = f(A) \cdot f(B)$. *Multiplication in the domain becomes multiplication in the codomain.*
- **theorem 7.2.14 :** (page 810) Let g be a group multiplicative map, then if $\text{tr} \circ g(A) \neq \text{tr} \circ g(B)$, we know that $A \not\sim B$.
- **symmetric groups:** (page 811) The set S_n is the collection of permutations on $\{1, 2, \dots, n\}$. This collection is made into a group via the operation of composition \circ .
- **permutation groups as matrices:** (page 811) We can represent a permutation in S_n as a matrix by applying the permutation to the columns of the identity matrix. Multiplication between two of these permutation matrices corresponds exactly to the composition of the two permutations in S_n .

- **fixed points:** (page 812) the number of elements in the domain of the permutation that are not reassigned in the permutation
- **trace of a permutation matrix:** (page 812) The trace of a permutation matrix counts the number of fixed points of the permutation
- **theorem 7.2.15 :** (page 812) Permutation matrices that have different numbers of fixed points are not similar.
- **the sign of a permutation:** (page 813) We can map our permutation matrix A to the 1×1 matrix $(+1)$ if it represents an even permutation and (-1) if it represents an odd permutation.
- **theorem 7.2.16 :** (page 813) Two permutation matrices are not similar if one represents an odd permutation and the other an even permutation.
- **conjugacy between permutations:** (page 816) Let a be a permutation with a *disjoint* cycle notation. Then gag^{-1} has the exact same disjoint cycle notation except every number j is replaced by $g(j)$.
- **cycle-type:** (page 816) The cycle-type of a permutation expressed in *disjoint* cycle notation is the list of the cycle sizes occurring with repetition as needed.
- **theorem 7.2.17 cycle types and conjugacy:** (page 817) Elements of a symmetric group S_n that share the same cycle-type are conjugate to each other.

7.2.9 Exercises

Finding the Characteristic Polynomial

Find the characteristic polynomial in each of the following...

(a) by using central submatrices.

(b) by cofactor expansion.

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

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

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

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

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

$$6. \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

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

$$8. \begin{pmatrix} 2 & 0 & 0 \\ -1 & 2 & -1 \\ 0 & 1 & -1 \end{pmatrix}$$

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

$$10. \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & 2 \end{pmatrix}$$

$$11. \begin{pmatrix} 0 & -1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$12. \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix}$$

$$13. \begin{pmatrix} -1 & -1 & 2 \\ 0 & 2 & 2 \\ -1 & 0 & 2 \end{pmatrix}$$

$$14. \begin{pmatrix} -1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & -1 & 0 & -1 \end{pmatrix}$$

$$15. \begin{pmatrix} 1 & 2 & 2 \\ 0 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix}$$

$$16. \begin{pmatrix} 2 & 0 & 0 & 1 \\ -1 & 0 & -1 & 1 \\ 2 & 2 & -1 & 2 \\ 2 & 2 & 0 & 0 \end{pmatrix}$$

$$17. \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$$

$$18. \begin{pmatrix} 0 & -1 & 1 & 2 \\ 1 & 1 & 1 & 0 \\ 0 & -1 & 1 & -1 \\ 2 & 0 & 0 & -1 \end{pmatrix}$$

$$19. \begin{pmatrix} 1 & 2 & 1 \\ -1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$20. \begin{pmatrix} 0 & 1 & 2 \\ -1 & 1 & 1 \\ 0 & 2 & 0 \end{pmatrix}$$

Counting Spanning Trees

The following are incidence matrices of digraphs. Determine the number of spanning trees of the digraph using the technique in this section.

$$21. \begin{pmatrix} 1 & 0 & 1 & 0 \\ -1 & -1 & 0 & 1 \\ 0 & 1 & -1 & -1 \end{pmatrix}$$

$$22. \begin{pmatrix} -1 & 1 & 1 & 0 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

$$23. \begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & -1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$24. \begin{pmatrix} -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

25.
$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 1 \\ 0 & 0 & 1 & -1 & -1 \end{pmatrix}$$

26.
$$\begin{pmatrix} -1 & -1 & 1 & 0 & 1 \\ 1 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 1 & -1 \end{pmatrix}$$

27.
$$\begin{pmatrix} -1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix}$$

28.
$$\begin{pmatrix} -1 & 1 & 0 & 1 & 0 \\ 1 & -1 & -1 & 0 & 1 \\ 0 & 0 & 1 & -1 & -1 \end{pmatrix}$$

29.
$$\begin{pmatrix} -1 & 0 & 1 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}$$

30.
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ -1 & -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & -1 & -1 \end{pmatrix}$$

31.
$$\begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

32.
$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ -1 & 1 & 0 & 0 & 1 \\ 0 & -1 & -1 & 0 & 0 \\ 1 & 0 & 1 & -1 & -1 \end{pmatrix}$$

33.
$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 1 \\ 1 & 0 & 1 & -1 & -1 \end{pmatrix}$$

34.
$$\begin{pmatrix} -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 1 & 1 & -1 \end{pmatrix}$$

35.
$$\begin{pmatrix} -1 & -1 & 1 & 0 \\ 1 & 0 & -1 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

36.
$$\begin{pmatrix} -1 & 0 & 0 & 0 & 1 \\ 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 1 & -1 \end{pmatrix}$$

Areas of parallelograms

Given the following vectors that form a two-dimensional parallelogram in an ambient vector space of higher dimension, compute the area of the parallelogram.

$$\mathbf{37.} (-1, -1, 0, 0, -1)$$

$$(0, 0, 0, 1, 1)$$

$$\mathbf{38.} (1, 1, 1, 0)$$

$$(2, 0, -1, -1)$$

$$\mathbf{39.} (2, 0, -1, -1, 0)$$

$$(0, 2, 2, 0, 0)$$

$$\mathbf{40.} (0, 2, 0, 1)$$

$$(0, 0, 0, 2)$$

$$\mathbf{41.} (0, 0, -1, 1)$$

$$(2, 0, 2, 1)$$

$$\mathbf{42.} (2, 0, 0, -1, -1, 1)$$

$$(0, 2, 0, 1, 0, 0)$$

$$\mathbf{43.} (1, -1, 2, 2)$$

$$(0, 0, 0, 0)$$

$$\mathbf{44.} (-1, -1, 1, -1, 0)$$

$$(0, 1, 0, 2, 0)$$

$$\mathbf{45.} (1, 2, 0, 0, -1, 1)$$

$$(1, 0, 2, 0, 0, 2)$$

$$\mathbf{46.} (-1, 2, 0)$$

$$(0, 1, 0)$$

$$\mathbf{47.} (1, 0, 1)$$

$$(1, 0, -1)$$

$$\mathbf{48.} (0, 1, -1, 0)$$

$$(1, -1, 1, 2)$$

$$\mathbf{49.} (1, 0, 0, 2, -1)$$

$$(0, 2, 2, 0, 0)$$

$$\mathbf{50.} (0, 0, 0, 1, -1)$$

$$(0, 0, 2, 0, 0)$$

$$\mathbf{51.} (2, 1, -1, 1, -1, 0)$$

$$(-1, 1, 1, 1, 2, 1)$$

$$\mathbf{52.} (-1, 0, -1, -1, 2)$$

$$(2, 2, 1, 0, 2)$$

7.2.10 Solutions

1. $x^3 - x^2 - 5x + 3$

2. $x^2 - 2x$

3. $x^3 - 3x$

4. $x^3 - 4x^2 + 4x$

5. $x^3 - 2x^2 - x + 2$

6. $x^2 - x$

7. $x^3 - 3x^2 - x + 6$

8. $x^3 - 3x^2 + x + 2$

9. $x^3 - 2x^2 + 4x - 2$

10. $x^3 - 2x^2 - 2x$

11. $x^3 + x$

12. $x^2 - 2x$

13. $x^3 - 3x^2 + 2x - 2$

14. $x^4 + 2x^3 - 3x^2$

15. $x^3 - x^2 - 4x + 4$

16. $x^4 - x^3 - 4x^2 + 2x - 2$

17. $x^3 - 2x^2 + 2$

18. $x^4 - x^3 - 3x^2 + 13x - 12$

19. $x^3 - x^2 + 2x$

20. $x^3 - x^2 - x + 4$

21. 5

22. 6

23. 2

24. 2

25. 5

26. 8

27. 2**28.** 8**29.** 2**30.** 8**31.** 4**32.** 5**33.** 5**34.** 5**35.** 5**36.** 8**37.** 5**38.** 17**39.** 44**40.** 16**41.** 17**42.** 34**43.** 0**44.** 11**45.** 54**46.** 1**47.** 4**48.** 10**49.** 48**50.** 8**51.** 63**52.** 90

The Minimal Polynomial

7.3

7.3.1 Proof That The Minimal Polynomial Exists	828
7.3.2 Finding a Diagonal Polynomial Matrix	831
7.3.3 Polynomial Spans	834
7.3.4 Invariant Subspaces	840
7.3.5 The Minimal Polynomial from Row and Column Operations	844
7.3.6 Comparing the Minimal and Characteristic Polynomials	848
7.3.7 Just Using Column Operations	849
7.3.8 Invariant Subspaces Along the Way	850
7.3.9 Computing the Minimal Polynomial via Trial and Error	851
7.3.10 When the Characteristic and Minimal Polynomials are the Same	853
7.3.11 Technology Exploration	855
7.3.12 Nilpotents, Zero Divisors, and Idempotents	855
7.3.13 Exercises	862
7.3.14 Solutions	867

Questions to Guide Your Study:

- *What is the minimal polynomial of a matrix?*
- *How can we use row and column operations on a polynomial matrix to turn it into a diagonal matrix?*
- *How do you express the polynomial span of a vector without any polynomials?*
- *What is an invariant subspace?*
- *What is an eigenvalue and an eigenvector?*
- *When should you stop the diagonalization process to quickly determine what the minimal polynomial is?*
- *How can you use the characteristic polynomial and trial and error to find the minimal polynomial?*

We have seen so far that the characteristic polynomial of a matrix is a zero scalar.

But there may be a polynomial scalar that has even smaller degree that is also a zero scalar.

Minimal Polynomial

A polynomial in the variable x of smallest positive degree whose leading coefficient is 1 and that is a zero scalar is called a *minimal polynomial* of a square matrix whose action is represented by the scalar x .

Understanding the workings of the minimal polynomial can help us *find a new basis such that if we rewrite the matrix with respect to that basis, we get a diagonal matrix*. Diagonal matrices are so much easier to work with—the way they multiply together is easier. Geometrically they can even help us identify coordinates on rotated and skewed axes more easily. In differential equations, One can change a system of differential equations into a diagonal form which is easier to solve. In the next little subsection that follows we prove that:

Theorem 7.3.1

The minimal polynomial is a factor of every zero polynomial scalar.

This fact guarantees that there is one and only one minimal polynomial. *It is minimal not only in degree but in a factorization sense too.*

7.3.1 Proof That The Minimal Polynomial Exists

To discuss this point, let's say

x represents a square nonzero matrix and that Z is the collection of all polynomials in $\mathbb{R}[x]$ that are zero scalars.

We already know that the characteristic polynomial of A is a zero scalar so that Z is nonempty.

Next, we will show that given two elements $a(x), b(x) \in Z$, that their greatest common factor is also in Z .

Suppose that $\deg(a(x)) \geq \deg(b(x))$ Then, we apply the division process of dividing $b(x)$ into $a(x)$ and get the following:

$$a(x) = \underbrace{q_0(x)}_{\text{quotient}} b(x) + \underbrace{r_0(x)}_{\text{remainder}}$$

Notice that any polynomial that is a factor of both $b(x)$ and $r_0(x)$ must be a factor of $a(x)$ since we can factor it out of $q_0(x)b(x) + r_0(x)$. Also, any polynomial that is a factor of both $a(x)$ and $b(x)$ must be a factor of

$$r_0(x) = a(x) - q_0(x)b(x)$$

since we can factor it out of $a(x)$ and $b(x)$.

Now, if we divide $r_0(x)$ into $b(x)$, we get something like:

$$b(x) = \underbrace{q_1(x)}_{\text{quotient}} r_0(x) + \underbrace{r_1(x)}_{\text{remainder}}$$

Now notice by the same reasoning as above, anything that is a factor of both $b(x)$ and $r_0(x)$ is also a factor of $r_1(x)$. Yet anything that is a factor of $b(x)$ and $r_0(x)$, we already noted was a factor of $a(x)$. It turns out that we are making a sequence:

$$a(x), b(x), r_0(x), r_1(x), \dots$$

where the common factors of any two consecutive entries are the same as the common factors of any other two consecutive entries. We continue this list out by the following process:

$$\begin{aligned} a(x) &= q_0(x) b(x) + r_0(x) \\ b(x) &= q_1(x) r_0(x) + r_1(x) \\ r_0(x) &= q_2(x) r_1(x) + r_2(x) \\ r_1(x) &= q_3(x) r_2(x) + r_3(x) \\ &\vdots && \vdots && \vdots \\ r_{m-2}(x) &= q_m(x) r_{m-1}(x) + r_m(x) \\ r_{m-1}(x) &= q_{m+1}(x) r_m(x) + 0 \end{aligned}$$

We stop precisely when we get a 0 remainder—because we cannot not divide by it in the next step. The last two remainders $r_m(x)$ and 0 have the same common factors as the first two polynomials in the list $a(x)$ and $b(x)$. Yet, the shared factors of $r_m(x)$ and 0 are simply the factors of $r_m(x)$ itself. This tells us that $r_m(x)$ itself is the *greatest common factor* of $a(x)$ and $b(x)$.

Greatest Common Factor

A greatest common factor between two polynomials in $\mathbb{R}[x]$ is a common factor that all other common factors are factors of. If we declare that the leading coefficient of the greatest common factor must be 1, then the greatest common factor is unique.

But using the following idea, we can even get more from this list of equations.

Theorem 7.3.2

If we add two zero scalars together, we again get a zero scalar. If we multiply a zero scalar by any other polynomial, we again get a zero scalar.

If $a(x)$ and $b(x)$ are zero scalars, then by the first line, $r_0(x)$ must also be a zero scalar. Then by the second line, $r_1(x)$ must also be a zero scalar and so on. This tells us:

Theorem 7.3.3

If $a(x)$ and $b(x)$ are zero scalars, then their greatest common factor is also a zero scalar.

Euclidean Algorithm

The *Euclidean Algorithm* applied to two polynomials $a(x)$ and $b(x)$ is the process of building the sequence

$$a(x), b(x), r_0(x), r_1(x), \dots, r_m(x)$$

until we come to the greatest common factor $r_m(x)$.

Let's think about this set Z of zero scalars again. Suppose that $p(x)$ is a polynomial zero scalar of minimal degree and suppose that $g(x)$ is any other zero scalar. Then if we divide $g(x)$ by $p(x)$ we get that

$$g(x) = \underbrace{q(x)}_{\text{quotient}} p(x) - \underbrace{r(x)}_{\text{remainder}}$$

Thus,

$$r(x) = \underbrace{g(x)}_{\in Z} + \underbrace{q(x)p(x)}_{\in Z} \in Z.$$

Either this remainder $r(x)$ is 0 or its degree is less than the degree of $p(x)$. Yet we assumed that $p(x)$ had *minimal* degree. So there is only one working option: $r(x) = 0$. This tells us that $g(x) = q(x)p(x)$. In other words, $g(x)$ is a multiple of $p(x)$.

Theorem 7.3.4

All zero scalars are polynomial multiples of the minimal polynomial.

7.3.2 Finding a Diagonal Polynomial Matrix

To find the minimal polynomial for a matrix A , we need to be able to first perform row and column operations on our zero matrix $x \cdot \text{id} - A$ to turn it into a diagonal one—a lot like what we do for Smith normal form. Even just doing some of the steps in this direction may be enough. In this little subsection we see our first example of performing polynomial row and column operations to get to a diagonal one.

This is just to get our feet wet. In a couple more subsections we will make the connection with how this helps us find the minimal polynomial, and also discuss some strategies and early stopping points.

Theorem 7.3.5

Only by switching rows, columns and airdropping with polynomial multiples, we can turn a square matrix of polynomials into a diagonal matrix.

Proof. First, realize that we can represent the steps of the Euclidean algorithm by going back and forth between two entries by an airdropping mechanism:

$$\begin{array}{ccc}
 & \xrightarrow{-q_0(x)b(x)} & \\
 a(x) & & b(x) \implies
 \end{array}$$

$$\begin{array}{ccc}
 & \xrightarrow{-q_1(x)r_0(x)} & \\
 r_0(x) & & b(x) \implies
 \end{array}$$

$$\begin{array}{ccc}
 & \xrightarrow{-q_2(x)r_1(x)} & \\
 r_0(x) & & r_1(x) \implies
 \end{array}$$

$$\begin{array}{cc}
 r_2(x) & r_1(x)
 \end{array}$$

Now start with the top row and pick two entries in it. Perform this Euclidean algorithm mechanism back and forth until one of them is their greatest common factor. Now choose another entry in that row. Do the same thing between this entry and the greatest common factor entry until we find a new greatest common factor entry. Keep going through all of the entries in the row. The last greatest common factor we find will be the greatest common factor of the whole row. Now do some column switching to bring the greatest common factor

to the front of the row.

Next do this same process on the *first column* bringing the greatest common factor of that column to the top. By the end of this process, the top left entry of the whole matrix is the greatest common factor of the first row and the first column. We can now row airdrop from the first row down until all the entries below the top left one are 0's because all of these entries are multiples of the greatest common factor at the top left. Then, repeat this idea for columns. In the end, we get the following where we have one entry $r(x)$ remaining in the top row and first column:

$$\left(\begin{array}{cccc} r(x) & 0 & 0 & 0 \\ 0 & \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet & \bullet \end{array} \right)$$

Now repeat this process with the submatrix which is given by eliminating the first row and the first column which we just took care of—and repeat over and over with smaller and smaller submatrices until we arrive at a diagonal matrix. □

We at least know that a diagonal matrix is obtainable by these operations. *Finding such a diagonal matrix will help us to find minimal polynomials. We will only look at simple examples where finding the diagonal matrix does not require so many Euclidean mechanisms. We may even be able to do all of the column operations needed first!*

Example 1. Let's consider an example of this process of turning a matrix of polynomials into a diagonal one. We do row and column operations—but never once do we divide by a nonconstant polynomial—i.e. a polynomial of degree greater than 1 Take the following matrix which represents the zero function if x represents the action of the matrix A as a scalar:

$$\underbrace{\begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix}}_{x \cdot \text{id}} - \underbrace{\begin{pmatrix} 0 & 0 & -1 \\ 1 & -1 & -1 \\ 1 & 0 & -2 \end{pmatrix}}_A = \underbrace{\begin{pmatrix} x & 0 & 1 \\ -1 & x+1 & 1 \\ -1 & 0 & x+2 \end{pmatrix}}_{x \cdot \text{id} - A}$$

Column Operations:

$$\begin{array}{c}
 \left(\begin{array}{ccc} x & 0 & 1 \\ -1 & x+1 & 1 \\ -1 & 0 & x+2 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 0 & 0 & 1 \\ -x-1 & x+1 & 1 \\ -x \cdot (x+2) & 0 & x+2 \end{array} \right) \rightarrow \\
 \left(\begin{array}{ccc} 0 & 0 & 1 \\ 0 & x+1 & 1 \\ -x^2-2x-1 & 0 & x+2 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 1 & 0 & 0 \\ 1 & x+1 & 0 \\ x+2 & 0 & -x^2-2x-1 \end{array} \right)
 \end{array}$$

Now Row Operations:

$$\left(\begin{array}{ccc} 1 & 0 & 0 \\ 1 & x+1 & 0 \\ x+2 & 0 & -x^2-2x-1 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 1 & 0 & 0 \\ -(x+2) \cdot 1 & x+1 & 0 \\ 0 & 0 & -x^2-2x-1 \end{array} \right) \rightarrow$$

Extra row operation: make all diagonal entries have leading coefficient 1:

$$\left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & x+1 & 0 \\ 0 & 0 & -x^2-2x-1 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & x+1 & 0 \\ 0 & 0 & x^2+2x+1 \end{array} \right)$$

Note that we switched columns one time and here we multiply a column by (-1) . Therefore, we have multiplied $(+1) = (-1)(-1)$ to the overall determinant.

The last matrix we obtained has a special name:

Smith Normal Form over $\mathbb{R}[x]$

The Smith normal form of a matrix of polynomials is a diagonal matrix obtained only by *polynomial* airdropping, switching and perhaps dividing by *constants* so that every entry has leading coefficient 1 and so that as we move down the diagonal from top left to bottom right each entry is a factor of the next one.

How did we arrive at this Smith normal form in the last example? By row and column operations—but never once dividing by a nonconstant polynomial. *Note: only constants (degree 0 polynomials) have multiplicative inverses which can also be called polynomials. Polynomials of greater degree do not. The multiplicative inverse of a polynomial like $x + 1$ is $\frac{1}{1+x}$ which is not a polynomial.*

Do you remember that row and column operations when the matrix entries are in \mathbb{R} can be thought of as isomorphisms between vector spaces before and after the function given by the matrix? Let's expand that idea—thinking about something called $\mathbb{R}[x]$ -modules.

7.3.3 Polynomial Spans

In this little subsection we talk about what it means to have a *polynomial span* of a vector. *We will use these later in order to find nice bases with respect to which would be nice to write a matrix.*

We know what it means to have a span of a vector normally. Say we have $v = (1, 2, 3)$. Then, the span of v notated as $\langle v \rangle$ or $\mathbb{R} \cdot v$ is simply all multiples of v by real numbers. This includes things like $\pi \cdot (1, 2, 3) = (\pi, 2\pi, 3\pi)$ or $5 \cdot (1, 2, 3) = (5, 10, 15)$. These are real number multiples of v .

A polynomial span of v is all *polynomial multiples* of v . So, $x \cdot (1, 2, 3) = (x, 2x, 3x)$ or $(x^2 + 1) \cdot (1, 2, 3) = (x^2 + 1, 2x^2 + 2, 3x^3 + 3)$ would be included. But we are not interested in what this span looks like as vectors with polynomial entries. No—we would like a simple way of describing what this span looks like in terms of just regular vectors in \mathbb{R}^3 without any polynomials at all.

Let's review an idea. What is a module? It is essentially the same as a vector space except the scalars themselves might not have multiplicative inverses. If we are dealing with 3-tuples of polynomials, we are dealing with a $\mathbb{R}[x]$ -module: $\mathbb{R}[x]^3$. That is, the scalars come from polynomials ($\mathbb{R}[x]$). Remember that reciprocals (i.e. multiplicative inverses) of nonzero polynomials are not always polynomials. That is, the multiplicative inverses of scalars often are not scalars—this is why we say $\mathbb{R}[x]^3$ is a $\mathbb{R}[x]$ -module *instead* of a “ $\mathbb{R}[x]^3$ -vector space.”

On the other hand, the *vector space* \mathbb{R}^3 with scalars in \mathbb{R} is itself a \mathbb{R} -module. Since the nonzero scalars in \mathbb{R} have reciprocals again in \mathbb{R} , \mathbb{R}^3 is not just a \mathbb{R} -module, it is a vector space.

In the last subsection, we were performing certain types of row and column operations. These are not vector space isomorphisms—because they do not happen between vector spaces. Rather, they are:

$\mathbb{R}[x]$ -module isomorphisms

A $\mathbb{R}[x]$ -module isomorphism f is a bijective map (i.e. a bijective function) between two $\mathbb{R}[x]$ -modules such that:

- It preserves addition: $f(v + w) = f(v) + f(w)$.
- It preserves scalar multiplication from $\mathbb{R}[x]$. That is, polynomials can pass from domain to codomain *No guarantee for polynomial reciprocals (i.e. multiplicative inverses)*:

$$f(p(x) \cdot v) = p(x) \cdot f(v).$$

They preserve the $\mathbb{R}[x]$ -module structure.

So we know that row and column operations on a matrix of polynomials done in the way we have discussed can be thought of as $\mathbb{R}[x]$ -module isomorphisms. This will help us to pass zero scalar polynomials back from the diagonal matrix that we find to be in league with our matrix $x \cdot \text{id} - A$ which we already know acts like zero. *This will help us find our minimal polynomial!*

Before we proceed further, we need to think more about $\mathbb{R}[x]^3$. We had a theorem in the last section that said when we make x represent the action of a square matrix on the vector space \mathbb{R}^3 , then $\mathbb{R}[x]^3$ naturally collapses to \mathbb{R}^3 . How it collapses can be useful—especially when we think of something called the $\mathbb{R}[x]$ -span of a vector or a collection of vectors.

$\mathbb{R}[x]$ -span of a vector

Suppose that x represents a square matrix action on \mathbb{R}^n . Then the $\mathbb{R}[x]$ -span of a vector v is the set $\mathbb{R}[x] \cdot v$. That is, it is all polynomial scalar multiples of v —like $(x^3 + 2x) \cdot v$ or $(x^5 - 2x^4 + 2) \cdot v$. Another way of thinking of this span is as the following \mathbb{R} span:

$$\langle 1, x \cdot v, x^2 \cdot v, x^3 \cdot v, \dots \rangle$$

going through all powers of x .

All polynomial spans come about in such a way.

Example 2. Suppose that

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

Then take $v = (1, 2)$. We compute:

$$\underbrace{1, 2}_v \quad \underbrace{(-1, 0)}_{x \cdot v} \quad \underbrace{(-1, 0)}_{x^2 \cdot v} \quad \underbrace{(-1, 0)}_{x^3 \cdot v} \quad \dots$$

All \mathbb{R} -linear combinations of these equals the polynomial span of $(1, 2)$.

Notice that $x \cdot (-1, 0) = (-1, 0)$. This tells us that x behaves like the scalar 1 on the subspace $\langle(-1, 0)\rangle$. Remember that our overall goal is to view a nice change of basis in which to view our matrix x . Finding subspaces like $\langle(-1, 0)\rangle$ is an important step in that process.

Example 3. In the last example, x behaves like 1 on the subspace $\langle(-1, 0)\rangle$. This is like saying that $(x - 1)$ behaves like 0 *on that subspace*. In fact, $(x - 1)$ is the minimal polynomial *on just that subspace*—but not overall. For instance, let's take a vector outside that subspace like $(1, 1)$. Then,

$$(x - 1) \cdot (1, 1) = x \cdot (1, 1) - (1, 1) = (0, 1) - (1, 1) = (-1, 0) \neq (0, 0)$$

Therefore, $(x - 1)$ does not behave like a zero scalar on all of \mathbb{R}^2 . It does on a subspace. On the other hand, one can check that

$$(x - 1)^2 \cdot (1, 1) = (x - 1) \cdot \underbrace{(-1, 0)}_{(x-1) \cdot (1, 1)} = (0, 0)$$

The polynomial $(x - 1)^2$ is actually the minimal polynomial in this case. We will soon see how we can determine this.

This last example motivates the following notion.

Minimal Polynomial on a Subspace

Suppose that x is represented by a square matrix A . Let A be thought of as a function under the column interpretation and let V be a *subspace* of the domain of that function. Then the minimal polynomial on the subspace V is the smallest degree polynomial $p(x)$ in x with leading coefficient 1 such that $p(x) \cdot v = (\text{zero vector})$ for all $v \in V$.

It is also a factor of all zero polynomial scalars on that subspace.

As we think about this idea of $\mathbb{R}[x]$ -spans, this idea about minimal polynomials *on just a subspace* becomes very important.

It is especially important when that subspace is the \mathbb{R} -span of a single vector.

Suppose, as an example, that minimal polynomial *on a subspace spanned by one particular vector v* is $x^2 + 1$.

Then, *every* polynomial scalar $p(x)$ acting on v can be thought of in a *simpler way*.

For instance,

$$p(x) = \underbrace{(x^2 + 2)}_{\text{zero scalar}} \cdot (\text{quotient}) + (\text{remainder}).$$

So, $p(x)$ behaves the *same as its remainder*. The remainder has degree less than degree 2 which is the degree of $x^2 + 1$.

This means to get the $\mathbb{R}[x]$ -span of v we only need to consider polynomials up to degree 1.

Really, we just need the \mathbb{R} -span of $1 \cdot v$ and $x \cdot v$. That would be it!



Example 4. *Finding the polynomial span of a vector.* [Video](#)

Consider the matrix

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

and let x represent the action of this matrix as a scalar. Take the vector $v = (0, 1, 1)$ and consider $(x^2 + 1) \cdot v$. Think of $x^2 + 1$ as a matrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}^2 + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Notice that this matrix multiplied by the column $(0, 1, 1)$ on the right is $(0, 0, 0)$. That is, $x^2 + 1$ acts like a zero scalar on v . This means that the $\mathbb{R}[x]$ -span of v is:

$$\langle 1 \cdot v, x \cdot v \rangle$$

Notice that

$$x \cdot v = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = (0, -1, 1)$$

Hence, the $\mathbb{R}[x]$ -span of v is the subspace of \mathbb{R}^3 given as:

$$\langle \underbrace{(0, 1, 1)}_{1 \cdot v}, \underbrace{(0, -1, 1)}_{x \cdot v} \rangle$$

Example 5. *Finding the polynomial span of a vector.* Suppose that

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

If x acts like A , then $x^3 - 2x^2 - x + 2$ which has degree 3 is a zero scalar on \mathbb{R}^3 . This means that to find the $\mathbb{R}[x]$ -span of a vector $v \in \mathbb{R}^3$, we simply need to take powers of x less than x^3 : so 1, x , and x^2 for the span. Hence:

$$\mathbb{R}[x] \cdot v = \langle v, x \cdot v, x^2 \cdot v \rangle.$$

In particular, let $v = (1, 0, 0)$. Then:

$$\mathbb{R}[x] \cdot (1, 0, 0) = \langle \underbrace{(1, 0, 0)}_v, \underbrace{(0, 1, 0)}_{x \cdot v}, \underbrace{(0, 0, 1)}_{x^2 \cdot v} \rangle.$$

In this particular case, the $\mathbb{R}[x]$ -span of the vector $(1, 0, 0)$ is all of \mathbb{R}^3 .

Polynomial Span and Minimal Polynomial

Suppose that the minimal polynomial of the action of a square matrix on a vector v is given by $p(x)$ of degree n . Then, the polynomial span of v is given as:

$$1 \cdot v \quad x \cdot v \quad \dots \quad x^{n-1} \cdot v$$

Theorem 7.3.6

Suppose that the degree of the minimal polynomial of $\langle v \rangle$ is n . The following vector collection is linearly independent:

$$1 \cdot v \quad x \cdot v \quad \dots \quad x^{n-1} \cdot v$$

Proof. We proceed by contradiction. Suppose that they were dependent. This would mean that there is some linear combination

$$a_0 \cdot 1 \cdot v + a_1 \cdot x \cdot v + \dots + a_{n-1} \cdot x^{n-1} \cdot v = (\text{zero vector})$$

Let m be the maximum index such that a_m is nonzero. Then:

$$a_0 \cdot 1 \cdot v + a_1 \cdot x \cdot v + \cdots + a_m \cdot x^{m-1} \cdot v = (\text{zero vector})$$

$$\frac{a_0}{a_m} \cdot 1 \cdot v + \frac{a_1}{a_m} \cdot x \cdot v + \cdots + \frac{a_{m-1}}{a_m} \cdot x^{m-1} \cdot v = (\text{zero vector})$$

$$\underbrace{\left(x^m + \frac{a_{m-1}}{a_m} x^{m-1} + \cdots + \frac{a_1}{a_m} x + \frac{a_0}{a_m} \right) \cdot v}_{q(x)} = (\text{zero vector})$$

Yet notice that $\deg(q(x)) \leq m < n = \deg(p(x))$. This contradicts the minimality of $p(x)$. Therefore, the vectors are linearly independent. \square

Corollary 7.3.7

If $p(x)$ is the minimal polynomial on the subspace $\langle v \rangle$, then $\langle v \rangle$ has dimension $\deg(p(x))$.

Theorem 7.3.8

Let v be any vector in \mathbb{R}^n and let x be the action by any $n \times n$ matrix. Then, there is a minimal polynomial of x on the subspace $\langle v \rangle$.

Proof. If there were no minimal polynomial on $\langle v \rangle$, then there would never be any zero polynomial scalars other than 0 itself. This means that

$$a_0 \cdot 1 \cdot v + a_1 \cdot x \cdot v + \cdots + a_m \cdot x^m \cdot v \neq (\text{zero vector})$$

for any m and any choices of scalars a_0, \dots, a_n . This would mean that $\mathbb{R}[x] \cdot v$ would be infinite dimensional. Yet, multiplication by polynomial scalars send vectors in \mathbb{R}^n to \mathbb{R}^n . The output of the polynomial scalar multiplication is in \mathbb{R}^n . We have just found an infinite dimensional \mathbb{R} -vector space, namely $\mathbb{R}[x] \cdot v$ inside of \mathbb{R}^n . This is a contradiction. Hence, there must be a minimal polynomial of the action x on $\langle v \rangle$. \square

Theorem 7.3.9

If $\langle v \rangle$ has a degree 0 minimal polynomial (i.e. a constant $k \in \mathbb{R}$), then v is the zero vector.

Proof. This is an exercise for the reader! \square

7.3.4 Invariant Subspaces

As we look at polynomial spans of a vector we encounter subspaces in which polynomial actions keep us within the subspace. Such subspaces are called *invariant* with respect to the action of x .

Example 6. An invariant subspace. Suppose that

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

and let x represent the action of this matrix as a scalar as we had in a previous example. Suppose that we take the vector $w = (1, 0, 0)$. Then you can check that $(x - 1) \cdot w$ is the zero vector. The polynomial scalar $x - 1$ only has degree 1. That means that the $\mathbb{R}[x]$ -span of w is simply $\langle 1 \cdot w \rangle$.

That is, the polynomials in $\mathbb{R}[x]$ keep w in the list of multiples of w . They all act as scalars in \mathbb{R} . In fact, degree 0 polynomials (the possible remainders upon division by $(x - 1)$) are simply elements of \mathbb{R} .

This means that the action of $\mathbb{R}[x]$ on the subspace $\langle \underbrace{(1, 0, 0)}_w \rangle$ leaves the subspace alone.

In other words, the matrix A acting on the subspace $\langle \underbrace{(1, 0, 0)}_w \rangle$ (which is a line) does not move any vector out of that subspace (i.e. line). That is, $\langle \underbrace{(1, 0, 0)}_w \rangle$ is an *invariant* subspace of A : it is *invariant* under the action of A .

Invariant Subspace

Let A be a square $n \times n$ matrix with entries in \mathbb{R} that acts on \mathbb{R}^n . Let V be a subspace of \mathbb{R}^n and let the action of A be represented by the scalar x . Then, if the $\mathbb{R}[x]$ -span of all of the vectors in V is again V , we say that V is an invariant subspace of \mathbb{R}^n with respect to the action of A .

That is, A is a linear transformation that does not take vectors that are in V out of V . If V is a plane, the matrix A would “keep the plane inside the plane”—not take any points out of it and put them anywhere else.

Notice that $1 \cdot v = v$ and $1 \in \mathbb{R}[x]$. This tells us that $V \subset \mathbb{R}[x] \cdot V$. So we are saying that the action of $\mathbb{R}[x]$ on all of V will yield no more than V —but it definitely will yield at least V itself.

Theorem 7.3.10

The polynomial span of a vector *is an invariant subspace* in and of itself.

Proof. The polynomial span of a vector v can be represented as

$$\mathbb{R}[x] \cdot v = \{a(x) \cdot v : a(x) \in \mathbb{R}[x]\}$$

Then, an arbitrary element of $\mathbb{R}[x] \cdot v$ could be represented as $a(x) \cdot v$. Then, for any polynomial $q(x)$ in $\mathbb{R}[x]$, $q(x) \cdot a(x) \cdot v \in \mathbb{R}[x] \cdot v$. Therefore, $\mathbb{R}[x] \cdot v$ is an invariant subspace. \square

Example 7. *Invariant subspace.* We consider the polynomial span of $(0, 1, 1)$ that we found in [example 4](#) where x again represents action by

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

Let's call this polynomial span V . We already found that:

$$V = \langle \underbrace{(0, 1, 1)}_{1 \cdot v}, \underbrace{(0, -1, 1)}_{x \cdot v} \rangle$$

Since V is a polynomial span, *it is an invariant subspace of A .*

Example 8. *Invariant subspace.* Suppose that

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

We check that $\langle (0, 1) \rangle$ is an invariant subspace of A . Notice that $(x - 2)$ can be thought of as the matrix

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

so that $(x - 2) \cdot (0, 1) = (0, 0)$. Hence, $x - 2$ can be thought of as a zero scalar on $\langle (0, 1) \rangle$. In particular, $x \cdot (0, 1) = 2 \cdot (0, 1)$. Therefore, the $\mathbb{R}[x]$ -span of $\langle (0, 1) \rangle$ is again $\langle (0, 1) \rangle$ and is therefore an invariant subspace with respect to A .

We just saw a subspace that had a degree one minimal polynomial. *Any subspace with such a minimal polynomial is invariant with respect to the action of x .*

Theorem 7.3.11

Suppose that x represents the action of a matrix on a vector space. Let $(x - a)$ be the minimal polynomial on a subspace W . Then W is an invariant subspace with respect to the action of x .

Proof. Let $w \in W$. Then $\langle w \rangle$ has a minimal polynomial $q(x)$. The polynomial $p(x)$ is a zero scalar on all of W and so is also a zero scalar on $\langle w \rangle \subset W$. This means that $q(x)$ is a factor of $p(x)$. Since the leading coefficient of $q(x)$ is 1, then $q(x) = 1$ or $(x - a)$. If $q(x) = 1$, then w is the zero vector and of course $\mathbb{R}[x] \cdot \langle 0 \rangle \subset W$. If $q(x) = (x - a)$, then since $q(x)$ is degree 1, $\mathbb{R}[x] \cdot \langle w \rangle = \langle 1 \cdot w \rangle \subset W$. This tells us that the action of $\mathbb{R}[x]$ on any element in W , keeps us in W . \square

It is possible that more than one subspace has the same minimal polynomial with respect to the action of x . But putting all of these together actually yields a subspace again—a larger one. Such a subspace of all vectors that have the same degree one minimal polynomial $(x - a)$ will be useful for us and has a special name. But first, we prove the following:

Theorem 7.3.12

Let x denote the action of a square matrix on a vector space V . Let $p(x)$ be the minimal polynomial on the subspace $\langle v \rangle$ for some $v \in V$. Let W be the set of all vectors $w \in V$ such that the minimal polynomial on $\langle w \rangle$ is $p(x)$. Then, W is a subspace of V .

Proof. Let $u, w \in W$ and $k \in \mathbb{R}$. Then,

$$p(x) \cdot (k \cdot u + w) = \underbrace{k \cdot p(x) \cdot u}_{\text{zero vector}} + \underbrace{p(x) \cdot w}_{\text{zero vector}} = \text{zero vector}$$

This shows that W is closed under both addition and scalar multiplication by \mathbb{R} . This is enough to ensure that W is a subspace of V . \square

Eigenspace

Let x denote the action of a square matrix A on a vector space V . Let W be the \mathbb{R} -span of all vectors $w \in V$ such that the minimal polynomial on $\langle w \rangle$ is a degree one polynomial $(x - a)$. Then, W is called an *eigenspace* of A .

Eigenspaces are Invariant

Since an eigenspace has a degree 1 minimal polynomial, it automatically is an invariant subspace. That means it is closed with respect to polynomial scalars.

Eigenvector

An eigenvector is a vector in an eigenspace.

Eigenvalue

Suppose that the minimal polynomial for an eigenspace is $(x - a)$. Then a is called the eigenvalue for that eigenspace.

Theorem 7.3.13

Let x denote the action of a square matrix A on a vector space and let a be an eigenvalue for A . Then if v is in the eigenspace associated to a , the matrix action x behaves *just like* the scalar action of a :

$$x \cdot v = a \cdot v$$

Proof.

$$\text{zero vector} = (x - a) \cdot v = x \cdot v - a \cdot v \implies x \cdot v = a \cdot v.$$

□

Example 9. Consider the matrix

$$A = \begin{pmatrix} 0 & -6 \\ 1 & 5 \end{pmatrix}$$

Notice that

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

That is, A acts the same way on $(2, -1)$ as does the scalar 3. So, $(2, -1)$ is an eigenvector for A and 3 is its associated eigenvalue. The minimal polynomial of A on the subspace $\langle (2, -1) \rangle$ is $x - 3$.

In the section on diagonalizing matrices we will discuss strategies and techniques for determining the eigenspaces of a matrix. Eigenspaces are a special case of the scenery along the way to computing the minimal polynomial of a matrix

7.3.5 The Minimal Polynomial from Row and Column Operations

We now have enough ideas in hand to come up with a technique for determining the minimal polynomial of a matrix.

Let's go back to the example when we did polynomial row and column operations to make a diagonal matrix out of $x \cdot \text{id} - A$ for

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

We started with

$$\underbrace{\begin{pmatrix} x & 0 & 1 \\ -1 & x+1 & 1 \\ -1 & 0 & x+2 \end{pmatrix}}_{x \cdot \text{id} - A}$$

and the column operations took us to

$$\underbrace{(x \cdot \text{id} - A)}_{\text{Zero Function}} \cdot \underbrace{C}_{\text{Column Operations}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & x+1 & 0 \\ x+2 & 0 & -x^2 - 2x - 1 \end{pmatrix}$$

Notice that every output of $(x \cdot \text{id} - A) \cdot C$ is the zero vector. The output of the matrix $(x \cdot \text{id} - A) \cdot C$ is the span of its columns. Let's take a look at its columns which you can double check are all the zero vector:

$$\begin{pmatrix} 1 \\ 1 \\ x+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$(x+1) \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$(-x^2 - 2x - 1) \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

gcd: Greatest Common Factor

We have factored out the greatest common factors of each column individually. This can be notated as “gcd” which stands for “greatest common divisor.”

Right away, looking at the middle column, this tells us that $(x+1)$ behaves like the zero scalar on the subspace spanned by $(0, 1, 0)$. Also, looking at the last column,

$$(x^2 + 2x + 1) = -(-x^2 - 2x - 1)$$

behaves like the zero scalar on the vector $(0, 0, 1)$. In fact, when we notice that

$$(0, 0, 0) = x \cdot (0, 0, 0) = x \cdot (x^2 + 2x + 1) \cdot (0, 0, 1) = (x^2 + 2x + 1) \cdot (x \cdot (0, 0, 1)),$$

we see that $x^2 + 2x + 1$ behaves like the zero scalar on the whole subspace

$$\langle (0, 0, 1), x \cdot (0, 0, 1) \rangle.$$

We will see that these are actually the *minimal polynomials of these subspaces*. To see this, we realize first that all the row operations R represent a $\mathbb{R}[x]$ -module isomorphism and recall that

$$R \cdot (x \cdot \text{id} - A) \cdot C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+1 & 0 \\ 0 & 0 & x^2 + 2x + 1 \end{pmatrix}$$

This means that R has the following action from the output of $(x \cdot \text{id} - A) \cdot C$ to the output of $R \cdot (x \cdot \text{id} - A) \cdot C$:

$$\begin{pmatrix} 1 \\ 1 \\ x+2 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ x+1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ x+1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ -x^2 - 2x - 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 0 \\ x^2 + 2x + 1 \end{pmatrix}$$

In particular, because scalars pass in and out of this map, we must have:

$$\begin{pmatrix} 1 \\ 1 \\ x+2 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = e_1 \quad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = e_2 \quad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} = -e_3$$

This means that the row operations together in reverse (again a $\mathbb{R}[x]$ -module isomorphism) send the collection of basis vectors e_1, e_2 , and $-e_3$ to the collection $(1, 1, x+2)$, $(0, 1, 0)$, and $(0, 0, 1)$. That is, the $\mathbb{R}[x]$ -span (all linear combinations with scalars in $\mathbb{R}[x]$) of $(1, 1, x+2)$, $(0, 1, 0)$, and $(0, 0, 1)$ is all of $\mathbb{R}[x]^3$.

Do you remember that $\mathbb{R}[x]^3$ must itself collapse all of the way down to \mathbb{R}^3 when assume that x behaves like the 3×3 matrix A ? We know that

$$\mathbb{R}[x]^3 = \mathbb{R}[x] \cdot (1, 1, x+2) + \mathbb{R}[x] \cdot (0, 1, 0) + \mathbb{R}[x] \cdot (0, 0, 1)$$

since this is simply the $\mathbb{R}[x]$ -span of $(1, 1, x+2)$, $(0, 1, 0)$, and $(0, 0, 1)$.

$$\mathbb{R}[x]^3 = \underbrace{\mathbb{R}[x] \cdot (1, 1, x+2)}_{\mathbb{R}[x]\text{-span of } (1, 1, x+2)} + \underbrace{\mathbb{R}[x] \cdot (0, 1, 0)}_{\mathbb{R}[x]\text{-span of } (0, 1, 0)} + \underbrace{\mathbb{R}[x] \cdot (0, 0, 1)}_{\mathbb{R}[x]\text{-span of } (0, 0, 1)}$$

$$\begin{array}{lll} \mathbb{R}[x]\text{-span of} & \mathbb{R}[x]\text{-span of} & \mathbb{R}[x]\text{-span of} \\ (1, 1, x+2) & (0, 1, 0) & (0, 0, 1) \end{array}$$

Now declaring that x behaves like A tells us that $(1, 1, x+2)$ is the zero vector, $(x+1)$ is a zero scalar on $(0, 1, 0)$, and $x^2 + 2x + 1$ is a zero scalar on $(0, 0, 1)$:

$$\mathbb{R}^3 = \mathbb{R}[x]^3 \text{ with } x \text{ as } A = \underbrace{\mathbb{R}[x] \cdot (1, 1, x+2)}_{\text{zero vector}} + \underbrace{\mathbb{R}[x] \cdot (0, 1, 0)}_{\langle 1 \cdot (0, 1, 0) \rangle} + \underbrace{\mathbb{R}[x] \cdot (0, 0, 1)}_{\langle 1 \cdot (0, 0, 1), x \cdot (0, 0, 1) \rangle}$$

Because we have three vectors $(0, 1, 0)$, $(0, 0, 1)$, and $x \cdot (0, 0, 1) = (-1, -1, -2)$ spanning \mathbb{R}^3 they must be linearly independent and form a basis which they do. If the polynomial $(x+1)$ was not minimal on $(0, 1, 0)$ or if $(x^2 + 2x + 1)$ were not minimal on $(0, 0, 1)$, we would have gotten less than 3 vectors that span \mathbb{R}^3 by how we think of $\mathbb{R}[x]$ -spans. This would have been a contradiction. Hence, *these really are minimal on their subspaces!*

Now, how do we move from these minimal polynomials on subspaces to the minimal polynomial for the matrix A —that is minimal for A on all of \mathbb{R}^3 ? Take any vector $v \in \mathbb{R}^3$ and notice that

$$v = a \cdot (0, 1, 0) + b \cdot (0, 0, 1) + c \cdot (-1, -1, -2)$$

for some scalars $a, b, c \in \mathbb{R}$ since we are dealing with a basis. Suppose that $p(x)$ is the *least common multiple* of the polynomial scalars $(x+1)$ and $(x^2 + 2x + 1) = (x+1)^2$.

Least Common Multiple

The least common multiple between two polynomials in $\mathbb{R}[x]$ is a multiple of both polynomials that is a factor of all other common multiples. If we declare that the leading coefficient of the least common multiple must be 1, then the least common multiple is unique.

The least common multiple is the smallest polynomial that is a multiple of both of these which is $(x+1)^2$. Then,

$$(x+1)^2 \cdot v = a \cdot (x+1) \cdot \underbrace{(x+1) \cdot (0, 1, 0)}_{(0, 0, 0)} + b \cdot \underbrace{(x+1)^2 \cdot (0, 0, 1)}_{(0, 0, 0)} + c \cdot \underbrace{(x+1)^2 \cdot (-1, -1, -2)}_{(0, 0, 0)} = (0, 0, 0)$$

This is true for all of \mathbb{R}^3 . So, the minimal polynomial of A has to be a factor of $(x+1)^2$. Any smaller would not yield zero on the subspace that has minimal polynomial $(x+1)^2$. Hence, $(x+1)^2 = x^2 + 2x + 1$ is the minimal polynomial of A .

We used the full strength of C : *all of the necessary column operations to get to Smith normal form.* But is this quite necessary? Could C have been just some of the column operations? Further, just so we do not increase the degree of the determinant, let's restrict ourselves to *not rescale any columns.*

Theorem 7.3.14

On our way to getting the minimal polynomial, we can stop our column operations precisely when the degrees of the greatest common factors of each column add up to n (if we are working with an $n \times n$ matrix).

Proof. We will focus our argument in terms of our last example. But this can be easily generalized. Instead of using the row operations matrix per se, let's use another isomorphism to guarantee that our columns after stripping the greatest common factors actually span all of $\mathbb{R}[x]^3$. This is the only reason why we used the row operations matrix R .

Our column operations only involved one column switch and no rescalings so that we have multiplied the determinant (i.e. the characteristic polynomial) by (-1) . Now, dividing the columns by their greatest common factor will divide the determinant by those greatest common factors too. Yet we know that *the determinant after dividing out by greatest common factors is still a polynomial*. Then the *product* of the greatest common factors must itself be a factor of the characteristic polynomial. Since this product *has the same degree* of the characteristic polynomial, when we divide, we should get a constant. You can see that in our case the determinant is (-1) multiplied to the characteristic polynomial: $(-x^2 - 2x - 1)(x + 1)$. Yet this is also the product of the greatest common factors so that the determinant of the following matrix should be 1:

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ x+2 & 0 & 1 \end{pmatrix}$$

Using the cofactor method for finding the inverse, the only time we divide anything is when we divide by the determinant of 1 so that M^{-1} should be completely expressible with entries in $\mathbb{R}[x]$. That is, M^{-1} represents our desired $\mathbb{R}[x]$ -module isomorphism instead of R —we do not even need to think of the row operations that take us all the way to Smith normal form! In our case, in particular:

$$M^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -x-2 & 0 & 1 \end{pmatrix}$$

□

7.3.6 Comparing the Minimal and Characteristic Polynomials

Minimal Polynomial versus Characteristic polynomial

After the row and the column operations that take us to a diagonal matrix:

- The characteristic polynomial is the product of the diagonal entries.
- The minimal polynomial is the least common multiple of the diagonal entries.

It seems that the minimal polynomial and the characteristic polynomial share a lot of the same factors. To make this idea precise we make a definition.

irreducible polynomial

A polynomial is called irreducible over \mathbb{R} if its only factors in $\mathbb{R}[x]$ are constants and constant multiples of itself. One could similarly talk about being irreducible over $\mathbb{C}[x]$ if its only factors in $\mathbb{C}[x]$ are complex constant and complex constant multiples of itself.

Example 10. The polynomials $x + 1$ and $x^2 + 1$ cannot be nontrivially factored further in $\mathbb{R}[x]$. Therefore, they are irreducible over \mathbb{R} . Yet the polynomial $x^2 + 1 = (x + \underbrace{i}_{\sqrt{-1}})(x - i)$ is not irreducible over \mathbb{C} because it factors in $\mathbb{C}[x]$. We say that it is **reducible** over \mathbb{C} .

We will focus on irreducibility in $\mathbb{R}[x]$ in this text.

Irreducible polynomials are like the *prime factors* among the polynomials.

Thinking about product versus least common multiple, we have the following:

Theorem 7.3.15

The minimal polynomial and the characteristic polynomial share *the same* irreducible factors.

Example 11. The minimal polynomial that we just computed for the matrix A above was $(x + 1)^2$. The characteristic polynomial was $(x + 1)^3$. They both only have one irreducible factor and it is the same among

them: $(x + 1)$.

7.3.7 Just Using Column Operations

Finding the Minimal Polynomial—Method 1

For a $n \times n$ matrix A :

1. Perform column *airdrops* ($\mathbb{R}[x]$ -isomorphisms) on $x \cdot \text{id} - A$ until the degrees of the greatest common factors of individual columns add up to n .
2. Take the least common multiple of these.

As a rule of thumb, try to use column operations that cause a row to have only one nonzero entry. Then, after that, restrict yourself to column operations that do not use the column with that nonzero entry.



[Video](#)

Example 12. *Finding the minimal polynomial.* Let's find the minimal polynomial of the matrix

$$A = \begin{pmatrix} 2 & -1 & 2 \\ 0 & 4 & -4 \\ 0 & 1 & 0 \end{pmatrix}$$

First, we change it to:

$$x \cdot \text{id} - A = \begin{pmatrix} x - 2 & 1 & -2 \\ 0 & x - 4 & 4 \\ 0 & -1 & x \end{pmatrix}$$

$$\left(\begin{array}{ccc} x - 2 & 1 & -2 \\ 0 & x - 4 & 4 \\ 0 & -1 & x \end{array} \right) \longrightarrow \left(\begin{array}{ccc} x - 2 & 1 & x - 2 \\ 0 & x - 4 & x^2 - 4x + 4 \\ 0 & -1 & 0 \end{array} \right)$$

Notice how we cleared out the bottom row to only have one nonzero entry. Now it's time to work with the remaining columns. At this point, if we temporarily ignore the row and column that has the last row's nonzero

entry -1 , we have the submatrix:

$$\begin{pmatrix} x-2 & x-2 \\ 0 & x^2-4x+4 \end{pmatrix}.$$

Think of column operations here that would make *another row in this submatrix* have only one nonzero entry:

$$\left(\begin{array}{ccc} x-2 & 1 & x-2 \\ 0 & x-4 & x^2-4x+4 \\ 0 & -1 & 0 \end{array} \right) \rightarrow \left(\begin{array}{ccc} x-2 & 1 & 0 \\ 0 & x-4 & x^2-4x+4 \\ 0 & -1 & 0 \end{array} \right)$$

One should notice that we need to do no more steps once we factor out what is common from each column since the sum of the degrees of these column common factors is 3 (and this is a 3×3 matrix):

$$\underbrace{(x-2)}_{\text{degree 1}} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \underbrace{(1)}_{\text{degree 0}} \cdot \begin{pmatrix} 1 \\ x-4 \\ -1 \end{pmatrix} \quad \underbrace{(x^2-4x+4)}_{\text{degree 2}} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$$1 + 0 + 2 = 3$$

Now, we take the least common multiple of what we just factored out:

$$(x-2) \quad 1 \quad \underbrace{(x^2-4x+4)}_{(x-2)^2}$$

and notice that we obtain $(x-2)^2$. Therefore, $(x-2)^2$ is the minimal polynomial of the matrix A .

7.3.8 Invariant Subspaces Along the Way

Example 13. *Finding Invariant Subspaces.* Notice that in the last example that

$$\langle (1, 0, 0) \rangle$$

is a subspace of \mathbb{R}^3 whose minimal polynomial with x representing A is $x-2$. Since, $x-2$ has degree 1, then

$$\langle (1, 0, 0) \rangle = \mathbb{R}[x] \cdot (1, 0, 0).$$

This subspace is an eigenspace for the eigenvalue $x = 2$. All of the vectors in this eigenspace are eigenvectors for the eigenvalue $x = 2$. In particular, $(1, 0, 0)$ is such an eigenvector.

Now consider the vector $(0, 1, 0)$ on which $x^2 - 4x + 4 = (x - 2)^2$ acts minimally:

$$V = \mathbb{R}[x] \cdot (0, 1, 0) = \langle (0, 1, 0), \underbrace{x \cdot (0, 1, 0)}_{(-1, 4, 1)} \rangle$$

(since $(x - 2)^2$ has degree 2 we take $(0, 1, 0)$ and $x \cdot (0, 1, 0)$). The minimal polynomial on this subspace is $(x - 2)^2$. Since this polynomial does not have degree 1, we do not use the terms eigenvalue, eigenvector, or eigenspace. These words are reserved for subspaces that have minimal polynomial of degree 1.

But, realize that $(x - 2) \cdot (x - 2) \cdot V = (0, 0, 0)$. This means that $(x - 2)$ is the minimal polynomial on the subspace $(x - 2) \cdot V$ which we can find by applying $(x - 2)$ to the basis vectors of V : $(0, 1, 0)$ and $(-2, 4, 2)$:

$$(x - 2) \cdot V = \langle \underbrace{(x - 2) \cdot (0, 1, 0)}_{(-1, 2, 1)}, \underbrace{(x - 2) \cdot (-1, 4, 1)}_{(-2, 4, 2)} \rangle$$

Notice that these two vectors $(-1, 2, 1)$ and $(-2, 4, 2)$ of which we are taking a span are multiples of each other. Hence, we have:

$$(x - 2) \cdot V = \langle (-1, 2, 1) \rangle$$

Now we know that:

$$\underbrace{\langle (1, 0, 0) \rangle}_{\text{minimum polynomial } x-2} \qquad \qquad \qquad \underbrace{\langle (-1, 2, 1) \rangle}_{\text{minimum polynomial } x-2}$$

Hence, if take the subspace $H = \langle (1, 0, 0), (-1, 2, 1) \rangle$, we get a dimension 2 subspace that has minimum polynomial $(x - 2)$. In fact, H is the eigenspace for the eigenvalue $x = 2$. The eigenspace associated with $x = 2$ has dimension 2: one dimension coming from each of the column common factors $(x - 2)$ and $(x - 2)^2$ that have $(x - 2)$ as a factor. We will discuss simple techniques for determining these things soon. This example is here to be instructive as we learn how to interpret the process of finding the minimum polynomial.

7.3.9 Computing the Minimal Polynomial via Trial and Error

Since the minimal polynomial is just a factor of the characteristic polynomial, why can't we just test each factor of the characteristic polynomial?

Finding the Minimal Polynomial—Method 2

For a $n \times n$ matrix A :

1. Compute the characteristic polynomial $p(x)$.
2. List out the irreducible factors of $p(x)$ as $a_1(x), \dots, a_m(x)$.
3. List all the factors of $p(x)$ of the form $a_1(x)^{r_1}, \dots, a_m(x)^{r_m}$ where $r_1 \neq 0, r_2 \neq 0, \dots, r_m \neq 0$.
This is because *the minimal polynomial must have all of these irreducibles as factors.*
4. See which of the factors in this last list we have just created come out to the zero matrix.
5. The smallest degree factor from this list that is equivalent to the zero matrix is the minimal polynomial.



Example 14. Let's find the minimal polynomial of the matrix:

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

We perform a cofactor expansion along the last row of:

$$x \cdot \text{id} - A = \begin{pmatrix} x & -1 & 0 \\ -1 & x & 0 \\ 0 & 0 & x-1 \end{pmatrix}$$

This is nice since we can see that $(x-1)$ is a factor already. We have:

$$(x-1) \cdot \det \underbrace{\begin{pmatrix} x & -1 \\ -1 & x \end{pmatrix}}_{(x^2-1)} = (x-1)(x-1)(x+1)$$

Out of the five nontrivial factors, we choose the ones that have *both* the irreducibles $(x+1)$ and $(x-1)$ as factors:

$$\cancel{(x-1)} \quad \cancel{(x+1)} \quad (x+1)(x-1) \quad \cancel{(x-1)^2} \quad \underbrace{(x-1)^2(x+1)}_{\text{characteristic polynomial}}$$

Since we already know that the characteristic polynomial comes out to the zero matrix, it suffices to check $(x + 1)(x - 1) = x^2 - 1$.

$$\begin{aligned} x^2 - 1 &= \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{x^2}^2 - \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_1 \\ &= \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{x^2} - \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

Since the degree of this polynomial is smaller than the degree of the characteristic polynomial, it must be the *minimal polynomial*.

7.3.10 When the Characteristic and Minimal Polynomials are the Same

Let v be a vector in \mathbb{R}^n and let x represent the action of a square matrix $n \times n$ matrix A . Earlier in this section, we showed that the dimension of $\mathbb{R}[x] \cdot \langle v \rangle$ is equal to the degree of the minimal polynomial $q(x)$ of A just on the subspace $\langle v \rangle$. We know that since the characteristic polynomial $c(x)$ of A is a zero polynomial scalar on $\langle v \rangle$. Hence, $q(x)$ is a factor of $c(x)$. For the same reason, we know that $q(x)$ is a factor of the minimal polynomial $m(x)$ of A . So, what if $\dim \langle v \rangle = n$? Then

$$n = \deg q(x) \leq \deg m(x) \leq \deg c(x) = n$$

Hence, $m(x) = c(x)$.

Remember that

$$\mathbb{R}[x] \cdot \langle v \rangle = \langle 1 \cdot v, x \cdot v, x^2 \cdot v, \dots x^{m-1} \cdot v \rangle$$

where $m = \deg q(x)$.

Proving the Equivalence of the Characteristic and Minimal Polynomials

Suppose that A is a $n \times n$ matrix whose action is represented by x . Look at the powers of x :

$1, x, x^2, \dots, x^{n-1}$ as matrices. If you can find v such that the collection

$\{1 \cdot v, x \cdot v, x^2 \cdot v, \dots, x^{n-1} \cdot v\}$ is linearly independent, then this proves that the characteristic polynomial of A is the same as the minimal polynomial of A .

In practice, you could try $v = e_1$ or $v = e_2$ or $v = e_3$ or \dots . This just amounts to considering the same column in each power of x thought of as a matrix. *Remember that if you cannot seem to find such a v you have not proven anything.*

Example 15. Consider the matrix

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

We will represent the action of A by x . Considering powers of x up to 2 we have:

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{x^0} \quad \underbrace{\begin{pmatrix} 1 & 0 & -1 \\ 0 & -1 & 0 \\ 0 & 1 & 2 \end{pmatrix}}_{x} \quad \underbrace{\begin{pmatrix} 1 & -1 & -3 \\ 0 & 1 & 0 \\ 0 & 1 & 4 \end{pmatrix}}_{x^2}$$

Look at all the second columns and line them up next to each other in a matrix:

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

One can see through some swift column and row operations to Smith normal form that the rank of this matrix is 3. This tells us the the columns are linearly independent since the range under a column interpretation is the span of the columns and if the span has dimension 3, the columns must be linearly independent.

Or one could take the determinant quickly by using a cofactor expansion on the first row to notice a determinant of -1 which is nonzero. This indicates also the the columns are linearly independent.

Either way, we know that the $\mathbb{R}[x]$ span of $e_2 = (0, 1, 0)$ has dimension 3 which is all of \mathbb{R}^3 . Then the minimal polynomial on $\langle e_2 \rangle$ has degree 3. This sandwiches the actual minimal polynomial up to the characteristic polynomial which has degree 3. Therefore, the minimal polynomial is exactly the characteristic polynomial.

To find the characteristic polynomial, we use a cofactor expansion on the first column of

$$\det(x \cdot \text{id} - A) = \det \begin{pmatrix} x-1 & 0 & 1 \\ 0 & x+1 & 0 \\ 0 & -1 & x-2 \end{pmatrix} = (x-1) \cdot \det \begin{pmatrix} x+1 & 0 \\ -1 & x-2 \end{pmatrix} = (x-1)(x+1)(x-2)$$

Hence, the minimal polynomial is also $(x-1)(x+1)(x-2)$.

7.3.11 Technology Exploration

Everything that we have been doing in this section can be programmed on a computer. See the following SageMath activity for code that you can explore:



7.3.12 Nilpotents, Zero Divisors, and Idempotents

Nilpotent Matrix

A Nilpotent matrix is a square matrix whose minimal polynomial is a power of x like x^2 or x^3 .

The prefix “nil” means “zero” and the root “potent” means “power”—yet you can think of it as signifying “potential.” So we are saying that a matrix has “zero potential” as we keep multiplying it to itself.

Example 16. The matrix

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

is nilpotent. As an exercise, using a column interpretation, demonstrate how nonzero columns shift to the right until finally they are gone when we repeatedly multiply A to itself.

Exploration

Find your own examples of nilpotent matrices. Think about how to get a characteristic polynomial or minimal polynomial looking like x^n for some n .

Zero Divisor Matrix

A nonzero square matrix A is a zero divisor if there is another nonzero matrix B (also a zero divisor) such that $A \cdot B$ is the zero matrix.

We are literally saying that “zero” (i.e. the zero matrix) has nonzero factors (a.k.a. divisors).

The proof of the following theorems are left as exercises to the reader:

Theorem 7.3.16

A square matrix A is a zero divisor if the constant term of the *characteristic polynomial* is 0. (*The constant term being zero is the same as saying that x is a factor of the characteristic polynomial.*)

How does the constant term of the characteristic polynomial equalling zero also guarantee that the minimal polynomial has a constant term of 0?

If we know the *minimal polynomial* of a zero divisor matrix, how does this help us find a nonzero matrix it can be multiplied by to yield the zero matrix?

Exploration

Use this idea to find pairs of nonzero matrices that multiply together to give the zero matrix. *Hint: how does a matrix with a top row of all 0's guarantee that x is a factor of the characteristic polynomial? Think about a cofactor expansion.*

Corollary 7.3.17

Nonzero nilpotent matrices are zero divisors.

Idempotent matrix

An idempotent matrix is a square matrix A whose minimal polynomial is a factor of $x^2 - x$.

The prefix “idem” means “same” so that “idempotent” means that the matrix remains the same when we raise it to any power. Indeed, notice that $x^2 - x = 0$ implies that $x = x^2$.

Example 17. The $n \times n$ identity matrix for any integer $n \geq 1$ is $x - 1$ and clearly $\text{id}_{n \times n}^2 = \text{id}_{n \times n}$. So identity matrices are idempotent.

Example 18. The following matrix is idempotent:

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

Theorem 7.3.18

Any matrix with only 0's and 1's on the diagonal and 0's elsewhere is idempotent.

Proof. This is an exercise for the reader. Hint: think about method 1 for finding the minimal polynomial. \square

Key Concepts from this Section

- **minimal polynomial:** (page 828) A polynomial in the variable x of smallest positive degree whose leading coefficient is 1 and that is a zero scalar is called a *minimal polynomial* of a square matrix whose action is represented by the scalar x .
- **theorem 7.3.1 :** (page 828) The minimal polynomial is a factor of *every* zero polynomial scalar.
- **greatest common factor:** (page 829) A greatest common factor between two polynomials in $\mathbb{R}[x]$ is a common factor that all other common factors are factors of. If we declare that the leading coefficient of the greatest common factor must be 1, then the greatest common factor is unique.
- **theorem 7.3.2 :** (page 829) If we add two zero scalars together, we again get a zero scalar. If we multiply a zero scalar by any other polynomial, we again get a zero scalar.
- **theorem 7.3.3 :** (page 830) If $a(x)$ and $b(x)$ are zero scalars, then their greatest common factor is also a zero scalar.
- **euclidean algorithm:** (page 830) The *Euclidean Algorithm* applied to two polynomials $a(x)$ and $b(x)$ is the process of building the sequence

$$a(x), b(x), r_0(x), r_1(x), \dots, r_m(x)$$

until we come to the greatest common factor $r_m(x)$.

- **theorem 7.3.4 :** (page 830) All zero scalars are polynomial multiples of the minimal polynomial.
- **theorem 7.3.5 :** (page 831) Only by switching rows, columns and airdropping with polynomial multiples, we can turn a square matrix of polynomials into a diagonal matrix.

- **smith normal form over $\mathbb{R}[x]$:** (page 833) The Smith normal form of a matrix of polynomials is a diagonal matrix obtained only by *polynomial* airdropping, switching and perhaps dividing by *constants* so that every entry has leading coefficient 1 and so that as we move down the diagonal from top left to bottom right each entry is a factor of the next one.
- **$\mathbb{R}[x]$ -module isomorphisms:** (page 834) A $\mathbb{R}[x]$ -module isomorphism f is a bijective map (i.e. a bijective function) between two $\mathbb{R}[x]$ -modules such that:
 - It preserves addition: $f(v + w) = f(v) + f(w)$.
 - It preserves scalar multiplication from $\mathbb{R}[x]$. That is, polynomials can pass from domain to codomain *No guarantee for polynomial reciprocals (i.e. multiplicative inverses)*: $f(p(x) \cdot v) = p(x) \cdot f(v)$.

They preserve the $\mathbb{R}[x]$ -module structure.

- **$\mathbb{R}[x]$ -span of a vector:** (page 835) Suppose that x represents a square matrix action on \mathbb{R}^n . Then the $\mathbb{R}[x]$ -span of a vector v is the set $\mathbb{R}[x] \cdot v$. That is, it is all polynomial scalar multiples of v —like $(x^3 + 2x) \cdot v$ or $(x^5 - 2x^4 + 2) \cdot v$. Another way of thinking of this span is as the following \mathbb{R} span:

$$\langle 1, x \cdot v, x^2 \cdot v, x^3 \cdot v, \dots \rangle$$

going through all powers of x .

All polynomial spans come about in such a way.

- **minimal polynomial on a subspace:** (page 836) Suppose that x is represented by a square matrix A . Let A be thought of as a function under the column interpretation and let V be a *subspace* of the domain of that function. Then the minimal polynomial on the subspace V is the smallest degree polynomial $p(x)$ in x with leading coefficient 1 such that $p(x) \cdot v = (\text{zero vector})$ for all $v \in V$.

It is also a factor of all zero polynomial scalars on that subspace.

- **polynomial span and minimal polynomial:** (page 838) Suppose that the minimal polynomial of the action of a square matrix on a vector v is given by $p(x)$ of degree n . Then, the polynomial span of v is given as:

$$1 \cdot v \quad x \cdot v \quad \dots \quad x^{n-1} \cdot v$$

- **theorem 7.3.6:** (page 838) Suppose that the degree of the minimal polynomial of $\langle v \rangle$ is n . The following vector collection is linearly independent:

$$1 \cdot v \quad x \cdot v \quad \dots \quad x^{n-1} \cdot v$$

- **corollary 7.3.7 :** (page 839) If $p(x)$ is the minimal polynomial on the subspace $\langle v \rangle$, then $\langle v \rangle$ has dimension $\deg(p(x))$.
- **theorem 7.3.8 :** (page 839) Let v be any vector in \mathbb{R}^n and let x be the action by any $n \times n$ matrix. Then, there is a minimal polynomial of x on the subspace $\langle v \rangle$.
- **theorem 7.3.9 :** (page 839) If $\langle v \rangle$ has a degree 0 minimal polynomial (i.e. a constant $k \in \mathbb{R}$), then v is the zero vector.
- **invariant subspace:** (page 840) Let A be a square $n \times n$ matrix with entries in \mathbb{R} that acts on \mathbb{R}^n . Let V be a subspace of \mathbb{R}^n and let the action of A be represented by the scalar x . Then, if the $\mathbb{R}[x]$ -span of all of the vectors in V is again V , we say that V is an invariant subspace of \mathbb{R}^n with respect to the action of A .

That is, A is a linear transformation that does not take vectors that are in V out of V . If V is a plane, the matrix A would “keep the plane inside the plane”—not take any points out of it and put them anywhere else.

- **theorem 7.3.10 :** (page 841) The polynomial span of a vector *is an invariant subspace* in and of itself.
- **theorem 7.3.11 :** (page 842) Suppose that x represents the action of a matrix on a vector space. Let $(x - a)$ be the minimal polynomial on a subspace W . Then W is an invariant subspace with respect to the action of x .
- **theorem 7.3.12 :** (page 842) Let x denote the action of a square matrix on a vector space V . Let $p(x)$ be the minimal polynomial on the subspace $\langle v \rangle$ for some $v \in V$. Let W be the set of all vectors $w \in V$ such that the minimal polynomial on $\langle w \rangle$ is $p(x)$. Then, W is a subspace of V .
- **eigenspace:** (page 842) Let x denote the action of a square matrix A on a vector space V . Let W be the \mathbb{R} -span of all vectors $w \in V$ such that the minimal polynomial on $\langle w \rangle$ is a degree one polynomial $(x - a)$. Then, W is called an *eigenspace* of A .
- **eigenspaces are invariant:** (page 842) Since an eigenspace has a degree 1 minimal polynomial, it automatically is an invariant subspace. That means it is closed with respect to polynomial scalars.
- **eigenvector:** (page 842) An eigenvector is a vector in an eigenspace.
- **eigenvalue:** (page 843) Suppose that the minimal polynomial for an eigenspace is $(x - a)$. Then a is called the eigenvalue for that eigenspace.
- **theorem 7.3.13 :** (page 843) Let x denote the action of a square matrix A on a vector space and let a be an eigenvalue for A . Then if v is in the eigenspace associated to a , the matrix action x behaves *just like* the scalar action of a :

$$x \cdot v = a \cdot v$$

- **gcd: greatest common factor:** (page 844) We have factored out the greatest common factors of each column individually. This can be notated as “gcd” which stands for “greatest common divisor.”
- **least common multiple:** (page 846) The least common multiple between two polynomials in $\mathbb{R}[x]$ is a multiple of both polynomials that is a factor of all other common multiples. If we declare that the leading coefficient of the least common multiple must be 1, then the least common multiple is unique.
- **theorem 7.3.14 :** (page 847) On our way to getting the minimal polynomial, we can stop our column operations precisely when the degrees of the greatest common factors of each column add up to n (if we are working with an $n \times n$ matrix).
- **minimal polynomial versus characteristic polynomial:** (page 848) After the row and the column operations that take us to a diagonal matrix:
 - The characteristic polynomial is the product of the diagonal entries.
 - The minimal polynomial is the least common multiple of the diagonal entries.
- **irreducible polynomial:** (page 848) A polynomial is called irreducible over \mathbb{R} if its only factors in $\mathbb{R}[x]$ are constants and constant multiples of itself. One could similarly talk about being irreducible over $\mathbb{C}[x]$ if its only factors in $\mathbb{C}[x]$ are complex constant and complex constant multiples of itself.
- **reducible:** (page 848) A polynomial is reducible if it is not irreducible.
- **theorem 7.3.15 :** (page 848) The minimal polynomial and the characteristic polynomial share *the same* irreducible factors.
- **finding the minimal polynomial—method 1:** (page 849) For a $n \times n$ matrix A :
 1. Perform column *airdrops* ($\mathbb{R}[x]$ -isomorphisms) on $x \cdot \text{id} - A$ until the degrees of the greatest common factors of individual columns add up to n .
 2. Take the least common multiple of these.
- **finding the minimal polynomial—method 2:** (page 851) For a $n \times n$ matrix A :
 1. Compute the characteristic polynomial $p(x)$.
 2. List out the irreducible factors of $p(x)$ as $a_1(x), \dots, a_m(x)$.
 3. List all the factors of $p(x)$ of the form $a_1(x)^{r_1}, \dots, a_m(x)^{r_m}$ where $r_1 \neq 0, r_2 \neq 0, \dots, r_m \neq 0$.
This is because *the minimal polynomial must have all of these irreducibles as factors*.
 4. See which of the factors in this last list we have just created come out to the zero matrix.
 5. The smallest degree factor from this list that is equivalent to the zero matrix is the minimal polynomial.

- **proving the equivalence of the characteristic and minimal polynomials:** (page 853) Suppose that A is a $n \times n$ matrix whose action is represented by x . Look at the powers of x : $1, x, x^2, \dots, x^{n-1}$ as matrices. If you can find v such that the collection $\{1 \cdot v, x \cdot v, x^2 \cdot v, \dots, x^{n-1} \cdot v\}$ is linearly independent, then this proves that the characteristic polynomial of A is the same as the minimal polynomial of A .

In practice, you could try $v = e_1$ or $v = e_2$ or $v = e_3$ or \dots . This just amounts to considering the same column in each power of x thought of as a matrix. *Remember that if you cannot seem to find such a v you have not proven anything.*

- **nilpotent matrix:** (page 855) A Nilpotent matrix is a square matrix whose minimal polynomial is a power of x like x^2 or x^3 .
- **zero divisor matrix:** (page 855) A *nonzero* square matrix A is a zero divisor *if* there is another nonzero matrix B (also a zero divisor) such that $A \cdot B$ is the zero matrix.

We are literally saying that “zero” (i.e. the zero matrix) has nonzero factors (a.k.a. divisors).

- **theorem 7.3.16 :** (page 856) A square matrix A is a zero divisor if the constant term of the *characteristic* polynomial is 0. (*The constant term being zero is the same as saying that x is a factor of the characteristic polynomial.*)
- **corollary 7.3.17 :** (page 856) Nonzero nilpotent matrices are zero divisors.
- **idempotent matrix:** (page 856) An idempotent matrix is a square matrix A whose minimal polynomial is a factor of $x^2 - x$.
- **theorem 7.3.18 :** (page 857) Any matrix with only 0's and 1's on the diagonal and 0's elsewhere is idempotent.

7.3.13 Exercises

Minimal Polynomials

Find the minimal polynomial of each of the following matrices and compare it to the characteristic polynomial.

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

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

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

4.
$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

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

6.
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

7.
$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

8.
$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

9.
$$\begin{pmatrix} 0 & -2 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

10.
$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

11.
$$\begin{pmatrix} 0 & 3 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

12.
$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

13.
$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

14.
$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

15.
$$\begin{pmatrix} 0 & -2 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

16.
$$\begin{pmatrix} 0 & -2 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

17.
$$\begin{pmatrix} 0 & 3 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

18.
$$\begin{pmatrix} 0 & -2 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

19.
$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

20.
$$\begin{pmatrix} 0 & 3 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

21.
$$\begin{pmatrix} 0 & -2 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

22.
$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

If using method 1, the following may require things like adding $-x - 1$ to $x + 2$ to get a 1 or $-(x + 1) \cdot x$ to $x^2 + 2x$ to get an x . If you cannot get a 1 in a row, then at least try to reduce the degree of something until you can! You could also use method 2.

23.
$$\begin{pmatrix} -2 & 0 & 1 \\ 0 & -2 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

24.
$$\begin{pmatrix} 0 & -5 & -1 \\ 1 & 5 & 1 \\ -1 & -4 & 0 \end{pmatrix}$$

25.
$$\begin{pmatrix} 0 & -2 & 1 \\ 1 & 3 & -1 \\ 1 & 2 & 0 \end{pmatrix}$$

26.
$$\begin{pmatrix} 0 & -2 & 1 \\ 1 & -3 & 1 \\ 1 & -2 & 0 \end{pmatrix}$$

27.
$$\begin{pmatrix} -2 & 3 & -2 \\ 0 & 4 & -4 \\ 0 & 9 & -8 \end{pmatrix}$$

28.
$$\begin{pmatrix} 0 & -6 & -2 \\ 1 & -5 & -1 \\ -1 & 3 & -1 \end{pmatrix}$$

Minimal Polynomials and Invariant Subspaces

Use column operations to find the minimal polynomial and invariant subspaces associated with the columns you use.

29.
$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & -2 \end{pmatrix}$$

30.
$$\begin{pmatrix} 0 & -4 & 0 \\ 1 & 4 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

31.
$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

32.
$$\begin{pmatrix} 0 & -4 & 0 \\ 1 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

33.
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & 1 & 4 \end{pmatrix}$$

34.
$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

35.
$$\begin{pmatrix} 0 & -6 & 2 \\ 1 & 5 & -1 \\ 1 & 3 & 1 \end{pmatrix}$$

36.
$$\begin{pmatrix} 1 & -2 & 1 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

37.
$$\begin{pmatrix} 0 & 4 & -2 \\ 1 & 0 & -1 \\ 1 & 2 & -3 \end{pmatrix}$$

38.
$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

39.
$$\begin{pmatrix} 0 & -2 & 1 \\ 1 & 3 & -1 \\ 1 & 2 & 0 \end{pmatrix}$$

40.
$$\begin{pmatrix} -2 & -3 & 2 \\ 0 & 4 & -4 \\ 0 & 9 & -8 \end{pmatrix}$$

Polynomial Spans

For each of the following, find vectors in \mathbb{R}^3 which span the *polynomial span* $\mathbb{R}[x] \cdot v$ where x is represented by the action of the matrix A . The idea is that we can use $v, x \cdot v, \dots, x^d \cdot v$ where d is the degree of the minimal polynomial.

41. $v = (1, 1, 0)$

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

42. $v = (2, 0, 0)$

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

43. $v = (-1, 0, 0)$

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

44. $v = (0, 1, 0)$

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

45. $v = (2, 0, 0)$

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

46. $v = (0, 1, 0)$

$$A = \begin{pmatrix} 2 & 3 & 2 \\ 0 & -4 & -4 \\ 0 & 9 & 8 \end{pmatrix}$$

47. $v = (2, 0, 2)$

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

48. $v = (2, 0, 0)$

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

49. $v = (1, 0, 0)$

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

50. $v = (0, 2, 0)$

$$A = \begin{pmatrix} 2 & 3 & 2 \\ 0 & -4 & -4 \\ 0 & 9 & 8 \end{pmatrix}$$

51. $v = (0, -1, -1)$

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

52. $v = (0, 2, 2)$

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

Proof Practice

- 53.** Find your own examples of nilpotent matrices.
- 54.** Prove that a nonzero square matrix A is a zero divisor if the constant term of the *characteristic* polynomial is 0.
- 55.** If we know the *minimal* polynomial of a zero divisor matrix, how does this help us find a nonzero matrix it can be multiplied by to yield the zero matrix?
- 56.** Use the idea of the last exercise to find pairs of nonzero matrices that multiply together to give the zero matrix. *Hint: how does a matrix with a top row of all 0's guarantee that x is a factor of the characteristic polynomial? Think about a cofactor expansion.*
- 57.** Find pairs of nonzero *nilpotent* matrices that multiply together to give the zero matrix.
- 58.** Prove that any matrix with only 0's and 1's on the diagonal and 0's elsewhere is idempotent. *Hint: think about method 1 for finding the minimal polynomial.*

7.3.14 Solutions

1. Minimal polynomial:

$$x^3 - x$$

Characteristic Polynomial:

$$x^3 - x$$

2. Minimal polynomial:

$$x^2 + x$$

Characteristic Polynomial:

$$x^3 + 2x^2 + x$$

3. Minimal polynomial:

$$x - 1$$

Characteristic Polynomial:

$$x^3 - 3x^2 + 3x - 1$$

4. Minimal polynomial:

$$x^2 - x$$

Characteristic Polynomial:

$$x^3 - x^2$$

5. Minimal polynomial:

$$x^2 + x$$

Characteristic Polynomial:

$$x^3 + 2x^2 + x$$

6. Minimal polynomial:

$$x - 2$$

Characteristic Polynomial:

$$x^3 - 6x^2 + 12x - 8$$

7. Minimal polynomial:

$$x - 3$$

Characteristic Polynomial:

$$x^3 - 9x^2 + 27x - 27$$

8. Minimal polynomial:

$$x^2 - 2x + 1$$

Characteristic Polynomial:

$$x^3 - 3x^2 + 3x - 1$$

9. Minimal polynomial:

$$x^2 - 3x + 2$$

Characteristic Polynomial:

$$x^3 - 4x^2 + 5x - 2$$

10. Minimal polynomial:

$$x^2 - 1$$

Characteristic Polynomial:

$$x^3 - x^2 - x + 1$$

11. Minimal polynomial:

$$x^2 + 2x - 3$$

Characteristic Polynomial:

$$x^3 + x^2 - 5x + 3$$

12. Minimal polynomial:

$$x^3 - x^2 + x - 1$$

Characteristic Polynomial:

$$x^3 - x^2 + x - 1$$

13. Minimal polynomial:

$$x^3 - x^2 + x - 1$$

Characteristic polynomial: $x^3 - x^2 + x - 1$

14. Minimal polynomial:

$$x^2 - 1$$

Characteristic polynomial: $x^3 - x^2 - x + 1$

15. Minimal polynomial:

$$x^3 - 2x^2 - x + 2$$

Characteristic polynomial: $x^3 - 2x^2 - x + 2$

16. Minimal polynomial:

$$x^2 - 3x + 2$$

Characteristic polynomial: $x^3 - 4x^2 + 5x - 2$

17. Minimal polynomial:

$$x^3 + 3x^2 - x - 3$$

Characteristic polynomial: $x^3 + 3x^2 - x - 3$

18. Minimal polynomial:

$$x^2 - 3x + 2$$

Characteristic polynomial: $x^3 - 4x^2 + 5x - 2$

19. Minimal polynomial:

$$x^2 - 2x + 1$$

Characteristic polynomial: $x^3 - 3x^2 + 3x - 1$

20. Minimal polynomial:

$$x^3 + 3x^2 - x - 3$$

Characteristic polynomial: $x^3 + 3x^2 - x - 3$

21. Minimal polynomial:

$$x^2 - 3x + 2$$

Characteristic polynomial: $x^3 - 4x^2 + 5x - 2$

22. Minimal polynomial:

$$x^2 - 1$$

Characteristic polynomial: $x^3 + x^2 - x - 1$

23. Minimal polynomial:

$$(x - 1) \cdot (x + 2)$$

Possible result of column operations:

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & x+2 & 0 \\ -x+1 & 0 & x^2+x-2 \end{pmatrix}$$

24. Minimal polynomial:

$$(x - 1) \cdot (x - 2)^2$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 - 5x + 5 & x^4 - 9x^3 + 28x^2 - 36x + 16 \\ -1 & 0 & 0 \\ 1 & x - 1 & x^3 - 5x^2 + 8x - 4 \end{pmatrix}$$

25. Minimal polynomial:

$$(x - 1)^2$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 - 3x + 2 & x^2 - 2x + 1 \\ -1 & 0 & 0 \\ -1 & -x + 1 & 0 \end{pmatrix}$$

26. Minimal polynomial:

$$(x + 1)^2$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 + 3x + 2 & x^2 + 2x + 1 \\ -1 & 0 & 0 \\ -1 & -x - 1 & 0 \end{pmatrix}$$

27. Minimal polynomial:

$$(x + 2)^2$$

Possible result of column operations:

$$\begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{3}x + \frac{4}{3} & x^2 - 2x - 8 & \frac{1}{9}x^2 + \frac{4}{9}x + \frac{4}{9} \\ 3 & -9x - 18 & 0 \end{pmatrix}$$

28. Minimal polynomial:

$$(x + 2)^2$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 + 5x + 6 & -x^2 - 4x - 4 \\ -1 & 0 & 0 \\ 1 & x + 2 & 0 \end{pmatrix}$$

29. Minimal polynomial:

$$x \cdot (x + 2)$$

Invariant Subspaces:

$$\langle(-1, 0, 0)\rangle$$

$$\langle(0, 1, 0), (0, 0, 1)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} x & -x & 0 \\ x & 0 & x^2 + 2x \\ -1 & 0 & 0 \end{pmatrix}$$

30. Minimal polynomial:

$$x \cdot (x - 2)^2$$

Invariant Subspaces:

$$\langle(-1, 0, \frac{1}{4}), (0, -1, 0), (4, -4, 0)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 - 4x + 4 & -x^3 + 4x^2 - 4x \\ -1 & 0 & 0 \\ 0 & -\frac{1}{4}x^2 + x & \frac{1}{4}x^3 - x^2 + x \end{pmatrix}$$

31. Minimal polynomial:

$$x^2$$

Invariant Subspaces:

$$\langle(0, 1, 1)\rangle$$

$$\langle(-1, 0, 0), (0, -1, 0)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 & -x^2 \\ -1 & 0 & 0 \\ 0 & x & 0 \end{pmatrix}$$

32. Minimal polynomial:

$$(x - 2)^2$$

Invariant Subspaces:

$$\langle(-2, 1, 1)\rangle$$

$$\langle(-1, 0, 0), (0, -1, 0)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 - 4x + 4 & -x^2 + 4x - 4 \\ -1 & 0 & 0 \\ 0 & x - 2 & 0 \end{pmatrix}$$

33. Minimal polynomial:

$$(x - 2)^2$$

Invariant Subspaces:

$$\langle(-1, 0, 0)\rangle$$

$$\langle(0, 1, 0), (0, 0, 1)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} x - 2 & -x + 2 & 0 \\ x & 0 & x^2 - 4x + 4 \\ -1 & 0 & 0 \end{pmatrix}$$

34. Minimal polynomial:

$$x \cdot (x + 2)$$

Invariant Subspaces:

$$\langle(2, 1, 1)\rangle$$

$$\langle(-1, 0, 0), (0, -1, 0)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 + 2x & -x^2 - 2x \\ -1 & 0 & 0 \\ 0 & x & 0 \end{pmatrix}$$

35. Minimal polynomial:

$$(x - 2)^2$$

Invariant Subspaces:

$$\langle(-3, 1, 0)\rangle$$

$$\langle(1, 0, 0), (0, 1, 1)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 - 5x + 6 & x^2 - 4x + 4 \\ -1 & 0 & 0 \\ -1 & -x + 2 & 0 \end{pmatrix}$$

36. Minimal polynomial:

$$(x - 1) \cdot (x + 1)$$

Invariant Subspaces:

$$\langle(0, 1, 2)\rangle$$

$$\langle(0, 0, 1), (1, 1, 1)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2}x + \frac{1}{2} & x - 1 & 0 \\ 0 & 2x - 2 & x^2 - 1 \end{pmatrix}$$

37. Minimal polynomial:

$$(x - 1) \cdot (x + 2)$$

Invariant Subspaces:

$$\langle(-2, 1, 0)\rangle$$

$$\langle(1, 0, 0), (0, 1, 1)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 - 4 & x^2 + x - 2 \\ -1 & 0 & 0 \\ -1 & -x - 2 & 0 \end{pmatrix}$$

38. Minimal polynomial:

$$(x - 1)^2$$

Invariant Subspaces:

$$\langle(0, 1, 0)\rangle$$

$$\langle(0, 0, 1), (-1, -1, 1)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & x - 1 & 0 \\ x - 1 & 0 & x^2 - 2x + 1 \end{pmatrix}$$

39. Minimal polynomial:

$$(x - 1)^2$$

Invariant Subspaces:

$$\langle(-2, 1, 0)\rangle$$

$$\langle(1, 0, 0), (0, 1, 1)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 - 3x + 2 & x^2 - 2x + 1 \\ -1 & 0 & 0 \\ -1 & -x + 1 & 0 \end{pmatrix}$$

40. Minimal polynomial:

$$(x + 2)^2$$

Invariant Subspaces:

$$\langle(-3, 0, 0)\rangle$$

$$\langle(0, \frac{1}{9}, 0), (-\frac{1}{3}, \frac{4}{9}, 1)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{3}x - \frac{4}{3} & x^2 - 2x - 8 & \frac{1}{9}x^2 + \frac{4}{9}x + \frac{4}{9} \\ -3 & -9x - 18 & 0 \end{pmatrix}$$

41. $\langle (1, 1, 0), (1, 2, -3), (-1, 0, 1) \rangle$

minimum polynomial:

$$x^3 + x^2$$

42. $\langle (2, 0, 0), (0, 2, -2) \rangle$

minimum polynomial:

$$x^2 + 2x + 1$$

43. $\langle (-1, 0, 0), (-1, 0, 0), (-1, 0, 0) \rangle$

minimum polynomial:

$$x^3 + x^2 - x - 1$$

44. $\langle (0, 1, 0), (-2, -1, 4) \rangle$

minimum polynomial:

$$x^2 - 2x + 1$$

45. $\langle (2, 0, 0), (0, 0, 0), (0, 0, 0) \rangle$

minimum polynomial:

$$x^3 + 2x^2 + x$$

46. $\langle (0, 1, 0), (3, -4, 9) \rangle$

minimum polynomial:

$$x^2 - 4x + 4$$

47. $\langle (2, 0, 2), (0, 0, 0) \rangle$

minimum polynomial:

$$x^2$$

48. $\langle (2, 0, 0), (0, 2, -2) \rangle$

minimum polynomial:

$$x^2 - 4x + 4$$

49. $\langle (1, 0, 0), (0, 1, -1) \rangle$

minimum polynomial:

$$x^2 - 2x$$

50. $\langle (0, 2, 0), (6, -8, 18) \rangle$

minimum polynomial:

$$x^2 - 4x + 4$$

51. $\langle (0, -1, -1), (4, 4, 4) \rangle$

minimum polynomial:

$$x^2 + 4x + 4$$

52. $\langle (0, 2, 2), (-2, 0, 2), (0, 0, 0) \rangle$

minimum polynomial:

$$x^3 - 2x^2$$

53. Some examples are $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ or $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ or $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. Think about the characteristic polynomial. You want the determinant of $x \cdot \text{id} - A$ to be of the form x^n . In figuring out a possible A , think of what you would need to replace the $*$'s with in $x \cdot \text{id} - A = \begin{pmatrix} x & * & * \\ * & x & * \\ * & * & * \end{pmatrix}$ so that the determinant is x^3 . Then figure out what A would make those $*$'s possible.

54. The characteristic and the minimal polynomials share the same irreducible factors. The factor “ x ” itself

is irreducible. Saying that the constant term of the characteristic polynomial is 0 is the same as saying that x is a factor of the characteristic polynomial. Therefore, it is also a factor of the minimal polynomial. Suppose that the minimal polynomial is $p(x) = x \cdot q(x)$. Since $p(x)$ is the minimal degree nonzero polynomial in x yielding the zero matrix, $q(x)$ cannot be the zero matrix—since it has degree less than $p(x)$. We are assuming that $x = A$ is a nonzero matrix. Therefore, A and $q(A)$ are two nonzero matrices that multiply together to yield the zero matrix (since they multiply together to give the minimal polynomial *which is the zero matrix*).

55. The proof of the last exercise answers this question—you use A and $q(A)$.

56. Consider the matrix

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

From

$$\det(x \cdot \text{id} - A) = \det \begin{pmatrix} x & 0 & 0 \\ 0 & x-1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

the characteristic polynomial is $x \cdot (x-1)^2$. One can check that

$$\underbrace{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_x \cdot \underbrace{\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{x-1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

57. One example is $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ($= A$) since the minimal polynomial of A is x^2 . So we know that $x \cdot x = 0$. Therefore, when we plug A in for x , we have: $A \cdot A =$ (zero matrix).

58. Right away $x \cdot \text{id} - A$ is in the proper form—no column operations are necessary. Just take the least common multiple of the nonzero entries here and we get x or $x-1$ or $x(x-1)$. This is enough.

Diagonalization of Matrices

7.4

7.4.1 Eigenvectors Help Diagonalize	873
7.4.2 Exploring Why We Could Find Enough Eigenvectors	876
7.4.3 Eigenvectors in $\mathbb{R}[x] \cdot v$	879
7.4.4 Minimal Polynomials and Diagonalizability	882
7.4.5 Proof of Diagonalization By Ranges and Kernels	884
7.4.6 Finding Eigenvectors by Ranges	887
7.4.7 Finding Eigenvectors by Kernels	892
7.4.8 Powers of a matrix	895
7.4.9 Diagonalizing by Roots	896
7.4.10 Exercises	901
7.4.11 Solutions	905

Questions to Guide Your Study:

- *What does it mean to diagonalize a matrix?*
- *What conditions guarantee that we can diagonalize a matrix?*
- *How do we use “ranges” to diagonalize?*
- *How do we use “kernels” to diagonalize?*
- *How can diagonalizing help us to raise a matrix to a power?*

In this section we will see how we can change the basis in which a matrix is written so that in that basis the matrix is a diagonal matrix.

7.4.1 Eigenvectors Help Diagonalize

The notion of eigenvectors and eigenvalues was brought up in the last section. But let's introduce the idea again. An eigenvector is simply a vector whose minimal polynomial is something like $(x - a)$. The number

a is called the eigenvalue for that vector. An eigenspace is simply the smallest subspace containing all vectors whose minimal polynomial is $(x - a)$.

Eigenspace

Let x denote the action of a square matrix A on a vector space V . Let W be the \mathbb{R} -span of all vectors $w \in V$ such that the minimal polynomial on $\langle w \rangle$ is a degree one polynomial $(x - a)$. Then, W is called an *eigenspace* of A .

Eigenspaces are Invariant

Since an eigenspace has a degree 1 minimal polynomial, it automatically is an invariant subspace by a theorem in the last section. That means it is closed with respect to polynomial scalars.

Eigenvector

An eigenvector is a vector in an eigenspace.

Eigenvalue

Suppose that the minimal polynomial for an eigenspace is $(x - a)$. Then a is called the eigenvalue for that eigenspace.

Scalar Action on Eigenvectors

Let x denote the action of a square matrix A on a vector space and let a be an eigenvalue for A . Then if v is in the eigenspace associated to a , the matrix action x behaves *just like* the scalar action of a :

$$x \cdot v = a \cdot v$$

Example 1. Let's see eigenvalues and eigenvectors at work. Suppose that we have a matrix

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

and further suppose that we already know the following:

eigenvalue $x = 2$: eigenspace: $\langle (0, 1, 0) \rangle$

eigenvalue $x = 1$: eigenspace: $\langle (1, 0, -1), (0, 1, -1) \rangle$

What would happen if we wanted to write the matrix A with respect to the following basis?

$$(0, 1, 0) \quad (1, 0, -1) \quad (0, 1, -1)$$

Our unpretending matrix would be:

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

The matrix A with respect to this basis now becomes UAU^{-1} . Let's see what happens when we run e_1 through UAU^{-1} .

eigenvalue $x = 2$ eigenvectors	eigenvalue $x = 1$ eigenvectors	eigenvalue $x = 1$ eigenvectors
$\underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ -1 & 0 & -1 \end{pmatrix}}_{U^{-1}}$	$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_A$	$\underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix}}_U$
U^{-1} reverses what U did. $2 \cdot (\text{eigenvector})$ is sent to $2 \cdot e_1$.		
A acts on this eigenvector via multiplication by 2		
Send e_1 to first column of U which is an eigenvector.		

Notice that we get $e_1 \mapsto 2 \cdot e_1$. This means that the first column of $U^{-1}AU$ is $2 \cdot e_1$. This “2” happened because e_1 is first sent to the first column of U which is an eigenvector with eigenvalue 2.

Similarly, $e_2 \mapsto 1 \cdot e_2$ since “1” is the eigenvalue corresponding to the second column of U . Lastly, $e_3 \mapsto 1 \cdot e_3$ since “1” is the eigenvalue corresponding to the third column of U .

This tells us that

$$U^{-1}AU = \underbrace{\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_D$$

Diagonal Change of Basis

If we can select n linearly independent eigenvectors for a matrix A , then they serve as a basis with which we can diagonalize A . Writing these eigenvectors as the columns of an unpretending matrix U , we have:

$$U^{-1}AU = D$$

where D is a diagonal matrix.

7.4.2 Exploring Why We Could Find Enough Eigenvectors

It is not always possible to find such a nice collection of linearly independent eigenvectors to diagonalize a matrix. But in our example above we could. What was it about this matrix that allowed us to find this collection? Perhaps we should peer more into where these eigenvectors came from—and the minimal polynomial in particular.

The minimal polynomial of A is $(x - 2)(x - 1)$ and the characteristic polynomial is $(x - 2)(x - 1)^2$. Let's look at the process of how this minimal polynomial could be found via column operations on $x \cdot \text{id} - A$.

$$\left(\begin{array}{ccc} x-1 & 0 & 0 \\ -1 & x-2 & -1 \\ 0 & 0 & x-1 \end{array} \right) \rightarrow \left(\begin{array}{ccc} x-1 & 0 & 0 \\ -1 & 0 & -1 \\ 0 & (x-1)(x-2) & x-1 \end{array} \right) \rightarrow \left(\begin{array}{ccc} x-1 & 0 & 0 \\ 0 & 0 & -1 \\ -(x-1) & (x-1)(x-2) & x-1 \end{array} \right)$$

We have done enough since:

$$\gcd \begin{pmatrix} x-1 \\ 0 \\ -(x-1) \end{pmatrix} = \underbrace{(x-1)}_{\text{degree 1}} \quad \gcd \begin{pmatrix} 0 \\ 0 \\ (x-1)(x-2) \end{pmatrix} = \underbrace{(x-1)(x-2)}_{\text{degree 2}} \quad \gcd \begin{pmatrix} 0 \\ -1 \\ x-1 \end{pmatrix} = \underbrace{1}_{\text{degree 0}}$$

The minimal polynomial is the least common multiple of these: $(x-1)(x-2)$. Look at these columns in factored form:

$$(x-1) \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \quad (x-1)(x-2) \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad (1) \cdot \begin{pmatrix} 0 \\ -1 \\ x-1 \end{pmatrix}$$

We know the following:

- These are all zero columns when x represents the action of A .
- The factor $(x-1)$ is the minimal polynomial on the subspace $\langle (1, 0, -1) \rangle$ which has dimension 1.
- The factor $(x-1)(x-2)$ is the minimal polynomial on the subspace $\langle \underbrace{(0, 0, 1)}_v, \underbrace{(0, 1, 1)}_{x \cdot v} \rangle$ which has dimension 2.
- These subspaces are of the form $\mathbb{R}[x] \cdot v$.
- These subspaces are “linearly independent” to each other. That is, together they make all of \mathbb{R}^3 .
- All of the vectors in $\langle (1, 0, -1) \rangle$ are eigenvectors since the minimal polynomial of this space is $(x-1)$.

Our goal is to find 3 linearly independent eigenvectors.

We have one coming from the subspace $\langle (1, 0, -1) \rangle$: we may as well just take $(1, 0, -1)$. Now anything we find in the other subspace, $\langle \underbrace{(0, 0, 1)}_v, \underbrace{(0, 1, 1)}_{x \cdot v} \rangle$, will be linearly independent already to what we took from the first subspace.

So really the question amounts to just finding a linearly independent set of eigenvectors within each individual invariant subspace from our column process.

So, we turn our attention to $W = \langle \underbrace{(0, 0, 1)}_v, \underbrace{(0, 1, 1)}_{x \cdot v} \rangle$. The minimal polynomial on this subspace of dimension 2 is made up of two irreducible factors: $(x-1)$ and $(x-2)$. Now remember that W is a polynomial span so that it is invariant with respect to the action of x . That is,

$$x \cdot \underbrace{(\text{a polynomial}) \cdot v}_{\in W} = (\text{another polynomial}) \cdot v \in W$$

Theorem 7.4.1

For an invariant subspace W under the action of x , multiplication by x yields a linear transformation $W \rightarrow W$. It only sends vectors in W to vectors in W .

Note that $(x - 2)$ can be thought of as a matrix and $(x - 2) \cdot W$ can be thought of as the range of the linear transformation described by $x - 2$. Hence, $(x - 2) \cdot W$ is a vector space. We prove that the minimal polynomial on $(x - 2) \cdot W$ is $(x - 1)$.

Theorem 7.4.2

If the minimal polynomial on a subspace W is $(x - 1)(x - 2)$, then the minimal polynomial on $(x - 2) \cdot W$ is $(x - 1)$. This result is easily generalized. One example is if $(x - 1)(x - 2)(x - 3)$ is the minimal polynomial of a subspace H . Then in that case, $(x - 3)$ would be the minimal polynomial of $(x - 1)(x - 2) \cdot H$.

Proof. Note that $(x - 2) \cdot W$ has to contain a nonzero vector w because $(x - 2)$ is not the minimal polynomial on all of W . We know that $w \in (x - 2) \cdot W$ means that

$$(x - 1) \cdot w \in (x - 1)(x - 2) \cdot W = \{ \text{(zero vector)} \}$$

Since w is nonzero, the minimal polynomial on $\langle w \rangle$ which is a factor of $x - 1$ must have degree greater than 0. This forces the minimal polynomial on $\langle w \rangle$ to be $(x - 1)$. Since w was an arbitrary nonzero vector in $(x - 2) \cdot W$, the minimal polynomial of $(x - 2) \cdot W$ has to be $x - 1$.

□

Therefore, anything in $(x - 2) \cdot W$ is an eigenvector for the eigenvalue $x = 1$. We can choose a nonzero vector among these. Call it w_1 .

Similarly, anything in $(x - 1) \cdot W$ is an eigenvector for the eigenvalue $x = 2$. We can choose a nonzero vector among these. Call it w_2 .

We have two eigenvectors in W . That would be enough if they were linearly independent.

Theorem 7.4.3

These two eigenvectors that we have found are linearly independent. We want to show this is true if we only assume they are both nonzero and that one came from $(x - 2) \cdot W$ and the other from $(x - 1) \cdot W$. *The proof given here is via polynomials.*

Proof. Notice that

$$(x - 2) \cdot W \subsetneq \underbrace{W}_{\dim 2}$$

We use \subsetneq to signify that these subspaces are different. *This is because they have different minimal polynomials associated with them.* This forces $\dim (x - 2) \cdot W$ to be 1. Similarly, $\dim (x - 1) \cdot W = 1$. Also notice that

$$\mathbb{R}[x] \cdot (x - 2) \cdot W \supset \mathbb{R}[x] \cdot w_1 = \langle w_1 \rangle$$

since the minimal polynomial on $\langle w_1 \rangle$ has degree 1. This forces

$$\mathbb{R}[x] \cdot (x - 2) \cdot W = \langle w_1 \rangle$$

Similarly,

$$\mathbb{R}[x] \cdot (x - 1) \cdot W = \langle w_2 \rangle$$

Since the greatest common factor of $(x - 1)$ and $(x - 2)$ is 1, we can find 1 as a remainder in the steps of the Euclidean algorithm if we divide $(x - 1)$ into $(x - 2)$. The Euclidean algorithm can be worked backwards to find $a(x)$ and $b(x)$ such that

$$a(x)(x - 1) + b(x)(x - 2) = 1$$

So 1 is therefore a polynomial linear combination of $(x - 1)$ and $(x - 2)$. This means that

$$\underbrace{\mathbb{R}[x] \cdot (x - 2) \cdot W}_{\langle w_1 \rangle} + \underbrace{\mathbb{R}[x] \cdot (x - 1) \cdot W}_{\langle w_2 \rangle} = \mathbb{R}[x] \cdot 1 \cdot W = W$$

Therefore, w_1 and w_2 together span W which is a 2-dimensional vector space. Hence, w_1 and w_2 are linearly independent. \square

Hence, we have enough linearly independent eigenvectors.

7.4.3 Eigenvectors in $\mathbb{R}[x] \cdot v$

In our column process for finding the minimal polynomial, we use the least common multiple of the minimal polynomials of subspaces of the form $\mathbb{R}[x] \cdot v$.

Let's understand first what should happen within each $(\mathbb{R}[x] \cdot v)$ -type subspace.

Let $H = \mathbb{R}[x] \cdot v$. Now the only way to get an eigenvector in H is to take it from a subspace of H where $(x - a)$ is the minimal polynomial. The question is, do we have enough such subspaces?

Theorem 7.4.4

If $H = \mathbb{R}[x] \cdot v$ has a minimal polynomial $p(x)$ of degree n and $b(x)$ is a degree m factor of $p(x)$, then the dimension of $b(x) \cdot H$ is

$$\deg \frac{p(x)}{b(x)} = n - m$$

The minimal polynomial of $b(x) \cdot H$ is

$$\frac{p(x)}{b(x)}$$

Proof. The minimal polynomials of $\langle v \rangle$ and $\mathbb{R}[x] \cdot v$ are the same. Let $n = \deg p(x)$. Since this is the minimal polynomial of $\langle v \rangle$, we know that $\dim H = \dim \mathbb{R}[x] \cdot v = n$.

Now suppose that $b(x)$ is a factor of $p(x)$ with degree m . Then, let $w = b(x) \cdot v$. The minimal polynomial of $\langle w \rangle$ has to be a factor of $\frac{p(x)}{b(x)}$ since

$$\frac{p(x)}{b(x)} \cdot b(x) \cdot w = p(x) \cdot w = (\text{zero vector})$$

If the minimal polynomial were some factor $a(x)$ of $\frac{p(x)}{b(x)}$ not equal to $\frac{p(x)}{b(x)}$ itself, then

$$(\text{zero vector}) = a(x) \cdot w = a(x) \cdot b(x) \cdot v$$

But $\deg a(x) \cdot b(x) < n$. This contradicts the minimality of $p(x)$. Therefore, $\frac{p(x)}{b(x)}$ is the minimal polynomial of $\langle w \rangle$ so that the dimension of $\mathbb{R}[x] \cdot w$ is $\deg \frac{p(x)}{b(x)} = n - m$. Yet, $\mathbb{R}[x] \cdot w = \mathbb{R}[x] \cdot b(x) \cdot v = b(x) \cdot H$. Therefore, the dimension of $b(x) \cdot H$ is $n - m$.

□

Corollary 7.4.5

Let $W = \frac{p(x)}{x - a} \cdot H$. Then $\dim W = 1$.

Proof. This is just the computation: $\deg \frac{p(x)}{x - a} = n - (n - 1) = 1$.

□

Theorem 7.4.6

The only vectors in $H = \mathbb{R}[x] \cdot v$ with a minimal polynomial of $(x - a)$ are those in $W = \frac{p(x)}{x - a} \cdot H$.

Proof. If $h \in H$, then $h = r(x) \cdot v$ for some polynomial $r(x)$. If $(x - a)r(x) \cdot v$ is the zero vector, then $p(x)$ must be a factor of $(x - a)r(x)$. For $(x - a)r(x)$ to minimally be a multiple of $p(x)$ is the same as saying $r(x) = k \cdot \frac{p(x)}{(x - a)}$ for some scalar $k \in \mathbb{R}$. \square

We can only pull *just one* eigenvector from each $\frac{p(x)}{x - a} \cdot H$ as a ranges through the possible eigenvalues. Now are these linearly independent?

Theorem 7.4.7

Now, if w has a minimal polynomial such that one of its factors is different from the factors of any of the minimal polynomials of the vectors in a linearly independent list $\{w_1, w_2, \dots, w_m\}$, then extending the collection to $\{w, w_1, w_2, \dots, w_m\}$ is again a linearly independent collection.

Proof. If $\{w, w_1, w_2, \dots, w_m\}$ were linearly dependent, then w would be expressible in terms of $\{w_1, w_2, \dots, w_m\}$. Then the least common multiple $c(x)$ of all the minimal polynomials of $\{w_1, w_2, \dots, w_m\}$ would act like zero on w . This means that the minimal polynomial of w should be a factor of $c(x)$. This contradicts the fact that w does not share one of its factors with $c(x)$. \square

Corollary 7.4.8

Let $(x - a_1), (x - a_2), \dots, (x - a_k)$ be the distinct linear factors of $p(x)$ where $p(x)$ is the minimal polynomial of a vector v . Let w_i be a nonzero vector in the one-dimensional space $\frac{p(x)}{(x - a_i)} \cdot v$.

Then, the collection $\{w_1, \dots, w_k\}$ is linearly independent.

Proof. The minimal polynomial of w_i is $(x - a_i)$ which is different from any of the other $(x - a_j)$ where $j \neq i$. Therefore, by the last theorem via an induction argument we have the result.

An alternate proof of this fact can come from a repeated use of the Euclidean algorithm worked backwards until we obtain a polynomial linear combination of $\frac{p(x)}{(x - a_1)}, \dots, \frac{p(x)}{(x - a_k)}$ equal to the greatest common factor of these same polynomials. This tells us:

$$\underbrace{\mathbb{R}[x] \cdot \frac{p(x)}{(x - a_1)} \cdot v + \dots + \mathbb{R}[x] \cdot \frac{p(x)}{(x - a_k)} \cdot v}_{\langle w_1 \rangle} + \dots + \underbrace{\mathbb{R}[x] \cdot \frac{p(x)}{(x - a_k)} \cdot v}_{\langle w_k \rangle}$$

$$= \mathbb{R}[x] \cdot \gcd \left(\frac{p(x)}{(x - a_1)}, \dots, \frac{p(x)}{(x - a_k)} \right) \cdot v = \mathbb{R}[x] \cdot \underbrace{\frac{p(x)}{(x - a_1) \cdots (x - a_k)} \cdot v}_w$$

The minimal polynomial of this w is $(x - a_1) \cdots (x - a_k)$ so that the $\mathbb{R}[x]$ -span of w has dimension k . This proves the linear independence. \square

We have just learned:

Theorem 7.4.9

The only way to get k linearly independent eigenvectors in $H = \mathbb{R}[x] \cdot v$ is for there to be k distinct linear factors $(x - a)$ of the minimal polynomial $p(x)$ of $\langle v \rangle$ (which is the same as the minimal polynomial of H).

7.4.4 Minimal Polynomials and Diagonalizability

We have been talking about minimal polynomials on subspaces of the form $\mathbb{R}[x] \cdot v$.

Now let's consider the minimal polynomial $m(x)$ on the whole vector space domain of the square matrix A .

Theorem 7.4.10

The only way for $(x - a)^2$ to be a factor of $m(x)$ is for $(x - a)^2$ to be a factor of the minimal polynomial $p(x)$ of one of the subspaces $\mathbb{R}[x] \cdot v$.

Proof. If it was not a factor of any of the $p(x)$, then it would not show up in the least common multiple of all of the $p(x)$'s. \square

Theorem 7.4.11

As long as $m(x)$...

- is completely factorable into linear factors $(x - a)$
- has no factors of the form $(x - a)^2$

then we can find the right number of linearly independent eigenvectors to diagonalize the matrix.

Notice that in our example earlier, we had a vector v_1 with minimal polynomial $(x - 1)$ and a vector v_2 with minimal polynomial $(x - 1)(x - 2)$. This gives us two subspaces that are linearly independent to each other:

- $\mathbb{R}[x] \cdot v_1$ with dimension 1: can choose an eigenvector with eigenvalue $x = 1$
- $\mathbb{R}[x] \cdot v_2$ with dimension 2: can choose an eigenvector with eigenvalue $x = 1$ and another one with eigenvalue $x = 2$

The eigenspace for $x = 1$ has dimension 2 because it has one dimension from two different $\mathbb{R}[x] \cdot$ (vector) subspaces.

Theorem 7.4.12

Each $\mathbb{R}[x] \cdot$ (vector) subspace contributes *only one* dimension at most to each eigenspace.

Theorem 7.4.13

The characteristic polynomial and the minimal polynomials are exactly the same when the characteristic polynomial is factorable into *only* nonrepeating linear factors $(x - a)$.

Proof. This comes from the fact that both the characteristic and the minimal polynomials share the same irreducible factors. \square

Example 2. If the characteristic polynomial of a square matrix is $(x - 1)(x + 3)(x - 4)$, then automatically we know it is a 3×3 matrix since the characteristic polynomial always has the same degree as the number of rows or columns of the matrix. We also know that the minimal polynomial is precisely $(x - 1)(x + 3)(x - 4)$ since all these linear factors: $(x - 1)$, $(x + 3)$, and $(x - 4)$ are distinct.

7.4.5 Proof of Diagonalization By Ranges and Kernels

Eigenvectors for Diagonlization

In the *diagonalization* process we could use either of the following two methods:

- To find our eigenvectors we can look at the ranges of factors of the minimal polynomial. That is, the span of the columns of the matrix. For instance, if the minimal polynomial is $(x - 1)(x + 5)$, the range (the column span) of the matrix $(x + 5)$ gives all of the eigenvectors for $x = 1$. We will see more of this as we actually work through examples.
- To find our eigenvectors for $x = 1$, we could alternatively just compute the kernel of the matrix $x - 1$ by finding the reduced row echelon form and using our column technique for finding the kernel's basis.

If a matrix is *not diagonalizable*, however, method 1 could fail to find a specific eigenspace.

Eigenspaces *can always be found* by method 2.

Theorem 7.4.14

The eigenspace for $x = a$, i.e. the largest subspace whose minimal polynomial is $(x - a)$ is precisely the kernel of the matrix $(x - a)$

Proof. The kernel of $(x - a)$ is the subspace of all vectors v such that $(x - a) \cdot v$ is the zero vector. The minimal polynomial of each of these vectors must then be a factor of $(x - a)$. If the minimal polynomial is a constant, then v is the zero vector, otherwise the minimal polynomial of v is $(x - a)$. Therefore, the collection of all such vectors is the eigenspace of the matrix A for $x = a$. \square

Now we know that method 2 will always work. But what about method 1?

Both methods work as long as the matrix is *diagonalizable*.

We prove that the range method (method 1) will work when our minimal polynomial has the right form for diagonalizability. We need some preliminary ideas to our proof called *lemmas*.

Lemma 7.4.15

Suppose that $a(x)$ shares no common factor other than a constant in \mathbb{R} with the minimal polynomial $p(x)$ of a vector v . Then, the square matrix $a(x)$ when restricted as a function $\mathbb{R}[x] \cdot v \rightarrow \mathbb{R}[x] \cdot v$ is an isomorphism.

Proof. Suppose that $a(x) \cdot w = (\text{zero vector})$ for $w \in \mathbb{R}[x] \cdot v$. Then both $p(x)$ and $a(x)$ are zero scalars on w . This means that their greatest common factor, which is 1, is also a zero scalar. This forces w to be the zero vector. This means that the kernel of the matrix representing $a(x)$ has dimension 0. In this restriction, the domain and the codomain are the same and the dimension of the range added to the dimension of the kernel always equals the dimension of the domain—and in this case the codomain. Hence, this restricted linear transformation is surjective. With a zero kernel, it is also injective. \square

Lemma 7.4.16

Suppose that \mathbb{R}^n is formed from subspaces $\mathbb{R}[x] \cdot v_1, \dots, \mathbb{R}[x] \cdot v_k$ which are linear independent to each other. A way of notating this idea is:

$$\mathbb{R}[x] \cdot v_1 \bigoplus \mathbb{R}[x] \cdot v_2 \bigoplus \cdots \bigoplus \mathbb{R}[x] \cdot v_k$$

Then take any $a(x) \in \mathbb{R}[x]$ and think of it as a matrix function. Then,

$$\ker a(x) =$$

$$(\ker a(x) \text{ just on } \mathbb{R}[x] \cdot v_1) \bigoplus (\ker a(x) \text{ just on } \mathbb{R}[x] \cdot v_2) \bigoplus \cdots \bigoplus (\ker a(x) \text{ just on } \mathbb{R}[x] \cdot v_k)$$

Proof. Notice that each of the subspaces $\mathbb{R}[x] \cdot v_j$ are closed under polynomial scalar action. By linear independence, the only way to get the zero vector is to get it on each component. (Otherwise we would have a sum of nonzero linearly independent vectors equalling the zero vector.) \square

Theorem 7.4.17

Suppose that the minimal polynomial of a square $n \times n$ matrix A is

$$m(x) = (x - a_1)(x - a_2) \cdots (x - a_k)$$

where $a_i \neq a_j$ for $i \neq j$. Then the eigenspace for $x = a_1$ is the range of the matrix $(x - a_2) \cdots (x - a_k)$.

Proof. We know that through our column process we can find vectors v_1, v_2, \dots, v_r whose $\mathbb{R}[x]$ -span is all of \mathbb{R}^n .

Because of our first lemma above, the range of the map $(x - a_2) \cdots (x - a_k)$ restricted to any of the $\mathbb{R}[x] \cdot v_j$ subspaces is the same as the range of the minimal polynomial of v_j with $(x - a_1)$ missing. This is because the extra factors that are not part of the minimal polynomial on v_j can be ignored: they are isomorphisms which just transfer all of the input right out to the output.

So, let $m_j(x)$ be the minimal polynomial of v_j and let $m_j^*(x)$ be $m_j(x)$ with the factor $(x - a_1)$ missing. We are saying that the range of $m_j^*(x)$ restricted to $\mathbb{R}[x] \cdot v_j \rightarrow \mathbb{R}[x] \cdot v_j$ is the same as the range of $(x - a_2) \cdots (x - a_k)$ restricted to $\mathbb{R}[x] \cdot v_j \rightarrow \mathbb{R}[x] \cdot v_j$.

Now, suppose that $w \in \ker(x - a_1)$ where $(x - a_1)$ is restricted to $\mathbb{R}[x] \cdot v_j \rightarrow \mathbb{R}[x] \cdot v_j$. Remember that $w = b(x) \cdot v_j$ for some $b(x)$. So we are saying that $(x - a_1)b(x) \cdot v = (\text{zero vector})$.

By the minimality of $m_j(x)$, $b(x)$ must be a multiple of $m_j^*(x)$. That is, $w \in \text{range } m_j^*(x)$. This means that the kernel of $(x - a_1)$ restricted to $\mathbb{R}[x] \cdot v_j \rightarrow \mathbb{R}[x] \cdot v_j$ is contained in the range of $m_j^*(x)$ restricted to $\mathbb{R}[x] \cdot v_j \rightarrow \mathbb{R}[x] \cdot v_j$.

The range of $m_j^*(x)$ is contained in the kernel of $(x - a_1)$ when we are restricted to $\mathbb{R}[x] \cdot v_j$ since $(x - a_1) \cdot m_j^*(x) \cdot v_j$ always yields $m_j(x) \cdot v_j = (\text{zero vector})$ on our subspace. So this range and our desired kernel are at least equal in the restriction.

Then, by our second lemma, the overall kernel of $(x - a_1)$ is the span of each of these ranges in the various $\mathbb{R}[x] \cdot v_j$. Because any polynomial acting on $\mathbb{R}[x] \cdot v_j$ only outputs things in $\mathbb{R}[x] \cdot v_j$ and these subspaces together span all of \mathbb{R}^n , the span of these ranges is precisely the overall range of the matrix $(x - a_1)(x - a_2) \cdots (x - a_k)$.

So, the kernel of $(x - a_1)$ which is the same as the eigenspace for $x = a_1$ is the same as the range of $(x - a_2) \cdots (x - a_k)$. \square

Here is an example where the range method would fail to find an eigenspace. The matrix is not diagonalizable. Notice the importance in assuming that all of $m_j^*(x)$ in the proof above are restrictions of the *same* polynomial. This may not happen if there is a repeated factor $(x - a)^2$ in the minimal polynomial $m(x)$.

Example 3. The matrix

$$A = \begin{pmatrix} 2 & -1 & 2 \\ 0 & 4 & -4 \\ 0 & 1 & 0 \end{pmatrix}$$

has a minimal polynomial $(x - 1)^2$. We can find this by performing column operations to arrive at:

$$\begin{pmatrix} x - 2 & 1 & 0 \\ 0 & x - 4 & x^2 - 4x + 4 \\ 0 & -1 & 0 \end{pmatrix}$$

$$\underbrace{(x-2)}_{\text{degree 1}} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \underbrace{(1)}_{\text{degree 0}} \cdot \begin{pmatrix} 1 \\ x-4 \\ -1 \end{pmatrix} \quad \underbrace{(x-2)^2}_{\text{degree 2}} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

We desire to find the overall kernel of $(x-2)$ which is the eigenspace for $x = 2$.

- $v_1 = (1, 0, 0)$ has minimal polynomial $m_1 = (x-2)$.
- $v_2 = (0, 1, 0)$ has minimal polynomial $m_2 = (x-2)^2$

On $\mathbb{R}[x] \cdot v_1$, the kernel of $(x-2)$ is the *range of the identity map*—that is everything is in the kernel.

On $\mathbb{R}[x] \cdot v_2$, the kernel of $(x-2)$ is the *range of $(x-2)$* .

The polynomial 1 restricts to the identity map in both (wrong in one subspace and right in the other). The polynomial $(x-2)$ restricts to the zero map in one and just simply $(x-2)$ in the other (wrong in one subspace and right in the other).

There is no polynomial whose range restricts to $\mathbb{R}[x] \cdot v_1$ and $\mathbb{R}[x] \cdot v_2$ in such a way.

7.4.6 Finding Eigenvectors by Ranges



Ranges for Diagonalizing

To diagonalize a matrix A by ranges:

1. Compute the characteristic polynomial. Then, verify that the minimal polynomial does not have any repeated roots. Otherwise, diagonalization is impossible. Remember, if necessary even with non-integers and complex numbers we should be able to get to factored form with only powers of linear factors $(x - a)$.
2. Suppose that the minimal polynomial is $(x - a_1) \cdot (x - a_2) \cdots (x - a_k)$. To find the eigenspace for $x = a_1$, find the matrix $(x - a_2) \cdots (x - a_k)$ and determine a basis for its range (i.e. span of columns). This basis is what eigenvectors will correspond to the eigenvalue $x = a_1$ in the diagonalization process.
3. Repeat this process for each $x = a_j$ by finding a basis for the range of the polynomial that results from removing the factor $(x - a_j)$ from the minimal polynomial. These are the eigenvectors we will use for the eigenvalue $x = a_j$.
4. Form U by lining up all the eigenvectors we have selected as columns. Now:

$$U^{-1} \cdot A \cdot U = \text{Diagonal Matrix}$$

where the columns in U correspond to the columns in the diagonal matrix via an eigenvector/eigenvalue relationship.

Example 4. Let's find a new basis in which the following matrix will become a diagonal one:

$$A = \begin{pmatrix} -4 & -1 \\ 6 & 1 \end{pmatrix}$$

First, we find the characteristic polynomial:

$$\det \begin{pmatrix} x + 4 & 1 \\ -6 & x - 1 \end{pmatrix} = x^2 + 3x + 2 = (x + 1)(x + 2)$$

This characteristic polynomial is the same as the minimal polynomial because it has two distinct factors. Therefore, this matrix is diagonalizable.

Below we use the matrices $(x + 1)$ and $(x + 2)$. Let's go over how we determine the matrix $x + 2$:

$$\underbrace{\begin{pmatrix} -4 & -1 \\ 6 & 1 \end{pmatrix}}_x + \underbrace{\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}}_2 = \underbrace{\begin{pmatrix} -2 & -1 \\ 6 & 3 \end{pmatrix}}_{(x+2)}$$

minimal polynomial: $(x + 2)$

range $\underbrace{\begin{pmatrix} -3 & -1 \\ 6 & 2 \end{pmatrix}}_{(x+1)}$



eigenspace:

$$\langle(-1, 2)\rangle$$

eigenvalue $x = -2$

minimal polynomial: $(x + 1)$

range $\underbrace{\begin{pmatrix} -2 & -1 \\ 6 & 3 \end{pmatrix}}_{(x+2)}$



eigenspace:

$$\langle(-1, 3)\rangle$$

eigenvalue $x = -1$

$$\underbrace{\begin{pmatrix} -3 & -1 \\ 2 & 1 \end{pmatrix}}_{U^{-1}} \cdot \underbrace{\begin{pmatrix} -4 & -1 \\ 6 & 1 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} -1 & -1 \\ 2 & 3 \end{pmatrix}}_U = \underbrace{\begin{pmatrix} -2 & 0 \\ 0 & -1 \end{pmatrix}}_D$$

eigenvector eigenvector eigenvector eigenvector

eigenvalue eigenvalue eigenvalue eigenvalue

Note that each diagonal entry in D is in the column that corresponds to its eigenvector in U .

Example 5. Let's diagonalize the matrix

$$A = \begin{pmatrix} -1 & -2 & -10 \\ 1 & 1 & 5 \\ 0 & 1 & 1 \end{pmatrix}$$

First we compute its characteristic polynomial as $(x-2) \cdot (x-1) \cdot (x+2)$ which *must* be the minimal polynomial as well since all the factors are distinct.

Eigenspace $x = 2$: We find the range of

$$\underbrace{\begin{pmatrix} -2 & -2 & -10 \\ 1 & 0 & 5 \\ 0 & 1 & 0 \end{pmatrix}}_{x-1} \cdot \underbrace{\begin{pmatrix} 1 & -2 & -10 \\ 1 & 3 & 5 \\ 0 & 1 & 3 \end{pmatrix}}_{x+2} = \begin{pmatrix} -4 & -12 & -20 \\ 1 & 3 & 5 \\ 1 & 3 & 5 \end{pmatrix}$$

The span of the columns is $\langle (-4, 1, 1) \rangle$.

For the eigenvalue $x = 2$, we have the eigenvector $(-4, 1, 1)$ whose span is the whole eigenspace.

Eigenspace $x = 1$: We find the range of

$$\underbrace{\begin{pmatrix} -3 & -2 & -10 \\ 1 & -1 & 5 \\ 0 & 1 & -1 \end{pmatrix}}_{x-2} \cdot \underbrace{\begin{pmatrix} 1 & -2 & -10 \\ 1 & 3 & 5 \\ 0 & 1 & 3 \end{pmatrix}}_{x+2} = \begin{pmatrix} -5 & -10 & -10 \\ 0 & 0 & 0 \\ 1 & 2 & 2 \end{pmatrix}$$

The span of the columns is $\langle (-5, 0, 1) \rangle$

For the eigenvalue $x = 1$, we have the eigenvector $(-5, 0, 1)$ whose span is the whole eigenspace.

Eigenspace $x = -2$: We find the range of

$$\underbrace{\begin{pmatrix} -3 & -2 & -10 \\ 1 & -1 & 5 \\ 0 & 1 & -1 \end{pmatrix}}_{x-2} \cdot \underbrace{\begin{pmatrix} -2 & -2 & -10 \\ 1 & 0 & 5 \\ 0 & 1 & 0 \end{pmatrix}}_{x-1} = \begin{pmatrix} 4 & -4 & 20 \\ -3 & 3 & -15 \\ 1 & -1 & 5 \end{pmatrix}$$

The span of the columns is $\langle (4, -3, 1) \rangle$

For the eigenvalue $x = 1$, we have the eigenvector $(4, -3, 1)$ whose span is the whole eigenspace.

Making our matrix U out of our chosen eigenvectors, we have:

$$\underbrace{\begin{pmatrix} \frac{1}{4} & \frac{3}{4} & \frac{5}{4} \\ -\frac{1}{3} & -\frac{2}{3} & -\frac{2}{3} \\ \frac{1}{12} & -\frac{1}{12} & \frac{5}{12} \end{pmatrix}}_{U^{-1}} \cdot \underbrace{\begin{pmatrix} -1 & -2 & -10 \\ 1 & 1 & 5 \\ 0 & 1 & 1 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} -4 & -5 & 4 \\ 1 & 0 & -3 \\ 1 & 1 & 1 \end{pmatrix}}_U = \underbrace{\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}}_D$$

Choosing Eigenvectors

Really, in the diagonalization process, choose *any* eigenvectors that span the appropriate eigenspace.

Example 6. Consider the matrix:

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

Its characteristic polynomial is $(x - 1) \cdot (x - 2)^2$. If this were also its minimal polynomial, then the matrix would not be diagonalizable. But one can check that $(x - 1) \cdot (x - 2)$ is the zero matrix so that the minimal polynomial is $(x - 1) \cdot (x - 2)$. Therefore, this matrix is diagonalizable.

Eigenspace $x = 1$: We find the range of

$$\underbrace{\begin{pmatrix} -3 & -6 & -3 \\ 1 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix}}_{x=2}$$

The span of the columns is $\langle (-3, 1, 0) \rangle$

For the eigenvalue $x = 1$, we have the eigenvector $(-3, 1, 0)$ whose span is the whole eigenspace.

Eigenspace $x = 2$: We find the range of

$$\underbrace{\begin{pmatrix} -2 & -6 & -3 \\ 1 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{x=1}$$

The span of the columns is $\langle (-2, 1, 0), (-3, 1, 1) \rangle$

For the eigenvalue $x = 1$, we have the eigenvectors $(-2, 1, 0)$ and $(-3, 1, 1)$ which forms a basis for the eigenspace.

Making our matrix U out of our chosen eigenvectors, we have:

$$\underbrace{\begin{pmatrix} -1 & -2 & -1 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{U^{-1}} \cdot \underbrace{\begin{pmatrix} -1 & -6 & -3 \\ 1 & 4 & 1 \\ 0 & 0 & 2 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} -3 & -2 & -3 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_U = \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}}_D$$

7.4.7 Finding Eigenvectors by Kernels

Kernels for Diagonalization

To diagonalize a matrix by kernels:

1. Compute the characteristic polynomial. Then, verify that the minimal polynomial does not have any repeated roots. Otherwise, diagonalization is impossible. Remember, if necessary even with non-integers and complex numbers we should be able to get to factored form with only powers of linear factors $(x - a)$.
2. To find a basis of eigenvectors for the eigenspace corresponding to the eigenvalue $x = a$, simply find the kernel of the matrix $(x - a)$
3. Form U by lining up all the eigenvectors we have selected as columns. Now:

$$U^{-1} \cdot A \cdot U = \text{Diagonal Matrix}$$

where the columns in U correspond to the columns in the diagonal matrix via an eigenvector/eigenvalue relationship.

Example 7. We diagonalized the following matrix by ranges. But now, let's use kernels.

$$A = \begin{pmatrix} -1 & -2 & -10 \\ 1 & 1 & 5 \\ 0 & 1 & 1 \end{pmatrix}$$

Both the characteristic and the minimal polynomial of this matrix is $(x - 2) \cdot (x - 1) \cdot (x + 2)$.

Eigenspace $x = 2$: We find the kernel of $(x - 2)$ by computing reduced row echelon form (rref) and then using our column trick.

$$\underbrace{\begin{pmatrix} -3 & -2 & -10 \\ 1 & -1 & 5 \\ 0 & 1 & -1 \end{pmatrix}}_{x-2} \xrightarrow{\text{rref}} \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\text{column trick}} \begin{pmatrix} -4 \\ 1 \\ 1 \end{pmatrix}$$

For the eigenvalue $x = 2$, we have the eigenvector $(-4, 1, 1)$ forming a basis for the eigenspace.

Eigenspace $x = 1$: We find the kernel of $(x - 1)$ by computing reduced row echelon form (rref) and then using our column trick.

$$\underbrace{\begin{pmatrix} -2 & -2 & -10 \\ 1 & 0 & 5 \\ 0 & 1 & 0 \end{pmatrix}}_{x-1} \xrightarrow{\text{rref}} \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\text{column trick}} \begin{pmatrix} -5 \\ 0 \\ 1 \end{pmatrix}$$

For the eigenvalue $x = 1$, we have the eigenvector $(-5, 0, 1)$ forming a basis for the eigenspace.

Eigenspace $x = -2$: We find the kernel of $(x + 2)$ by computing reduced row echelon form (rref) and then using our column trick.

$$\underbrace{\begin{pmatrix} 1 & -2 & -10 \\ 1 & 3 & 5 \\ 0 & 1 & 3 \end{pmatrix}}_{x+2} \xrightarrow{\text{rref}} \begin{pmatrix} 1 & 0 & -4 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\text{column trick}} \begin{pmatrix} 4 \\ -3 \\ 1 \end{pmatrix}$$

For the eigenvalue $x = -2$, we have the eigenvector $(4, -3, 1)$ forming a basis for the eigenspace.

Again, as we had above, the following matrix U , which lines up all of our selected eigenvectors, makes $U^{-1}AU$

a diagonal matrix:

$$U = \begin{pmatrix} -4 & -5 & 4 \\ 1 & 0 & -3 \\ 1 & 1 & 1 \end{pmatrix}$$

Example 8. We diagonalized the following matrix by ranges. But now, let's use kernels.

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

We found that its characteristic polynomial was $(x - 1) \cdot (x - 2)^2$ and that its minimal polynomial was $(x - 1) \cdot (x - 2)$.

Eigenspace $x = 1$: We find the kernel of $(x - 1)$ by computing reduced row echelon form (rref) and then using our column trick:

$$\underbrace{\begin{pmatrix} -2 & -6 & -3 \\ 1 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{x-1} \xrightarrow{\text{rref}} \begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\text{column trick}} \begin{pmatrix} -3 \\ 1 \\ 0 \end{pmatrix}$$

For the eigenvalue $x = 1$, we have the eigenvector $(-3, 1, 0)$ forming a basis for the eigenspace.

Eigenspace $x = 2$: We find the kernel of $(x - 2)$ by computing reduced row echelon form (rref) and then using our column trick:

$$\underbrace{\begin{pmatrix} -3 & -6 & -3 \\ 1 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix}}_{x-1} \xrightarrow{\text{rref}} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\text{column trick}} \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$$

For the eigenvalue $x = 2$, we have the eigenvectors $(-2, 1, 0)$ and $(-1, 0, 1)$ forming a basis for the eigenspace.

Notice that when we used ranges, we had $(-2, 1, 0)$ and $(-3, 1, 1)$. But this is ok since $(-3, 1, 1) = (-2, 1, 0) + (-1, 0, 1)$ and:

$$\langle (-2, 1, 0), (-1, 0, 1) \rangle = \langle (-2, 1, 0), (-3, 1, 1) \rangle$$

All we need is a basis for the eigenspace. Any basis would do! With the eigenvectors that we have selected, the matrix U is:

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

This matrix U causes $U^{-1}AU$ to be a diagonal matrix.

7.4.8 Powers of a matrix

We can easily take powers of a matrix that we can diagonalize.

Example 9. Suppose that we would like to compute

$$\begin{pmatrix} -4 & -1 \\ 6 & 1 \end{pmatrix}^8$$

In an earlier example in this section, we found that:

$$\underbrace{\begin{pmatrix} -3 & -1 \\ 2 & 1 \end{pmatrix}}_{U^{-1}} \cdot \underbrace{\begin{pmatrix} -4 & -1 \\ 6 & 1 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} -1 & -1 \\ 2 & 3 \end{pmatrix}}_U = \underbrace{\begin{pmatrix} -2 & 0 \\ 0 & -1 \end{pmatrix}}_D$$

We could write:

$$\underbrace{\begin{pmatrix} -4 & -1 \\ 6 & 1 \end{pmatrix}}_A = \underbrace{\begin{pmatrix} -1 & -1 \\ 2 & 3 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} -2 & 0 \\ 0 & -1 \end{pmatrix}}_D \cdot \underbrace{\begin{pmatrix} -3 & -1 \\ 2 & 1 \end{pmatrix}}_{U^{-1}}$$

Notice that

$$A^2 = (UDU^{-1}) \cdot (UDU^{-1}) = UDU \underbrace{U^{-1}U}_{\text{id}} DU^{-1} = UD^2U^{-1}$$

Similarly,

$$A^8 = UD^8U^{-1}$$

So the only question is how to compute D^8 . Multiplication of diagonal matrices is easy! We just multiply the corresponding diagonal entries so that:

$$D^8 = \begin{pmatrix} (-2)^8 & 0 \\ 0 & (-1)^8 \end{pmatrix} = \begin{pmatrix} 256 & 0 \\ 0 & 1 \end{pmatrix}$$

Hence,

$$A^8 = \underbrace{\begin{pmatrix} -1 & -1 \\ 2 & 3 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} 256 & 0 \\ 0 & 1 \end{pmatrix}}_{D^8} \cdot \underbrace{\begin{pmatrix} -3 & -1 \\ 2 & 1 \end{pmatrix}}_{U^{-1}}$$

$$A^8 = \begin{pmatrix} 766 & 255 \\ -1530 & -509 \end{pmatrix}$$

7.4.9 Diagonalizing by Roots

Often the characteristic polynomial does not factor so nicely. Yet even if we can find a list of the roots of the characteristic polynomial via technology, we are in good shape. If the list of *distinct* roots is r_1, r_2, \dots, r_n where we have eliminated any repeats, then *if the matrix is diagonalizable*, the minimal polynomial will be:

$$(x - r_1) \cdot (x - r_2) \cdots (x - r_n)$$

Then, we could proceed by diagonalization by kernels or ranges as we have done previously. To experiment with this idea, see the SageMath activity: 

Key Concepts from this Section

- **eigenspace:** (page 874) Let x denote the action of a square matrix A on a vector space V . Let W be the \mathbb{R} -span of all vectors $w \in V$ such that the minimal polynomial on $\langle w \rangle$ is a degree one polynomial $(x - a)$. Then, W is called an *eigenspace* of A .
- **eigenspaces are invariant:** (page 874) Since an eigenspace has a degree 1 minimal polynomial, it automatically is an invariant subspace by a theorem in the last section. That means it is closed with respect to polynomial scalars.
- **eigenvector:** (page 874) An eigenvector is a vector in an eigenspace.
- **eigenvalue:** (page 874) Suppose that the minimal polynomial for an eigenspace is $(x - a)$. Then a is called the eigenvalue for that eigenspace.
- **scalar action on eigenvectors:** (page 874) Let x denote the action of a square matrix A on a vector space and let a be an eigenvalue for A . Then if v is in the eigenspace associated to a , the matrix action x behaves *just like* the scalar action of a :

$$x \cdot v = a \cdot v$$

- **diagonal change of basis:** (page 876) If we can select n linearly independent eigenvectors for a matrix A , then they serve as a basis with which we can diagonalize A . Writing these eigenvectors as the

columns of an unpretending matrix U , we have:

$$U^{-1}AU = D$$

where D is a diagonal matrix.

- **theorem 7.4.1 :** (page 878) For an invariant subspace W under the action of x , multiplication by x yields a linear transformation $W \rightarrow W$. *It only sends vectors in W to vectors in W .*
- **theorem 7.4.2 :** (page 878) If the minimal polynomial on a subspace W is $(x - 1)(x - 2)$, then the minimal polynomial on $(x - 2) \cdot W$ is $(x - 1)$. This result is easily generalized. One example is if $(x - 1)(x - 2)(x - 3)$ is the minimal polynomial of a subspace H . Then in that case, $(x - 3)$ would be the minimal polynomial of $(x - 1)(x - 2) \cdot H$.
- **theorem 7.4.3 :** (page 878) These two eigenvectors that we have found are linearly independent. We want to show this is true if we only assume they are both nonzero and that one came from $(x - 2) \cdot W$ and the other from $(x - 1) \cdot W$. *The proof given here is via polynomials.*
- **theorem 7.4.4 :** (page 880) If $H = \mathbb{R}[x] \cdot v$ has a minimal polynomial $p(x)$ of degree n and $b(x)$ is a degree m factor of $p(x)$, then the dimension of $b(x) \cdot H$ is

$$\deg \frac{p(x)}{b(x)} = n - m$$

The minimal polynomial of $b(x) \cdot H$ is

$$\frac{p(x)}{b(x)}$$

- **corollary 7.4.5 :** (page 880) Let $W = \frac{p(x)}{x - a} \cdot H$. Then $\dim W = 1$.
- **theorem 7.4.6 :** (page 880) The only vectors in $H = \mathbb{R}[x] \cdot v$ with a minimal polynomial of $(x - a)$ are those in $W = \frac{p(x)}{x - a} \cdot H$.
- **theorem 7.4.7 :** (page 881) Now, if w has a minimal polynomial such that one of its factors is different from the factors of any of the minimal polynomials of the vectors in a linearly independent list $\{w_1, w_2, \dots, w_m\}$, then extending the collection to $\{w, w_1, w_2, \dots, w_m\}$ is again a linearly independent collection.
- **corollary 7.4.8 :** (page 881) Let $(x - a_1), (x - a_2), \dots, (x - a_k)$ be the distinct linear factors of $p(x)$ where $p(x)$ is the minimal polynomial of a vector v . Let w_i be a nonzero vector in the one-dimensional space $\frac{p(x)}{(x - a_i)} \cdot v$. Then, the collection $\{w_1, \dots, w_k\}$ is linearly independent.
- **theorem 7.4.9 :** (page 882) The only way to get k linearly independent eigenvectors in $H = \mathbb{R}[x] \cdot v$ is for there to be k distinct linear factors $(x - a)$ of the minimal polynomial $p(x)$ of $\langle v \rangle$ (which is the same as the minimal polynomial of H).

- **theorem 7.4.10 :** (page 882) The only way for $(x - a)^2$ to be a factor of $m(x)$ is for $(x - a)^2$ to be a factor of the minimal polynomial $p(x)$ of one of the subspaces $\mathbb{R}[x] \cdot v$.
- **theorem 7.4.11 :** (page 882) As long as $m(x)$...
 - is completely factorable into linear factors $(x - a)$
 - has no factors of the form $(x - a)^2$

then we can find the right number of linearly independent eigenvectors to diagonalize the matrix.

- **theorem 7.4.12 :** (page 883) Each $\mathbb{R}[x] \cdot$ (vector) subspace contributes *only one* dimension at most to each eigenspace.
- **theorem 7.4.13 :** (page 883) The characteristic polynomial and the minimal polynomials are exactly the same when the characteristic polynomial is factorable into *only* nonrepeating linear factors $(x - a)$.
- **eigenvectors for diagonalization:** (page 884) In the *diagonalization* process we could use either of the following two methods:
 - To find our eigenvectors we can look at the ranges of factors of the minimal polynomial. That is, the span of the columns of the matrix. For instance, if the minimal polynomial is $(x - 1)(x + 5)$, the range (the column span) of the matrix $(x + 5)$ gives all of the eigenvectors for $x = 1$. We will see more of this as we actually work through examples.
 - To find our eigenvectors for $x = 1$, we could alternatively just compute the kernel of the matrix $x - 1$ by finding the reduced row echelon form and using our column technique for finding the kernel's basis.
- **theorem 7.4.14 :** (page 884) The eigenspace for $x = a$, i.e. the largest subspace whose minimal polynomial is $(x - a)$ is precisely the kernel of the matrix $(x - a)$
- **lemma 7.4.15 :** (page 884) Suppose that $a(x)$ shares no common factor other than a constant in \mathbb{R} with the minimal polynomial $p(x)$ of a vector v . Then, the square matrix $a(x)$ when restricted as a function $\mathbb{R}[x] \cdot v \rightarrow \mathbb{R}[x] \cdot v$ is an isomorphism.
- **lemma 7.4.16 :** (page 885) Suppose that \mathbb{R}^n is formed from subspaces $\mathbb{R}[x] \cdot v_1, \dots, \mathbb{R}[x] \cdot v_k$ which are linear independent to each other. A way of notating this idea is:

$$\mathbb{R}[x] \cdot v_1 \bigoplus \mathbb{R}[x] \cdot v_2 \bigoplus \cdots \bigoplus \mathbb{R}[x] \cdot v_k$$

Then take any $a(x) \in \mathbb{R}[x]$ and think of it as a matrix function. Then,

$$\ker a(x) =$$

$$(\ker a(x) \text{ just on } \mathbb{R}[x] \cdot v_1) \bigoplus (\ker a(x) \text{ just on } \mathbb{R}[x] \cdot v_2) \bigoplus \cdots \bigoplus (\ker a(x) \text{ just on } \mathbb{R}[x] \cdot v_k)$$

- **theorem 7.4.17 :** (page 885) Suppose that the minimal polynomial of a square $n \times n$ matrix A is

$$m(x) = (x - a_1)(x - a_2) \cdots (x - a_k)$$

where $a_i \neq a_j$ for $i \neq j$. Then the eigenspace for $x = a_1$ is the range of the matrix $(x - a_2) \cdots (x - a_k)$.

- **ranges for diagonalizing:** (page 887) To diagonalize a matrix A by ranges:

1. Compute the characteristic polynomial. *Then, verify that the minimal polynomial does not have any repeated roots. Otherwise, diagonalization is impossible.* Remember, if necessary even with non-integers and complex numbers we should be able to get to factored form with only powers of linear factors $(x - a)$.
2. Suppose that the minimal polynomial is $(x - a_1) \cdot (x - a_2) \cdots (x - a_k)$. To find the eigenspace for $x = a_1$, find the matrix $(x - a_2) \cdots (x - a_k)$ and determine a basis for its range (i.e. span of columns). This basis is what eigenvectors will correspond to the eigenvalue $x = a_1$ in the diagonalization process.
3. Repeat this process for each $x = a_j$ by finding a basis for the range of the polynomial that results from removing the factor $(x - a_j)$ from the minimal polynomial. These are the eigenvectors we will use for the eigenvalue $x = a_j$.
4. Form U by lining up all the eigenvectors we have selected as columns. Now:

$$U^{-1} \cdot A \cdot U = \text{Diagonal Matrix}$$

where the columns in U correspond to the columns in the diagonal matrix via an eigenvector/eigenvalue relationship.

- **choosing eigenvectors:** (page 891) Really, in the diagonalization process, choose *any* eigenvectors that span the appropriate eigenspace.
- **kernels for diagonalization:** (page 892) To diagonalize a matrix by kernels:

1. Compute the characteristic polynomial. *Then, verify that the minimal polynomial does not have any repeated roots. Otherwise, diagonalization is impossible.* Remember, if necessary even with non-integers and complex numbers we should be able to get to factored form with only powers of linear factors $(x - a)$.
2. To find a basis of eigenvectors for the eigenspace corresponding to the eigenvalue $x = a$, simply find the kernel of the matrix $(x - a)$
3. Form U by lining up all the eigenvectors we have selected as columns. Now:

$$U^{-1} \cdot A \cdot U = \text{Diagonal Matrix}$$

where the columns in U correspond to the columns in the diagonal matrix via an eigenvector/eigenvalue relationship.

7.4.10 Exercises

Diagonalizing 2×2 matrices

Write an equation that expresses the diagonalization of the following matrices.

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

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

$$3. \begin{pmatrix} -1 & -1 \\ -3 & 1 \end{pmatrix}$$

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

$$5. \begin{pmatrix} 8 & -15 \\ 6 & -11 \end{pmatrix}$$

$$6. \begin{pmatrix} 1 & -1 \\ -3 & -1 \end{pmatrix}$$

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

$$8. \begin{pmatrix} -2 & -3 \\ 0 & -1 \end{pmatrix}$$

$$9. \begin{pmatrix} -8 & -15 \\ 6 & 11 \end{pmatrix}$$

$$10. \begin{pmatrix} -2 & -1 \\ 2 & 1 \end{pmatrix}$$

$$11. \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$12. \begin{pmatrix} -2 & -3 \\ 0 & -1 \end{pmatrix}$$

$$13. \begin{pmatrix} -2 & -1 \\ 2 & 1 \end{pmatrix}$$

$$14. \begin{pmatrix} 0 & -1 \\ -2 & -1 \end{pmatrix}$$

$$15. \begin{pmatrix} 0 & -1 \\ -2 & 1 \end{pmatrix}$$

$$16. \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}$$

Diagonalizing using Ranges and Kernels

For each of the following matrices A , find D and P such that $D = U^{-1}AU\ldots$

(a) by using ranges

(b) by using kernels

The minimal polynomials of the following have 2 factors.

$$17. \begin{pmatrix} 2 & 1 & -2 \\ 0 & 0 & 4 \\ 0 & 1 & 0 \end{pmatrix}$$

$$18. \begin{pmatrix} -1 & -2 & 4 \\ 0 & 0 & -2 \\ 0 & 1 & -3 \end{pmatrix}$$

$$19. \begin{pmatrix} 1 & 3 & -1 \\ 1 & -1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

$$20. \begin{pmatrix} 0 & -1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

$$21. \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$22. \begin{pmatrix} 1 & -6 & -3 \\ 1 & -4 & -1 \\ 0 & 0 & -2 \end{pmatrix}$$

$$23. \begin{pmatrix} -1 & -6 & -2 \\ 1 & 4 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$24. \begin{pmatrix} -1 & 0 & 0 \\ 1 & -2 & -1 \\ 0 & 0 & -1 \end{pmatrix}$$

$$25. \begin{pmatrix} -1 & -2 & 4 \\ 0 & 0 & -2 \\ 0 & 1 & -3 \end{pmatrix}$$

$$26. \begin{pmatrix} 2 & -1 & 1 \\ 0 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}$$

The minimal polynomials of the following have 3 factors.

$$27. \begin{pmatrix} -1 & -2 & 4 \\ 1 & 1 & -1 \\ 0 & 1 & -3 \end{pmatrix}$$

$$28. \begin{pmatrix} -1 & -2 & -2 \\ 1 & 1 & -1 \\ 0 & 1 & 3 \end{pmatrix}$$

29. $\begin{pmatrix} -1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$

30. $\begin{pmatrix} -1 & -2 & -4 \\ 1 & 1 & 3 \\ 0 & 1 & 1 \end{pmatrix}$

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

32. $\begin{pmatrix} 1 & -2 & -2 \\ 1 & -1 & 2 \\ 0 & 1 & 2 \end{pmatrix}$

33. $\begin{pmatrix} -1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & -2 \end{pmatrix}$

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

35. $\begin{pmatrix} 1 & 0 & 6 \\ 1 & -1 & 3 \\ 0 & 1 & -1 \end{pmatrix}$

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

Powers of a Matrix

Use the diagonalization of the matrix in order to find the power of the matrix.

37. $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}^5$

38. $\begin{pmatrix} -1 & 3 \\ -1 & 3 \end{pmatrix}^4$

39. $\begin{pmatrix} -2 & -3 \\ 0 & -1 \end{pmatrix}^5$

40. $\begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}^5$

41. $\begin{pmatrix} 8 & -15 \\ 6 & -11 \end{pmatrix}^4$

42. $\begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}^6$

43. $\begin{pmatrix} 2 & 5 \\ 0 & -1 \end{pmatrix}^6$

44. $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}^5$

$$\mathbf{45.} \begin{pmatrix} -1 & 3 \\ 0 & 1 \end{pmatrix}^7$$

$$\mathbf{46.} \begin{pmatrix} 3 & -5 \\ 3 & -5 \end{pmatrix}^7$$

$$\mathbf{47.} \begin{pmatrix} -1 & 3 \\ -1 & 3 \end{pmatrix}^5$$

$$\mathbf{48.} \begin{pmatrix} -3 & -1 \\ 3 & 1 \end{pmatrix}^4$$

$$\mathbf{49.} \begin{pmatrix} 2 & 5 \\ 0 & -1 \end{pmatrix}^4$$

$$\mathbf{50.} \begin{pmatrix} -2 & -1 \\ 0 & 1 \end{pmatrix}^5$$

$$\mathbf{51.} \begin{pmatrix} -2 & -3 \\ 0 & -1 \end{pmatrix}^5$$

$$\mathbf{52.} \begin{pmatrix} 8 & -15 \\ 6 & -11 \end{pmatrix}^7$$

7.4.11 Solutions

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

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

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

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

5. $\begin{pmatrix} -1 & 0 \\ 0 & -2 \end{pmatrix} =$
 $\begin{pmatrix} 10 & -15 \\ -9 & 15 \end{pmatrix} \begin{pmatrix} 8 & -15 \\ 6 & -11 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \frac{3}{5} & \frac{2}{3} \end{pmatrix}$

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

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

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

9. $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} =$
 $\begin{pmatrix} -9 & -15 \\ 10 & 15 \end{pmatrix} \begin{pmatrix} -8 & -15 \\ 6 & 11 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -\frac{2}{3} & -\frac{3}{5} \end{pmatrix}$

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

11. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} =$
 $\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

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

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

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

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

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

17. $D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} =$
 $U = \begin{pmatrix} 1 & 1 & 0 \\ -2 & 0 & 2 \\ 1 & 0 & 1 \end{pmatrix}$

18. $D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} =$
 $U = \begin{pmatrix} 2 & 1 & 0 \\ -1 & 0 & 2 \\ -1 & 0 & 1 \end{pmatrix}$

19. $D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} =$
 $U = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 3 \end{pmatrix}$

20. $D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} =$
 $U = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 1 \end{pmatrix}$

21. $D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$
 $U = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & -2 \end{pmatrix}$

22. $D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix} =$
 $U = \begin{pmatrix} 3 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & -2 \end{pmatrix}$

$$\mathbf{23.} D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$

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

$$\mathbf{24.} D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} =$$

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

$$\mathbf{25.} D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} =$$

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

$$\mathbf{26.} D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} =$$

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

$$\mathbf{27.} D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} =$$

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

$$\mathbf{28.} D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} =$$

$$U = \begin{pmatrix} 1 & 0 & 4 \\ -2 & -1 & -3 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{29.} D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$U = \begin{pmatrix} 6 & 0 & 0 \\ -3 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{30.} D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix} =$$

$$U = \begin{pmatrix} -2 & 1 & -2 \\ -1 & -2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{31.} D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix} =$$

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

$$\mathbf{32.} D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix} =$$

$$U = \begin{pmatrix} -4 & -2 & -2 \\ -1 & -3 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{33.} D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \\ U = \begin{pmatrix} 0 & 0 & -2 \\ 3 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{34.} D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix} = \\ U = \begin{pmatrix} 1 & 4 & 0 \\ -2 & -3 & -1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{35.} D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \\ U = \begin{pmatrix} 6 & -2 & -3 \\ 3 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{36.} D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \\ U = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{37.} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{38.} \begin{pmatrix} -8 & 24 \\ -8 & 24 \end{pmatrix}$$

$$\mathbf{39.} \begin{pmatrix} -32 & -93 \\ 0 & -1 \end{pmatrix}$$

$$\mathbf{40.} \begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}$$

$$\mathbf{41.} \begin{pmatrix} -134 & 225 \\ -90 & 151 \end{pmatrix}$$

$$\mathbf{42.} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{43.} \begin{pmatrix} 64 & 105 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{44.} \begin{pmatrix} 16 & -16 \\ -16 & 16 \end{pmatrix}$$

$$\mathbf{45.} \begin{pmatrix} -1 & 3 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{46.} \begin{pmatrix} 192 & -320 \\ 192 & -320 \end{pmatrix}$$

$$\mathbf{47.} \begin{pmatrix} -16 & 48 \\ -16 & 48 \end{pmatrix}$$

$$\mathbf{48.} \begin{pmatrix} 24 & 8 \\ -24 & -8 \end{pmatrix}$$

$$\mathbf{49.} \begin{pmatrix} 16 & 25 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{50.} \begin{pmatrix} -32 & -11 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{51.} \begin{pmatrix} -32 & -93 \\ 0 & -1 \end{pmatrix}$$

$$\mathbf{52.} \begin{pmatrix} 1142 & -1905 \\ 762 & -1271 \end{pmatrix}$$

Symmetric Matrices and Applications

7.5

7.5.1 Symmetric Matrices are Diagonalizable	911
7.5.2 Orthogonality Between Eigenspaces	915
7.5.3 Orthogonal Diagonalization Reveals Rotations	919
7.5.4 Positive Definite Symmetric Matrices	923
7.5.5 Optimization	926
7.5.6 Finding the Center of a Rotated Ellipse	929
7.5.7 Diagonalizing a Trilinear Form	931
7.5.8 Revisiting Least Squares with a Pseudo Inverse	934
7.5.9 Exercises	944
7.5.10 Solutions	948

Questions to Guide Your Study:

- Why are symmetric matrices diagonalizable?
- Why are eigenspaces for different eigenvalues of a symmetric matrix orthogonal to each other? How can we use this fact?
- What does it mean for a symmetric matrix to be orthogonally diagonalizable?
- How can you use an orthogonal diagonalization to determine the angle that a graph has been rotated by if the rotated equation is given?
- How do we determine if a matrix is positive definite?
- How can we determine if a critical point of a multivariable function represents a maximum or a minimum?
- How can we find the center of a rotated and shifted ellipse if the equation which represents this rotation and shift is given?
- How can we think of what it means to diagonalize a trilinear form?
- What does it mean to take a psuedo inverse and how does this give us more flexibility in curve fitting?

7.5.1 Symmetric Matrices are Diagonalizable

We discuss some ideas about symmetric matrices that will help us see that all symmetric matrices are diagonalizable.

Think about the variable “ x ” as a symmetric matrix. Then,

$$(x^2 - 3x + 1)^T = (x \cdot x)^T - 3x^T + 1 = (x^T \cdot x^T) - 3x^T + 1$$

Now, since $x^T = x$, this is the same as $x^2 - 3x + 1$. That is,

$$(x^2 - 3x + 1)^T = (x^2 - 3x + 1)$$

is a symmetric matrix.

Theorem 7.5.1

Any polynomial where x represents a symmetric matrix again represents a symmetric matrix

Consider the symmetric matrix

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

Let x represent A and the matrix indicated by the polynomial $(x - 2)^2$:

$$\underbrace{\begin{pmatrix} -2 & 2 \\ 2 & -2 \end{pmatrix}}_{x-2}^2 = \underbrace{\begin{pmatrix} 4 & -4 \\ -4 & 4 \end{pmatrix}}_{(x-2)^2}$$

Let $v = (1, 1)$. Then clearly,

$$(x - 2)^2 \cdot v = \begin{pmatrix} 4 & -4 \\ -4 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Let M be the matrix representing $x - 2$. Then, we are saying that:

$$\underbrace{\begin{matrix} M \\ = M^T \end{matrix}}_{\substack{M \\ = M^T}} \cdot M \cdot v = (\text{zero vector})$$

Using the fact that M is symmetric, $M = M^T$. Now let's multiply by v^T on the left of both sides:

$$\underbrace{v^T \cdot M^T}_{(Mv)^T} \cdot M \cdot v = v^T \cdot (\text{zero vector}) = (\text{zero vector})$$

This is the same as the dot product:

$$\underbrace{(Mv) \bullet (Mv)}_{|Mv|} = (\text{zero vector})$$

So we are saying that the length of the vector Mv is zero. This can only happen if Mv is itself the zero vector. Sure enough:

$$\underbrace{\begin{matrix} -2 & 2 \\ 2 & -2 \end{matrix}}_{x-2} \cdot \underbrace{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}_v = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

It is true in general if a power of a symmetric matrix acting on a vector yields the zero vector, then so does the symmetric matrix itself.

Theorem 7.5.2

The minimal polynomial of a symmetric matrix cannot have any repeated linear factors.

Proof. Assume that x represents a symmetric matrix A . Then $(x - a)$ also represents a symmetric matrix M . Suppose that $(x - a)^{2n} \cdot v = (\text{zero vector})$ where $n \geq 1$. Then,

$$M^{2n} \cdot v = (\text{zero vector}) \implies v^T \cdot M^{2n} \cdot v = (\text{zero vector})$$

We can rewrite this as:

$$\underbrace{v^T \cdot M^n M^n \cdot v}_{v^T (M^n)^T} = (\text{zero vector})$$

Since M and hence M^n is symmetric (i.e. $(M \cdot M)^T = M^T \cdot M^T = M \cdot M$), we have that $(M^n)^T = M^n$ as indicated. We can write

$$v^T M^n = v^T (M^n)^T = (M^n v)^T$$

Hence:

$$(M^n v)^T (M^n \cdot v) = (\text{zero vector}) \implies (M^n \cdot v) \bullet (M^n \cdot v) = (\text{zero vector})$$

That is, the square of the length of $M^n \cdot v$ is 0. Hence,

$$(M^n \cdot v) = (\text{zero vector})$$

Now if $(x - a)^m \cdot v = (\text{zero vector})$, we can take 2^t to be the smallest power of 2 higher than m and $(x - a)^{2^t} \cdot v = (\text{zero vector})$. What we just shows now means that $(x - a)^{2^{t-1}} \cdot v = (\text{zero vector})$ since if $n = 2^{t-1}$, then $2n = 2^t$. Continuing this process we can down to $t = 1$, we get that $(x - a) \cdot v = (\text{zero vector})$.

If there were a factor $(x - a)^k$ where $k > 1$ in the minimal polynomial of A , then on an invariant subspace $\mathbb{R}[x] \cdot w$ for some w , any nonzero vector in the range of the polynomial resulting from removing all $(x - a)$ factors from the minimal polynomial of w must have $(x - a)^k$ as its minimal polynomial. Yet we have just shown that this is impossible. The minimum k that gives zero is 1. \square

As long as we know that the characteristic (and hence the minimal) polynomial of a symmetric matrix A completely breaks down to linear factors $(x - a)$ where $a \in \mathbb{R}$, then we know that we can diagonalize A only using real numbers.

It is true that:

Fundamental Theorem of Algebra

Any polynomial of degree n can be completely factored into n linear factors, not necessarily distinct, over the complex numbers. That is, each factor $(x - a)$ has $a \in \mathbb{C}$.

But we need this factorization to be over the *real numbers* for a symmetric matrix.

We now will take care of this idea by showing that symmetric matrices only have real eigenvalues. First, we provide a preliminary result about complex conjugates.

Complex Conjugate

Given a complex number $q + ri$. Its complex conjugate is given by changing the sign of the imaginary part: $q - ri$. The notation for taking a complex conjugate is by using a line over the complex number:

$$\overline{q + ri} = q - ri$$

If B is a matrix or a vector, we can write \overline{B} to signify we are taking the complex conjugate of each entry.

Conjugate Condition for Being Real Number

If $\overline{a} = a$, then $a \in \mathbb{R}$.

Lemma 7.5.3

Given $a, b \in \mathbb{C}$, then

$$\overline{a \cdot b} = \overline{a} \cdot \overline{b}$$

Also, for matrices A and B , we have:

$$\overline{A \cdot B} = \overline{A} \cdot \overline{B}$$

Proof.

$$\underbrace{\overline{q + ri} \cdot \overline{p + ki}}_{a} = \overline{(qp - kr) + (qk + rp)i} = (qp - kr) - (qk + rp)i$$

$$\underbrace{\overline{q + ri} \cdot \overline{p + ki}}_{b} = (q - ri) \cdot (p - ki) = (qp - kr) - (qk + rp)i$$

Since we can define matrix multiplication via multiplication of the entries, the matrix identity also holds. \square

Theorem 7.5.4

Symmetric Matrices only have real eigenvalues.

Proof. Suppose that a is an eigenvalue for the symmetric matrix A which only has entries in \mathbb{R} with an associated eigenvector v . Then, let's consider the following matrix product:

$$\overline{v}^T \underbrace{Av}_{=av}$$

We could write this product as:

$$\overline{v}^T(av) = a(\overline{v} \bullet v)$$

Or, we could have used the fact that $A = A^T$ to have written the product as:

$$\overline{v}^T \underbrace{A^T v}_A = (A\overline{v})^T v$$

Now, using the fact that A only has real entries, $\overline{A} = A$. We also know that $\overline{A\overline{v}} = \overline{Av}$ by noting how complex conjugates split over matrix multiplication. So, we have:

$$(\underbrace{\overline{Av}}_{=\overline{av}})^T v = (\overline{a} \cdot \overline{v}) \bullet v = \overline{a} \cdot (\overline{v} \bullet v)$$

So, we have written *the same* matrix product in two *different* ways:

$$a(\overline{v} \bullet v) = \overline{a} \cdot (\overline{v} \bullet v)$$

This implies that

$$a = \overline{a}$$

so that $a \in \mathbb{R}$.

□

Corollary 7.5.5

Symmetric matrices are diagonalizable.

Results for symmetric matrices come about *because of their symmetry*. This symmetry often leads to two different ways of doing the same thing. The results of doing it either way must be the same.

7.5.2 Orthogonality Between Eigenspaces

Theorem 7.5.6

The Eigenspaces for different eigenvalues for a symmetric matrix are orthogonal to each other.

Proof. Suppose that v is an eigenvector for a symmetric matrix A with associated eigenvalue a . Further suppose that w is an eigenvector for A with associated eigenvalue b and that $a \neq b$. Let's consider the matrix product

$$w^T A v$$

in two different ways. First,

$$w^T A v = w^T (Av) = w^T (av) = a \cdot (w \bullet v)$$

Second,

$$w^T A v = (w^T A)v = (w^T A^T)v = (Aw)^T v = (bw)^T v b \cdot (w \bullet v)$$

Therefore,

$$a \cdot (w \bullet v) = b \cdot (w \bullet v)$$

$$0 = a \cdot (w \bullet v) - b \cdot (w \bullet v) = (a - b) \cdot (w \bullet v)$$

Since $a \neq b$, $(a - b) \neq 0$. Therefore,

$$(w \bullet v) = 0$$

This means that $w \perp v$. □

Since our eigenspaces are orthogonal to each other, if we perform Gram Schmidt within each eigenspace, we can find enough eigenvectors that are orthogonal to each other to diagonalize a symmetric matrix. Not only can we obtain orthogonal eigenvectors, but we can rescale them so that they are an orthonormal collection (i.e. orthogonal all with length 1.)

Orthogonally Diagonalizable

A matrix A is orthogonally diagonalizable if when we diagonalize A as $D = U^{-1}AU$, the matrix U is an orthogonal matrix. That is, the columns of U make up an orthonormal collection of vectors.

Corollary 7.5.7

Symmetric Matrices are orthogonally diagonalizable.

The Inverse of an Orthogonal Matrix

If U is an orthogonal matrix, its inverse is simply U^T . Therefore, $U^T U = \text{id}$.

Orthogonally Diagonalize a Symmetric Matrix

1. Just diagonalize the matrix U . The columns of U that come from different eigenvalues will already be orthogonal.
2. If there are two or more columns that come from the same eigenvalue, apply Gram Schmidt just on those columns from that one eigenvalue.
3. Now, divide each column by its length. The modified U is the one to use!

Eigenbasis

An eigenbasis is a basis for an eigenspace.

When we orthogonally diagonalize a matrix, we are looking for an orthonormal eigenbasis.

Example 1. Suppose that we would like to orthogonally diagonalize the following symmetric matrix:

$$\begin{pmatrix} 3 & 1 & 1 \\ 1 & 3 & 1 \\ 1 & 1 & 3 \end{pmatrix}$$

We compute the characteristic polynomial:

$$x^3 - 9x^2 + 24x - 20 = (x - 2)^2(x - 5)$$

Since our matrix is symmetric, it is diagonalizable so that the minimal polynomial must be $(x - 2)(x - 5)$. We have:

$$(x - 2) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad (x - 5) = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}$$

Since we will be getting exactly three linearly independent eigenvectors from these columns, we take one

column from $x - 2$ and any two from $(x - 5)$ to build the matrix:

$$\begin{pmatrix} 1 & -2 & 1 \\ 1 & 1 & -2 \\ 1 & 1 & 1 \end{pmatrix}$$

The last two columns (which are from $(x - 5)$)

$$\begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

are made zero by $(x - 2)$ so make a eigenbasis for the eigenvalue $x = 2$. These are orthogonal to the first column $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ which is an eigenbasis for $x = 5$. All we need to do to make sure all three columns are orthogonal is to make the two columns associated with the eigenvalue $x = 2$ orthogonal to each other. So we apply Gram Schmidt. We can replace the last column $(1, -2, 1)$ with

$$(1, -2, 1) - \underbrace{\frac{(1, -2, 1) \bullet (-2, 1, 1)}{(-2, 1, 1) \bullet (-2, 1, 1)} (-2, 1, 1)}_{-\frac{1}{2}} = \left(0, -\frac{3}{2}, \frac{3}{2}\right) \xrightarrow{\text{rescale}} (0, -1, 1)$$

Now the columns of the following matrix are all orthogonal to each other and are all eigenvectors:

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

To make this an orthogonal matrix, we divide each column by its length:

$$U = \begin{pmatrix} \frac{1}{\sqrt{3}} & -\frac{2}{\sqrt{6}} & 0 \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

Now since $U^{-1} = U^T$, we have:

$$U^T A U = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

7.5.3 Orthogonal Diagonalization Reveals Rotations

Rotation Matrices are Orthogonal

Sometimes the matrix U signifies rotation on the plane. Then, U is an orthogonal matrix: rotating e_1 and e_2 which are already orthogonal produces two vectors which are still orthogonal to each other and each of length 1.

Example 2. Suppose that we have the equation

$$5x^2 + 6xy + 5y^2 = 8$$

This is the equation of a *rotated* ellipse. We want to determine what the rotation is. First, we write the equation in terms of a *symmetric* bilinear transformation (representable as a symmetric matrix). This can be done via differentiation as shown in section 6.4. Or, *one can proceed by inspection* to have:

$$(x \ y) \cdot \underbrace{\begin{pmatrix} 5 & 3 \\ 3 & 5 \end{pmatrix}}_A \cdot \begin{pmatrix} x \\ y \end{pmatrix} = 8$$

Orthogonally diagonalizing the matrix A will reveal the rotation that was made.

So, we want to diagonalize

$$A = \begin{pmatrix} 5 & 3 \\ 3 & 5 \end{pmatrix}$$

We compute the characteristic polynomial as

$$(x - 5)^2 - 9 = x^2 - 10x + 25 - 9 = x^2 - 10x + 16 = (x - 8)(x - 2)$$

Using ranges, considering rescalings of one of the columns:

$$x - 8 = \begin{pmatrix} -3 & 3 \\ 3 & -3 \end{pmatrix} \implies (1, -1) \text{ is an eigenvector for } x = 2$$

$$x - 2 = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix} \implies (1, 1) \text{ is an eigenvector for } x = 8$$

Therefore, lining these two eigenvectors in columns we have:

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

Notice that the columns are already orthogonal to each other! So, let's just divide by the length of each column to have:

$$U = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

Now,

$$D = \underbrace{U^{-1}AU}_{=U^T} = \begin{pmatrix} 2 & 0 \\ 0 & 8 \end{pmatrix}$$

We also have

$$A = UDU^T$$

Notice that the matrix U under a column interpretation has

$$e_1 \mapsto \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}} \right) \quad e_2 \mapsto \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right)$$

This is a rotation matrix by -45° (i.e. 45° clockwise). Let

$$W = U^T = U^{-1} : \text{ rotation by } 45^\circ \text{ counterclockwise.} \quad A = W^T DW$$

If we were to use D as our bilinear transformation instead of A , our equation would be *simpler* (without any xy term):

$$\underbrace{\begin{pmatrix} x & y \end{pmatrix}}_{v^T} \cdot \underbrace{\begin{pmatrix} 2 & 0 \\ 0 & 8 \end{pmatrix}}_D \cdot \underbrace{\begin{pmatrix} x \\ y \end{pmatrix}}_v = 8 \implies 2x^2 + 8y^2 = 8$$

To see how this equation relates to our first, replace A with $W^T DW$ in our original equation:

$$v^T W^T DW v = 8 \implies (Wv)^T \cdot D \cdot (Wv) = 8$$

To get from the simplified equation $(v)^T D(v) = 8$ to this one we have replace our input v by Wv . That is, we rotate v by 45° counterclockwise before we plug it into $(v)^T D(v) = 8$.

Remember that to rotate a graph by an angle θ , we rotate the input to the equation by $-\theta$ (i.e. in reverse).

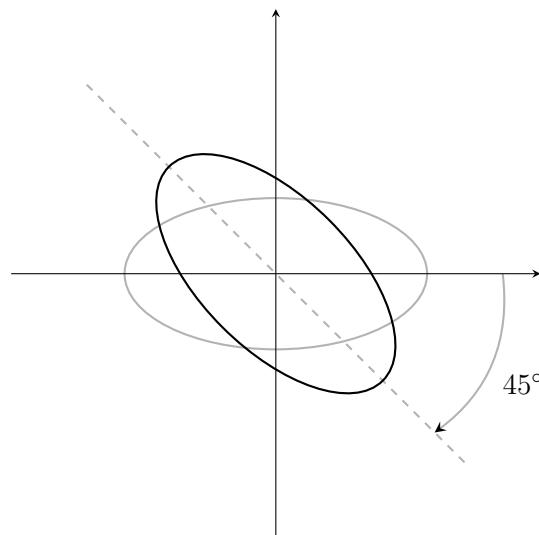
Therefore, the graph of $(v)^T D(v) = 8$ has been rotated by 45° clockwise (the opposite of W) to get to the graph of $(Wv)^T D(Wv) = v^T Av = 8$

The equation $v^T Dv = 8$ can be written as $2x^2 + 8y^2 = 8$ or rather

$$\left(\frac{x}{2}\right)^2 + y^2 = 1$$

which is the equation of an ellipse. This ellipse is a circle centered at the origin that has been stretched horizontally by a factor of 2.

An ellipse with vertices at $(\pm 2, 0)$ and $(0, \pm 1)$ has been rotated by 45° clockwise to get the graph of the equation $5x^2 + 6xy + 5y^2 = 8$.



Finding the Rotation of an Ellipse Centered at Origin

- First, write the conic in terms of a bilinear transformation (conics have zero linear part if they are centered at the origin). So our equation should look like:

$$v^T A v = k$$

for some constant k and where $v = (x, y)$.

- Next, find D and U that diagonalize A . Either make sure that U is a rotation matrix or just find one column of U and realize that there are two angles that work (180° from each other) within a 360° spectrum because of the symmetries of ellipses. If we take one column, we could always adjust the other column so that one of these two angles are achieved. So really, just seeing the image of e_1 is enough to identify an angle!
- The equation $v^T D v = k$, which is usually simpler to interpret (without any xy term), has been rotated by the angle represented by U to get to $v^T A v = k$.

Example 3. Consider

$$-4\sqrt{3}xy + 7x^2 + 3y^2 = 9$$

We can write this as

$$\underbrace{\begin{pmatrix} x \\ y \end{pmatrix}}_{v^T} \cdot \underbrace{\begin{pmatrix} 7 & -2\sqrt{3} \\ -2\sqrt{3} & 3 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} x \\ y \end{pmatrix}}_v = 9$$

The characteristic polynomial is, using the trace and the determinant,

$$x^2 - 10x + 9 = (x - 1)(x - 9)$$

Let's just get one column of U and send e_1 to it. Let's use the first column from $x - 1$ which is the same as the first column of x with -1 added to the first entry (the diagonal entry of the first column):

$$\begin{pmatrix} 7 - 1 \\ -2\sqrt{3} \end{pmatrix} = \begin{pmatrix} 6 \\ -2\sqrt{3} \end{pmatrix}$$

The eigenvalue associated to the columns of $x - 1$ is $x = 9$. This means that if this is our first column of U ,

that our diagonal matrix will be:

$$D = \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix}$$

so that we are considering a rotation of the equation

$$v^T D v = 9 \quad 9x^2 + y^2 = 9 \quad x^2 + \left(\frac{y}{3}\right)^2 = 1$$

which is an ellipse centered at the origin with vertices at $(\pm 1, 0)$ and $(0, \pm 3)$. The rotation is the one that will take e_1 to a rescaling of $(6, -2\sqrt{3})$. First rescale it to $(3, -\sqrt{3})$. Now divide by $\sqrt{3}$ to have $(\sqrt{3}, -1)$ which has length 2. Divide by 2 to have a unit vector

$$\left(\frac{\sqrt{3}}{2}, -\frac{1}{2} \right)$$

Sending e_1 to this is a rotation by 30° clockwise. So we have rotated the graph of $x^2 + \left(\frac{y}{3}\right)^2 = 1$ by 30° clockwise to arrive at the graph of $-4\sqrt{3}xy + 7x^2 + 3y^2 = 9$.

7.5.4 Positive Definite Symmetric Matrices

The eigenvalues of a matrix tell us what kind of scalar the matrix is behaving like on which vectors. If all the eigenvalues are positive, this means that the matrix elongates all the eigenvectors that are put as column input to the matrix function. Such an idea can be thought of as a surface version of “concave up” if the symmetric matrix itself describes the second derivative of a function describing a surface.

Positive Definite

A symmetric matrix is called positive definite if all of its eigenvalues are positive.

Negative Definite

A symmetric matrix is called negative definite if all of its eigenvalues are positive.

There are two equivalent conditions to a matrix being positive definite which are sometimes useful.

Theorem 7.5.8

Two equivalent conditions for a symmetric $n \times n$ matrix A to be positive definite are:

- (a) $A = B^T B$ for a matrix B whose map under a column interpretation is injective.
- (b) $v^T A v > 0$ for all nonzero vectors v in \mathbb{R}^n

Proof. Positive Definite \implies (a)

Suppose that A is positive definite. Since A is orthogonally diagonalizable, then $U^T A U = D$ for an orthogonal matrix U (i.e. U has orthonormal columns). Then, $A = U D U^T$. Let

$$D = \begin{pmatrix} a_1 & & & 0's \\ & \ddots & & \\ 0's & & & a_n \end{pmatrix}$$

Since A is positive definite, $a_1 > 0, \dots, a_n > 0$ so that

$$M = \begin{pmatrix} \sqrt{a_1} & & & 0's \\ & \ddots & & \\ 0's & & & \sqrt{a_n} \end{pmatrix}$$

is a matrix with real entries. Then,

$$A = U \underbrace{M M^T}_{D} U^T$$

Since $M = M^T$,

$$A = U M M^T U^T = (UM)(UM)^T$$

Let $B = (UM)^T$. Then, $A = B^T B$ where $B = UM$ which is the product of two square matrices each of which has nonzero determinant. Hence, the product has nonzero determinant representing an isomorphism and so represents an injective map.

(a) \implies (b) Now suppose that $A = B^T B$ where B represents an injective map. Let v be a nonzero vector in \mathbb{R}^n . This means that Bv is also a nonzero vector since the kernel of B is simply the zero vector. Then,

$$v^T A v = v^T B^T B v = (Bv)^T (Bv) = (Bv) \bullet (Bv) = |Bv|^2 > 0$$

(b) \implies Positive Definite

Now suppose that $v^T A v > 0$ for all nonzero vectors v in \mathbb{R}^n . Then if v is a nonzero eigenvector for A and

a is its eigenvalue,

$$0 < v^T(Av) = v^T(av) = a(v \bullet v) = a|v|^2 \implies a > 0$$

So then A would be positive definite.

□

The ideas in this proof can easily adjusted to discuss equivalences for *positive semi-definite matrices*.

Positive Semi-definite Matrix

A matrix is defined to be positive semi-definite if the eigenvalues are nonnegative. That is, we allow some of the eigenvalues to be zero and the rest positive.

Theorem 7.5.9

Two equivalent conditions for a symmetric $n \times n$ matrix A to be positive semi-definite are:

- (a) $A = B^T B$ for a matrix B .
- (b) $v^T Av \geq 0$ for all v in \mathbb{R}^n

We also have a nice way of determining whether or not a matrix is positive or negative definite by looking at its characteristic polynomial.

Coefficient Sign Changes

Suppose that we have a polynomial $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$. The number of coefficient sign changes for $f(x)$ is the number of times the sign \pm of the coefficients changes as we traverse the list from left to right:

$$a_n \curvearrowright a_{n-1} \curvearrowright \dots \quad \dots \quad a_1 \curvearrowright a_0$$

Descartes' Rule of Signs

This is a rule that helps us determine, *assuming all of the roots of $f(x)$ are real*, if all of them are negative, all of them are positive or if we have a mixture of positive and negative roots.

- The number of positive zeros (i.e. roots) counting multiplicities of $f(x)$ is less than or equal to the number of sign changes of the coefficients of $f(x)$.
- The number of negative zeros (i.e. roots) counting multiplicities of $f(x)$ is less than or equal to the number of sign changes of the coefficients of $f(-x)$.

Theorem 7.5.10

Let $p(x)$ be the characteristic polynomial of a symmetric matrix A . Then:

- A is positive definite if the number of coefficient sign changes of $p(-x)$ is zero.
- A is negative definite if the number of coefficient sign changes of $p(x)$ is zero.
- In all other cases, A is neither positive or negative definite.

Proof. Since the characteristic and minimal polynomial of A share the same roots, the roots of $p(x)$ are the eigenvalues of A . Since A is symmetric, all of these roots are real. Then the result follows from Descartes' rule of signs. \square

7.5.5 Optimization

In our section on multilinear functions, we briefly discussed the following idea:

Theorem 7.5.11

Suppose that $f : \mathbb{R}^n \rightarrow \mathbb{R}$ is equal to its multivariable Taylor expansion and that Df is the zero matrix at the point (c_1, \dots, c_n) . As the input moves from (c_1, \dots, c_n) to $(c_1 + h_1, \dots, c_n + h_n)$ then Δf is approximated by the bilinear part of the Taylor expansion:

$$\frac{1}{2} D^2 f((h_1, \dots, h_n), (h_1, \dots, h_n))$$

That is, the ratio of this approximated change to the actual change limits to 1 as

$$(h_1, \dots, h_n) \rightarrow (0, \dots, 0)$$

The second derivative is representable as a symmetric matrix A . Putting a vector $v = (h_1, \dots, h_n)$ into both inputs of this bilinear form is the same as computing $v^T A v$. Saying that $v^T A v > 0$ for all v is like saying that no matter the direction we travel from the point (c_1, \dots, c_n) , the output of the function f will have a positive change. So, if the function is instantaneously flat at our point in question (the first derivative is zero), then the function must have a minimum at that point. *The function is concave up.*

Corollary 7.5.12

Suppose that $f : \mathbb{R}^n \rightarrow \mathbb{R}$ is equal to its multivariable Taylor expansion and that Df is the zero matrix at the point (c_1, \dots, c_n) . If the second derivative matrix of f at (c_1, \dots, c_n) is positive definite, then f has a minimum at (c_1, \dots, c_n) . If the second derivative matrix of f at (c_1, \dots, c_n) is negative definite, then f has a maximum at (c_1, \dots, c_n) . If the second derivative matrix of f at (c_1, \dots, c_n) has *both* positive and negative eigenvalues, then f does not have a maximum nor a minimum at (c_1, \dots, c_n) .

Example 4. Suppose that we have determined that at $(x, y) = (1, -1)$ the first derivative of the following function is the derivative matrix:

$$f(x, y) = 35x^3 + 66x^2y + 42xy^2 + 9y^3 - 26x^2 - 32xy - 10y^2 + 5x + 3y$$

Let's find out if this point will yield a maximum or a minimum value of the function or neither.

$$Df : \begin{pmatrix} 105x^2 + 132xy + 42y^2 - 52x - 32y + 5 & 66x^2 + 84xy + 27y^2 - 32x - 20y + 3 \end{pmatrix}$$

Now:

$$D^2 f : \begin{pmatrix} 210x + 132y - 52 & 132x + 84y - 32 \\ 132x + 84y - 32 & 84x + 54y - 20 \end{pmatrix}$$

At $(x, y) = (1, -1)$, this is

$$A = \begin{pmatrix} 26 & 16 \\ 16 & 10 \end{pmatrix}$$

The characteristic polynomial of this matrix is

$$p(x) = x^2 - 36x + 4$$

Notice that $p(-x) = x^2 + 36x + 4$ has no sign changes. Hence, the matrix A is positive definite so that the function f has a *minimum* at $(x, y) = (1, -1)$.

Example 5. Suppose that

$$f(x, y, z) = -x^2 - 4y^2 - 2xz - yz - 4z^2 + 8x + 10y + 21z - \cos(z - 2) - 34$$

and that we know that at the point $(x, y, z) = (2, 1, 2)$ the first derivative matrix is zero. Let's determine whether this function has a maximum or a minimum at this point.

$$Df : \begin{pmatrix} -2x - 2z + 8 & -8y - z + 10 & -2x - y - 8z + \sin(z - 2) + 21 \end{pmatrix}$$

$$D^2 f : \begin{pmatrix} -2 & 0 & -2 \\ 0 & -8 & -1 \\ -2 & -1 & \cos(z - 2) - 8 \end{pmatrix}$$

At $(x, y, z) = (2, 1, 2)$, this matrix becomes:

$$\begin{pmatrix} -2 & 0 & -2 \\ 0 & -8 & -1 \\ -2 & -1 & -7 \end{pmatrix}$$

The characteristic polynomial is

$$x^3 + 17x^2 + 81x + 78$$

which has no sign changes. Hence, the function has a maximum at this point.

7.5.6 Finding the Center of a Rotated Ellipse

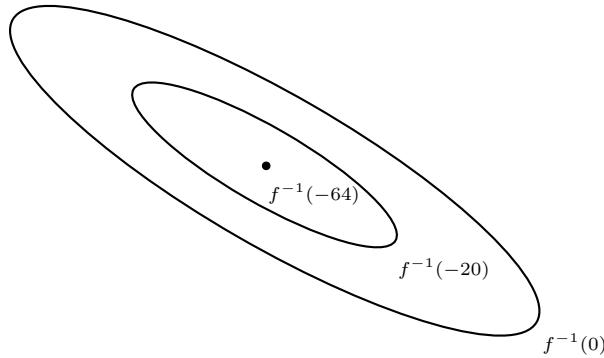
Example 6. Suppose that we are given the equation of a rotated ellipse which is not centered at the origin:

$$30\sqrt{3}xy + 19x^2 + 49y^2 - 30\sqrt{3}y - 38x - 45 = 0$$

We can think of the graph as being a fiber of the function

$$f(x, y) = 30\sqrt{3}xy + 19x^2 + 49y^2 - 30\sqrt{3}y - 38x + 19$$

The fibers of this function are nested ellipses. In particular, our ellipse is the fiber $f^{-1}(0)$. The altitude (i.e. the z value's) go down with a minimum output of -64 at the *center of all the ellipses*.



So to find the center of the ellipse, we find an ordered pair (x, y) that makes the first derivative matrix equal to $\begin{pmatrix} 0 & 0 \end{pmatrix}$.

$$Df : \begin{pmatrix} 30\sqrt{3}y + 38x - 38 & 30\sqrt{3}x + 98y - 30\sqrt{3} \end{pmatrix} = \begin{pmatrix} 0 & 0 \end{pmatrix}$$

$$\begin{aligned} 30\sqrt{3}y + 38x - 38 &= 0 \\ 30\sqrt{3}x + 98y - 30\sqrt{3} &= 0 \end{aligned}$$

Notice that the unique solution to this system of equations is $(x, y) = (1, 0)$. Hence, the minimum must occur at $(1, 0)$. To verify that we really do have a minimum here, we can compute the second derivative matrix at $(1, 0)$ and consider if it is positive definite:

$$D^2f : \begin{pmatrix} 38 & 30\sqrt{3} \\ 30\sqrt{3} & 98 \end{pmatrix}$$

The characteristic polynomial is $p(x) = x^2 - 136x + 1024$. Notice that $p(-x) = x^2 + 136x + 1024$ has no sign changes so that the matrix is positive definite and we indeed have a minimum. Therefore, the center of

our ellipse is at $(1, 0)$. Let's write our function $f(x, y)$ in terms of its multivariable Taylor expansion centered at $(1, 0)$:

$$\begin{aligned} f(x, y) &= \frac{1}{2} \cdot D^2 f_{(1,0)}((x - 1, y), (x - 1, y)) + Df_{(1,0)}((x - 1, y)) + f(1, 0) \\ &= (x - 1 \quad y) \cdot \begin{pmatrix} 19 & 15\sqrt{3} \\ 15\sqrt{3} & 49 \end{pmatrix} \cdot \begin{pmatrix} x - 1 \\ y \end{pmatrix} + (0 \quad 0) \cdot \begin{pmatrix} x - 1 \\ y \end{pmatrix} - 64 \end{aligned}$$

Our ellipse is the fiber $f^{-1}(0)$ (i.e. $f(x, y) = 0$) which is given as:

$$(x - 1 \quad y) \cdot \begin{pmatrix} 19 & 15\sqrt{3} \\ 15\sqrt{3} & 49 \end{pmatrix} \cdot \begin{pmatrix} x - 1 \\ y \end{pmatrix} = 64$$

Notice how writing the ellipse as a shift from the origin to $(1, 0)$ allows us to write the ellipse equation solely in terms of its bilinear part!

Now, to find the rotation of the ellipse, we diagonalize:

$$A = \begin{pmatrix} 19 & 15\sqrt{3} \\ 15\sqrt{3} & 49 \end{pmatrix} = \text{matrix for } \frac{1}{2} \cdot D^2 f_{(1,0)}$$

Its characteristic polynomial is $x^2 - 68 + 256 = (x - 64)(x - 4)$. We can make some choices. Let's send e_1 to a rescaled version of the first column of $x - 4$:

$$x - 4 = \begin{pmatrix} 15 \\ 15\sqrt{3} \end{pmatrix} \xrightarrow{\text{rescale}} \begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix} \xrightarrow{\text{rescale}} \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}$$

This looks like a 60° counterclockwise rotation. The eigenvalue associated with this column is 64. Therefore, the diagonal matrix in our diagonalization is:

$$D = \begin{pmatrix} 64 & 0 \\ 0 & 4 \end{pmatrix}$$

Therefore, if we unrotate the ellipse, we have

$$(x - 1 \quad y) \cdot \begin{pmatrix} 64 & 0 \\ 0 & 4 \end{pmatrix} \cdot \begin{pmatrix} x - 1 \\ y \end{pmatrix} = 64$$

If we further unshift our ellipse back to the origin, we have:

$$(x \ y) \cdot \begin{pmatrix} 64 & 0 \\ 0 & 4 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = 64 \implies 64x^2 + 4y^2 = 64$$

This simplifies to:

$$x^2 + \left(\frac{y}{4}\right)^2 = 1$$

which is an ellipse centered at the origin with vertices $(\pm 1, 0)$ and $(0, \pm 4)$.

We have rotated this ellipse by 60° counterclockwise and then shifted it so its center is at $(1, 0)$.

7.5.7 Diagonalizing a Trilinear Form

Example 7. Let's begin with an equation

$$x^3 + 7y^3 + x^2 + 5y^2 = 1$$

Let's rotate its graph by 45° clockwise. This is the same as replacing (x, y) in the equation with (x, y) being rotated by 45° *counterclockwise*. Let U represent rotation by 45° *counterclockwise*. Let $v = (x, y)$. Then, we replace v by Uv in our equation. We write our equation in a way that involves v . That is, we write $f(x, y) = x^3 + 7y^3 + x^2 + 5y^2$ in terms of its trilinear and bilinear parts as:

$$T(v, v, v) + B(v, v)$$

where T , a trilinear form, and B , a bilinear form, are given by:

$$T : \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{x \text{ level}} \quad \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 7 \end{pmatrix}}_{y \text{ level}} \qquad B : \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

The equation for the rotated graph looks like:

$$T(Uv, Uv, Uv) + B(Uv, Uv) = 1$$

We compute

$$U = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad U^{-1} = U^T = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

We have that

$$\begin{aligned}
 B(Uv, Uv) &= v^T U^T \cdot \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \cdot Uv \\
 &= \frac{1}{2} \cdot v^T \cdot \underbrace{\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}}_{= \begin{pmatrix} 1 & -1 \\ 5 & 5 \end{pmatrix}} \cdot v \\
 &= \begin{pmatrix} x & y \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 6 & 4 \\ 4 & 6 \end{pmatrix}}_A \cdot \begin{pmatrix} x \\ y \end{pmatrix}
 \end{aligned}$$

Let $D = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$. Going back,

$$D = U \cdot \underbrace{\begin{pmatrix} 6 & 4 \\ 4 & 6 \end{pmatrix}}_{U^T D U} \cdot U^T$$

so that U^T diagonalizes A as $D = (U^T)^{-1} A U^T$. (Note that U^T represents rotation by 45° clockwise since $U^T = U^{-1}$.)

If U^T diagonalizes A as the bilinear form B represented by D , does it also “diagonalize” the a trilinear form as T ?

First, think that to get A from D , we matrix multiply U to A on the *column side* and U to A (in the form of U^T) on the *row side* to get $A = U^T D U$. Letting \mathcal{D} be the trilinear matrix for T , we think:

$$\begin{matrix} U^S \\ \cdot \\ U^T \cdot \quad \mathcal{D} \quad \cdot U \end{matrix}$$

where U^S is just multiplication by U on the *stacking side*. What does the stacking side look like? Let’s just remember that our normal way at looking at U is the column side. When we transpose it over to the row side to look like U^T the rows are what the columns once were. So we can imagine that when we “stackify” U , the stacks will look like what the columns of U once looked like. The stacks of U^S are:

$$\text{Stack 1 of } U: \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad \qquad \text{Stack 2 of } U: \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

Consider the following computation:

$$U^S$$

$$\mathcal{D}$$

The first (i.e. “ x ”) level of this product is found by taking a linear combination of the levels of \mathcal{D} . The scalars in this linear combination come from the first stack of U^S (which is the first column of U):

$$\frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\mathcal{D} = \frac{1}{\sqrt{2}} \cdot (\text{Level 1 of } \mathcal{D}) + \frac{1}{\sqrt{2}} \cdot (\text{Level 2 of } \mathcal{D}) = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}$$

The second (i.e. “ y ”) level of this product is:

$$\frac{1}{\sqrt{2}} \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

$$\mathcal{D} = -\frac{1}{\sqrt{2}} \cdot (\text{Level 1 of } \mathcal{D}) + \frac{1}{\sqrt{2}} \cdot (\text{Level 2 of } \mathcal{D}) = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} -1 & 0 \\ 0 & 7 \end{pmatrix}$$

$$U^S$$

Therefore, \mathcal{D} is described by these two levels. Now to multiply U from the column side of this result, amounts to multiplying each of these levels by U on the right to obtain:

$$\underbrace{\frac{1}{2} \begin{pmatrix} 1 & -1 \\ 7 & 7 \end{pmatrix}}_{\text{Level 1}} \quad \underbrace{\frac{1}{2} \begin{pmatrix} -1 & 1 \\ 7 & 7 \end{pmatrix}}_{\text{Level 2}}$$

Lastly we multiply this trilinear form by U on the row side which means that we multiply each level by U^T on the left to obtain:

$$\tilde{T} : \underbrace{\frac{1}{2\sqrt{2}} \begin{pmatrix} 8 & 6 \\ 6 & 8 \end{pmatrix}}_{\text{Level 1}} \quad \underbrace{\frac{1}{2\sqrt{2}} \begin{pmatrix} 6 & 8 \\ 8 & 6 \end{pmatrix}}_{\text{Level 2}}$$

Notice that this is a *symmetric trilinear form!* If we look at both first columns or both second columns or both first rows or both second rows or the first level or the second level we see a symmetric matrix! Since U brings \mathcal{D} to \tilde{T} , working backwards, the inverse U^{-1} would thus diagonalize \tilde{T} to become \mathcal{D} .

7.5.8 Revisiting Least Squares with a Pseudo Inverse

Example 8. Let's suppose that we wanted to find the best fit line for the points $(1, 2)$, $(1, 3)$, $(1, 5)$. All of these points obviously lie on the line $x = 1$.

But let's find a line of the form $y = mx + b$ instead. And what does it even mean to find a line that is best fit of this form?

First of all, we attempt to find $\begin{pmatrix} m \\ b \end{pmatrix}$ such that

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} m \\ b \end{pmatrix} \stackrel{\text{get close}}{\approx} \begin{pmatrix} 2 \\ 3 \\ 5 \end{pmatrix}$$

The problem is that the range of A under a column interpretation is very one-dimensional: all \mathbb{R} -multiples of $(1, 1, 1)$. For sure $(2, 3, 4)$ is not in this range. *But we want to get close.* Let f represent the function we get from A via a column interpretation. Earlier in the text we accomplished this by finding a function g such that f is an orthogonal right inverse. We had that $\text{range}(f) \perp \ker(g)$. This was good because it causes the vector $f(g(w)) - w$ to be orthogonal to $\text{range}(f)$. That is, $f(g(w))$ is the *closest* we can get to w . But, this matrix A is not of full rank. It has no left inverse! Yet, there is a function \tilde{f} which we can use in place of g . It is called the *pseudo inverse* of f . Two important features of \tilde{f} is:

Pseudo Inverse Properties

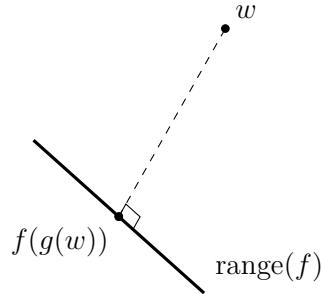
Suppose that \tilde{f} is the pseudo inverse of f . Then:

- $\tilde{f} \circ f \circ \tilde{f} = \tilde{f}$
- $\ker(\tilde{f}) \perp \text{range}(f)$

These properties do everything we could want. Note that $f(\tilde{f}(w)) - w$ is in $\ker(\tilde{f})$ since

$$\tilde{f}(f(\tilde{f}(w)) - w) = \underbrace{\tilde{f} \circ f \circ \tilde{f}(w)}_{\tilde{f}} - \tilde{f} = (\text{zero vector})$$

Since the kernel of \tilde{f} is orthogonal to the range of f , this vector $f(\tilde{f}(w)) - w$ provides the shortest distance from w to the range of f . Consider the following illustration:



Remember that to minimize a distance is to minimize the square of that distance which is a sum of squares. The vector w gives the y -values of the data points and $f(\tilde{f}(w))$ gives the corresponding y value(s) on the line $y = mx + b$ for $(m, b) = \tilde{f}(w)$. The square of the length of the vector $f(\tilde{f}(w)) - w$ is the sum of squares of differences of these corresponding y -values. We are minimizing *a sum of squares*.

A near vertical line would have some pretty large y differences. Getting close to the line $x = 1$ is far away from minimizing the result according to our schematic.

Great! Though not a left inverse, \tilde{f} has enough properties to give us a least squares solution! But what is this \tilde{f} and why did we wait until now to talk about it? We form it from an orthogonal diagonalization process of $A^T A$ which is a symmetric square matrix. We needed this in hand to get the powerful pseudo inverse idea! We compute:

$$A^T A = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}$$

The characteristic polynomial is $x^2 - 6x$ giving the eigenvalues 6 and 0. Diagonalizing, we find:

$$U = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad D = \begin{pmatrix} 6 & 0 \\ 0 & 0 \end{pmatrix} \implies U^T A^T A U = D$$

In particular, notice that D is $(AU)^T(AU)$. That is, the entries of D are just dot products of the columns of AU . This tells us that the nonzero columns of AU are orthogonal to each other. But in our case since there is a zero on the diagonal, the dot product of the last column with itself is 0: *so it is the zero vector!* In particular,

$$AU = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 2 & 0 \\ 2 & 0 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} \sqrt{2} & 0 \\ \sqrt{2} & 0 \\ \sqrt{2} & 0 \end{pmatrix}$$

Let's rescale this nonzero vector to $(1, 1, 1)$ and then using the column trick we can find a basis for $\langle(1, 1, 1)\rangle^\perp$ as the basis for the kernel of the matrix $\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$ under a column interpretation. We get a basis of $\{(-1, 0, 1), (-1, 1, 0)\}$. Applying Gram Schmidt to this basis we arrive at $\{(-1, 1, 0), (-\frac{1}{2}, -\frac{1}{2}, 1)\}$. Therefore, we now have a basis of orthogonal vectors

$$\{(1, 1, 1), (-1, 1, 0), \left(-\frac{1}{2}, -\frac{1}{2}, 1\right)\}$$

for \mathbb{R}^3 . Now, we make this basis orthonormal by dividing by the vector lengths and put the vectors as columns into a matrix:

$$V = \begin{pmatrix} \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \end{pmatrix}$$

Let's label the columns of this matrix as $(v_1 \ v_2 \ v_3)$. We label the columns of U above as $(u_1 \ u_2)$. Let's see what changes in the product $D = (AU)^T(AU)$ when we replace $(AU)^T$ by V^T . By construction, all the extra columns of V are orthogonal to the nonzero columns of (AU) . The dot product before of u_1 with itself was 6. But now we have $v_1 \bullet u_1$ in this product. The length of u_1 is $\sqrt{6}$ and v_1 is just u_1 rescaled to a unit vector, hence: $v_1 \bullet u_1 = \sqrt{6}$. The extra columns of V (extra rows of V^T) just produce rows of 0's in the product. Hence, we have:

$$V^T AU = \underbrace{\begin{pmatrix} \sqrt{6} & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}}_{\tilde{D}}$$

which has the same matrix size as our original matrix A . Since V and U are orthogonal square matrices, taking an inverse is the same as transposing. Hence:

$$V^T AU = \tilde{D} \implies V \cdot V^T AU \cdot U^T = V \cdot \tilde{D} \cdot U^T \implies A = V \cdot \tilde{D} \cdot U^T$$

Singular Value Decomposition

The decomposition that we just found in our example of

$$A = V \cdot \tilde{D} \cdot U^T$$

where V and U are orthogonal matrices and \tilde{D} has the same size as A is called a *singular value decomposition of a matrix*. All entries of \tilde{D} off of the diagonal are zero. The diagonal entries of \tilde{D} are square roots $\sqrt{\lambda}$ of the eigenvalues of $A^T A$. These eigenvalues are nonnegative because $A^T A$ is positive semi-definite. Hence, these square roots are real.

Let's use this singular value decomposition to find our pseudo inverse \tilde{f} .

We let \tilde{f} be described by the matrix:

$$P = U \cdot \underbrace{\begin{pmatrix} \frac{1}{\sqrt{6}} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_E \cdot V^T$$

Pseudo Inverse

Given a function f described by a matrix A whose singular value decomposition is $A = V \cdot \tilde{D} \cdot U^T$, the pseudo inverse \tilde{f} of A is given as:

$$P = U \cdot E \cdot V^T$$

where E is the same as \tilde{D}^T except we have taken reciprocals of the nonzero entries.

Theorem 7.5.13

$$\tilde{f} \circ f \circ \tilde{f} = \tilde{f}$$

Proof. Let A describe f and $P = U \cdot E \cdot V^T$ describe \tilde{f} where $A = V \cdot \tilde{D} \cdot U^T$ is a singular value decomposition of A . Then, we are considering PAP . We compute:

$$\begin{aligned} PAP &= \underbrace{U \cdot E \cdot V^T}_{P} \cdot \underbrace{V \cdot \tilde{D} \cdot U^T}_{A} \cdot \underbrace{U \cdot E \cdot V^T}_{P} \\ &= U \tilde{D} E V^T \end{aligned}$$

Therefore, the only question is whether $E \tilde{D} E \stackrel{?}{=} E$. Assume that the nonzero entries of \tilde{D} are pushed to the upper far left corner. Then, we can write \tilde{D} as a block matrix:

$$\tilde{D} = \begin{pmatrix} K & z_{12} \\ z_{21} & z_{22} \end{pmatrix}$$

where z_{12}, z_{21}, z_{22} are zero blocks and K is a diagonal matrix with only nonzero diagonal entries. The matrix

K^{-1} is also a diagonal matrix: just take the reciprocals of the diagonal entries of K . This tells us that:

$$E = \begin{pmatrix} K^{-1} & z_{21}^T \\ z_{12}^T & z_{22}^T \end{pmatrix}$$

In the following calculation, if we have two zero submatrices added together, we omit one of them since they are necessarily the same size. Also if a zero submatrix is added to nonzero submatrix, we omit the zero submatrix. *We are just concerned about the size of blocks.* One can check that zero matrix block sizes behave as labeled.

$$E\tilde{D}E = \underbrace{\begin{pmatrix} K^{-1} & z_{21}^T \\ z_{12}^T & z_{22}^T \end{pmatrix} \cdot \begin{pmatrix} K & z_{12} \\ z_{21} & z_{22} \end{pmatrix} \cdot \begin{pmatrix} K^{-1} & z_{21}^T \\ z_{12}^T & z_{22}^T \end{pmatrix}}_{\begin{pmatrix} \text{id} & z_{21}^T z_{22} \\ z_{22}^T z_{21} & z_{22}^T z_{22} \end{pmatrix}} = \underbrace{\begin{pmatrix} K^{-1} & z_{21}^T \\ z_{12}^T & z_{22}^T \end{pmatrix}}_E$$

This is what we wanted to show. \square

Theorem 7.5.14

$$\ker(\tilde{f}) \perp \text{range}(f)$$

Proof. Using the notation above, let f refer to $A = V \cdot \tilde{D} \cdot U^T$ and \tilde{f} refer to $P = U \cdot E \cdot V^T$. Suppose that $r = \text{rank}(\tilde{D}) = \text{rank}(E)$. Note that removing U from the product $U \cdot E \cdot V^T$ does not change what comes into E as a function of row vectors since U is surjective. Therefore, under a row interpretation, the range of P is the same as the range of $E \cdot V^T$ which is the span of the top r rows of V^T . This means that the rows of the matrix P are linear combinations of the top r rows of V^T . So anything in the kernel of P under a *column interpretation now* is orthogonal to the top r rows of V^T .

In a column interpretation, the range of A is equal to the span of the first r columns of V which is the same as the first r rows of V^T . This means that anything in the kernel of P is orthogonal to the range of A as desired. \square

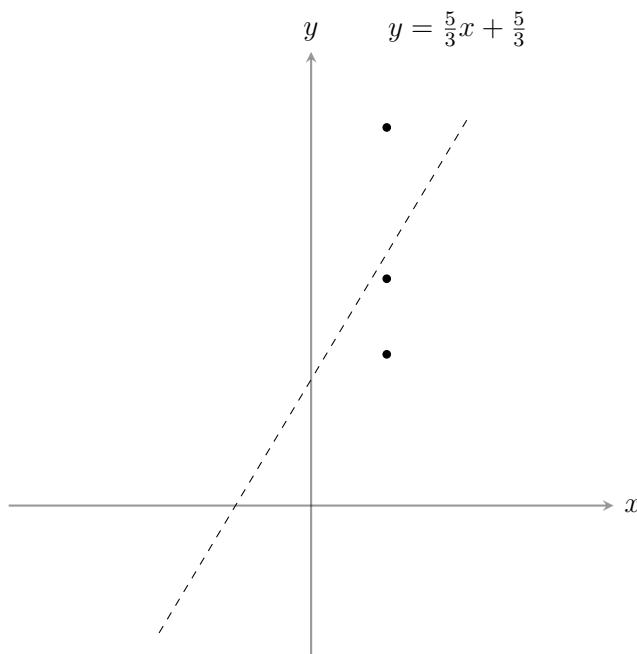
Back to our example,

$$P = \underbrace{\frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} \frac{1}{\sqrt{6}} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_E \cdot \underbrace{\begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} & \frac{2}{\sqrt{6}} \end{pmatrix}}_{V^T} = \begin{pmatrix} \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \end{pmatrix}$$

Hence, the best m and b we can use for our line can be found from:

$$\underbrace{\begin{pmatrix} \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \end{pmatrix}}_P \cdot \begin{pmatrix} 2 \\ 3 \\ 5 \end{pmatrix} = \begin{pmatrix} \frac{5}{3} \\ \frac{5}{3} \\ \frac{5}{3} \end{pmatrix}$$

Our best fit line is therefore $y = \frac{5}{3}x + \frac{5}{3}$.



Key Concepts from this Section

- **theorem 7.5.1 :** (page 911) Any polynomial where x represents a symmetric matrix again represents a symmetric matrix
- **theorem 7.5.2 :** (page 912) The minimal polynomial of a symmetric matrix cannot have any repeated linear factors.
- **fundamental theorem of algebra:** (page 913) Any polynomial of degree n can be completely factored into n linear factors, not necessarily distinct, over the complex numbers. That is, each factor $(x - a)$ has $a \in \mathbb{C}$.
- **complex conjugate:** (page 914) Given a complex number $q + ri$. Its complex conjugate is given by changing the sign of the imaginary part: $q - ri$. The notation for taking a complex conjugate is by using a line over the complex number:

$$\overline{q + ri} = q - ri$$

If B is a matrix or a vector, we can write \bar{B} to signify we are taking the complex conjugate of each entry.

- **conjugate condition for being real number:** (page 914) If $\bar{a} = a$, then $a \in \mathbb{R}$.
- **lemma 7.5.3 :** (page 914) Given $a, b \in \mathbb{C}$, then

$$\overline{a \cdot b} = \bar{a} \cdot \bar{b}$$

Also, for matrices A and B , we have:

$$\overline{A \cdot B} = \bar{A} \cdot \bar{B}$$

- **theorem 7.5.4 :** (page 914) Symmetric Matrices only have real eigenvalues.
- **corollary 7.5.5 :** (page 915) Symmetric matrices are diagonalizable.
- **theorem 7.5.6 :** (page 915) The Eigenspaces for different eigenvalues for a symmetric matrix are orthogonal to each other.
- **orthogonally diagonalizable:** (page 916) A matrix A is orthogonally diagonalizable if when we diagonalize A as $D = U^{-1}AU$, the matrix U is an orthogonal matrix. That is, the columns of U make up an orthonormal collection of vectors.
- **corollary 7.5.7 :** (page 916) Symmetric Matrices are orthogonally diagonalizable.
- **the inverse of an orthogonal matrix:** (page 916) If U is an orthogonal matrix, its inverse is simply U^T . Therefore, $U^T U = \text{id}$.
- **orthogonally diagonalize a symmetric matrix:** (page 916)
 1. Just diagonalize the matrix and get a matrix U . The columns of U that come from different eigenvalues will already be orthogonal.
 2. If there are two or more columns that come from the same eigenvalue, apply Gram Schmidt just on those columns from that one eigenvalue.
 3. Now, divide each column by its length. The modified U is the one to use!
- **eigenbasis:** (page 917) An eigenbasis is a basis for an eigenspace.
- **rotation matrices are orthogonal:** (page 919) Sometimes the matrix U signifies rotation on the plane. Then, U is an orthogonal matrix: rotating e_1 and e_2 which are already orthogonal produces two vectors which are still orthogonal to each other and each of length 1.
- **finding the rotation of an ellipse centered at origin:** (page 921)

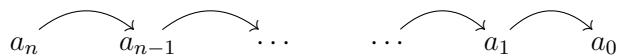
- First, write the conic in terms of a bilinear transformation (conics have zero linear part if they are centered at the origin). So our equation should look like:

$$v^T A v = k$$

for some constant k and where $v = (x, y)$.

- Next, find D and U that diagonalize A . Either make sure that U is a rotation matrix *or just find one column* of U and realize that there are *two angles that work* (180° from each other) *within a* 360° spectrum because of the symmetries of ellipses. If we take one column, we could always adjust the other column so that one of these two angles are achieved. So really, just seeing the image of e_1 is enough to identify an angle!
- The equation $v^T D v = k$, which is usually simpler to interpret (without any xy term), has been rotated by the angle represented by U to get to $v^T A v = k$.

- positive definite:** (page 923) A symmetric matrix is called positive definite if all of its eigenvalues are positive.
- negative definite:** (page 923) A symmetric matrix is called negative definite if all of its eigenvalues are positive.
- theorem 7.5.8 :** (page 923) Two equivalent conditions for a symmetric $n \times n$ matrix A to be positive definite are:
 - $A = B^T B$ for a matrix B whose map under a column interpretation is injective.
 - $v^T A v > 0$ for all nonzero vectors v in \mathbb{R}^n
- positive semi-definite matrix:** (page 925) A matrix is defined to be positive semi-definite if the eigenvalues are nonnegative. That is, we allow some of the eigenvalues to be zero and the rest positive.
- theorem 7.5.9 :** (page 925) Two equivalent conditions for a symmetric $n \times n$ matrix A to be positive semi-definite are:
 - $A = B^T B$ for a matrix B .
 - $v^T A v \geq 0$ for all v in \mathbb{R}^n
- coefficient sign changes:** (page 925) Suppose that we have a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. The number of coefficient sign changes for $f(x)$ is the number of times the sign \pm of the coefficients changes as we traverse the list from left to right:



- **descartes' rule of signs:** (page 925) This is a rule that helps us determine, *assuming all of the roots of $f(x)$ are real*, if all of them are negative, all of them are positive or if we have a mixture of positive and negative roots.
 - The number of positive zeros (i.e. roots) counting multiplicities of $f(x)$ is less than or equal to the number of sign changes of the coefficients of $f(x)$.
 - The number of negative zeros (i.e. roots) counting multiplicities of $f(x)$ is less than or equal to the number of sign changes of the coefficients of $f(-x)$.
- **theorem 7.5.10 :** (page 926) Let $p(x)$ be the characteristic polynomial of a symmetric matrix A . Then:
 - A is positive definite if the number of coefficient sign changes of $p(-x)$ is zero.
 - A is negative definite if the number of coefficient sign changes of $p(x)$ is zero.
 - In all other cases, A is neither positive or negative definite.
- **theorem 7.5.11 :** (page 926) Suppose that $f : \mathbb{R}^n \rightarrow \mathbb{R}$ is equal to its multivariable Taylor expansion and that Df is the zero matrix at the point (c_1, \dots, c_n) . As the input moves from (c_1, \dots, c_n) to $(c_1 + h_1, \dots, c_n + h_n)$ then Δf is approximated by the bilinear part of the Taylor expansion:

$$\frac{1}{2}D^2f((h_1, \dots, h_n), (h_1, \dots, h_n))$$

That is, the ratio of this approximated change to the actual change limits to 1 as

$$(h_1, \dots, h_n) \rightarrow (0, \dots, 0)$$
- **corollary 7.5.12 :** (page 927) Suppose that $f : \mathbb{R}^n \rightarrow \mathbb{R}$ is equal to its multivariable Taylor expansion and that Df is the zero matrix at the point (c_1, \dots, c_n) . If the second derivative matrix of f at (c_1, \dots, c_n) is positive definite, then f has a minimum at (c_1, \dots, c_n) . If the second derivative matrix of f at (c_1, \dots, c_n) is negative definite, then f has a maximum at (c_1, \dots, c_n) . If the second derivative matrix of f at (c_1, \dots, c_n) has *both* positive and negative eigenvalues, then f does not have a maximum nor a minimum at (c_1, \dots, c_n) .
- **pseudo inverse properties:** (page 934) Suppose that f is the pseudo inverse of f . Then:
 - $\tilde{f} \circ f \circ \tilde{f} = \tilde{f}$
 - $\ker(\tilde{f}) \perp \text{range}(f)$
- **singular value decomposition:** (page 936) The decomposition that we just found in our example of

$$A = V \cdot \tilde{D} \cdot U^T$$

where V and U are orthogonal matrices and \tilde{D} has the same size as A is called a *singular value decomposition of a matrix*. All entries of \tilde{D} off of the diagonal are zero. The diagonal entries of \tilde{D} are square roots $\pm\sqrt{\cdot}$ of the eigenvalues of $A^T A$. These eigenvalues are nonnegative because $A^T A$ is positive semi-definite. Hence, these square roots are real.

- **pseudo inverse:** (page 937) Given a function f described by a matrix A whose singular value decomposition is $A = V \cdot \tilde{D} \cdot U^T$, the pseudo inverse \tilde{f} of A is given as:

$$P = U \cdot E \cdot V^T$$

where E is the same as \tilde{D}^T except we have taken reciprocals of the nonzero entries.

- **theorem 7.5.13 :** (page 937)

$$\tilde{f} \circ f \circ \tilde{f} = \tilde{f}$$

- **theorem 7.5.14 :** (page 938)

$$\ker(\tilde{f}) \perp \text{range}(f)$$

7.5.9 Exercises

Rotating Conics

Identify what rotation of what standard conic the following represent by diagonalizing a matrix:

1. $10x^2 + 12xy + 10y^2 = 64$

2. $12\sqrt{3}xy + 19x^2 + 7y^2 = 25$

3. $-12\sqrt{3}xy + 7x^2 + 19y^2 = 25$

4. $6\sqrt{3}xy + 13x^2 + 7y^2 = 64$

5. $13x^2 - 24xy + 13y^2 = 25$

6. $-6\sqrt{3}xy + 7x^2 + 13y^2 = 64$

7. $-5\sqrt{3}xy - \frac{13}{2}x^2 - \frac{3}{2}y^2 = 9$

8. $\frac{5}{2}\sqrt{3}xy + \frac{11}{4}x^2 + \frac{1}{4}y^2 = 4$

9. $\frac{9}{2}x^2 + 41xy + \frac{9}{2}y^2 = 400$

10. $\frac{21}{2}x^2 + 29xy + \frac{21}{2}y^2 = 100$

Orthogonal Diagonalization

Orthogonally diagonalize the following matrices:

11.
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & \frac{3}{2} & -\frac{1}{2} \\ 0 & -\frac{1}{2} & \frac{3}{2} \end{pmatrix}$$

12.
$$\begin{pmatrix} \frac{3}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{3}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

13.
$$\begin{pmatrix} \frac{3}{2} & -\frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{3}{2} & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

14.
$$\begin{pmatrix} -1 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & -1 \end{pmatrix}$$

15.
$$\begin{pmatrix} -1 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & -1 \end{pmatrix}$$

16.
$$\begin{pmatrix} -1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & -1 \end{pmatrix}$$

17. $\begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & -1 \end{pmatrix}$

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

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

20. $\begin{pmatrix} -2 & 0 & 0 \\ 0 & -\frac{3}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{3}{2} \end{pmatrix}$

21. $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$

22. $\begin{pmatrix} -\frac{3}{2} & -\frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{3}{2} & 0 \\ 0 & 0 & -1 \end{pmatrix}$

23. $\begin{pmatrix} -1 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & -1 \end{pmatrix}$

24. $\begin{pmatrix} -\frac{3}{2} & 0 & \frac{1}{2} \\ 0 & -2 & 0 \\ \frac{1}{2} & 0 & -\frac{3}{2} \end{pmatrix}$

25. $\begin{pmatrix} \frac{1}{2} & 0 & \frac{3}{2} \\ 0 & -1 & 0 \\ \frac{3}{2} & 0 & \frac{1}{2} \end{pmatrix}$

26. $\begin{pmatrix} \frac{3}{2} & 0 & -\frac{1}{2} \\ 0 & 2 & 0 \\ -\frac{1}{2} & 0 & \frac{3}{2} \end{pmatrix}$

Apply Gram-Schmidt as necessary:

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

28. $\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & -1 & -1 \\ 0 & -1 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix}$

29. $\begin{pmatrix} -4 & 3 & 3 & 0 \\ 3 & -4 & 3 & 0 \\ 3 & 3 & -4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$

30. $\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$

31.
$$\begin{pmatrix} 2 & -2 & -2 \\ -2 & 2 & -2 \\ -2 & -2 & 2 \end{pmatrix}$$

32.
$$\begin{pmatrix} -1 & -2 & -2 \\ -2 & -1 & -2 \\ -2 & -2 & -1 \end{pmatrix}$$

33.
$$\begin{pmatrix} 4 & -3 & -3 & 0 \\ -3 & 4 & -3 & 0 \\ -3 & -3 & 4 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}$$

34.
$$\begin{pmatrix} 4 & 3 & 3 & 0 \\ 3 & 4 & 3 & 0 \\ 3 & 3 & 4 & 0 \\ 0 & 0 & 0 & 10 \end{pmatrix}$$

Optimization with two variables

Determine whether the given function has a maximum, minimum or neither at the given critical point.

35. $f(x, y) = -2x^2 - 2xy - 2y^2 - \cos(y)$

with critical point: $(0, 0)$

36. $f(x, y) = 4x^2 + 4xy + 4y^2 + 4x + 8y + \cos(y+1) + 6$

with critical point: $(0, -1)$

37. $f(x, y) = 4x^2 + 4xy + 4y^2 + 16x + 8y + \cos(x+2) + 15$

with critical point: $(-2, 0)$

38. $f(x, y) = -2x^2 - 4xy - 2y^2 - \cos(x) + 1$

with critical point: $(0, 0)$

39. $f(x, y) = -4x^2 - 4xy - 4y^2 - 12y - \cos(x-1) - 13$

with critical point: $(1, -2)$

40. $f(x, y) = -2x^2 - 4xy - 2y^2 + 16x + 16y - \cos(y-2) - 33$

with critical point: $(2, 2)$

41. $f(x, y) = -4x^2 - 2xy - 4y^2 - 2x - 8y - \cos(y+1) - 4$

with critical point: $(0, -1)$

42. $f(x, y) = 2x^2 + 4xy + 2y^2 + 8x + 8y + \cos(y) + 9$

with critical point: $(-2, 0)$

Optimization with three variables

Determine whether the given function has a maximum, minimum or neither at the given critical point.

43. $f(x, y, z) = x^2 + 4y^2 + 2xz + yz + 4z^2 - 8x - 2y - 20z + \cos(z - 2) + 28$

with critical point: $(2, 0, 2)$

44. $f(x, y, z) = -4x^2 - xy - 4y^2 - 4yz - z^2 + 9x + y - \cos(y - 1) - 3$

with critical point: $(1, 1, -2)$

45. $f(x, y, z) = -x^2 - 2y^2 - 2xz - yz - 2z^2 + 4x + 4z - \cos(z) - 5$

with critical point: $(2, 0, 0)$

46. $f(x, y, z) = -2x^2 - xy - 2y^2 - 4yz - z^2 - 2x - 4y - 6z - \cos(y + 2) - 1$

with critical point: $(0, -2, 1)$

47. $f(x, y, z) = 2x^2 + xy + 2y^2 + 2yz + z^2 - x - 4y - 2z + \cos(y - 1) + 2$

with critical point: $(0, 1, 0)$

48. $f(x, y, z) = x^2 + 2y^2 + 2xz + yz + 2z^2 + \cos(z)$

with critical point: $(0, 0, 0)$

49. $f(x, y, z) = -x^2 - 2y^2 - 2xz - yz - 2z^2 + 8y + 2z - \cos(z) - 10$

with critical point: $(0, 2, 0)$

50. $f(x, y, z) = 2x^2 + 4xy + y^2 + xz + 2z^2 + 10x + 8y - 7z + \cos(x + 1) + 22$

with critical point: $(-1, -2, 2)$

Best Fit Line via Pseudo Inverse

Go back to the problems in chapter 5 that dealt with finding a best fit line. Do these problems using the pseudo inverse technique of this section. You should get the same result.

7.5.10 Solutions

1. $\theta = +45^\circ$

$$16x^2 + 4y^2 = 64$$

2. $\theta = +30^\circ$

$$25x^2 + y^2 = 25$$

3. $\theta = +30^\circ$

$$x^2 + 25y^2 = 25$$

4. $\theta = +30^\circ$

$$16x^2 + 4y^2 = 64$$

5. $\theta = -45^\circ$

$$25x^2 + y^2 = 25$$

6. $\theta = -60^\circ$

$$16x^2 + 4y^2 = 64$$

7. $\theta = -60^\circ$

$$x^2 - 9y^2 = 9$$

8. $\theta = +30^\circ$

$$4x^2 - y^2 = 4$$

9. $\theta = +45^\circ$

$$25x^2 - 16y^2 = 400$$

10. $\theta = +45^\circ$

$$25x^2 - 4y^2 = 100$$

11. $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$

$$P = \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

12. $D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \end{pmatrix}$$

$$\mathbf{13.} D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \end{pmatrix}$$

$$\mathbf{14.} D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

$$\mathbf{15.} D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

$$\mathbf{16.} D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

$$\mathbf{17.} D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \end{pmatrix}$$

$$\mathbf{18.} D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$P = \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

$$\mathbf{19.} D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

$$\mathbf{20.} D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

$$P = \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

$$\mathbf{21.} D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$P = \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

$$\mathbf{22.} D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \end{pmatrix}$$

$$23. D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

$$24. D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

$$25. D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

$$26. D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

$$27. D = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & -3 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{3}\sqrt{3} & 0 & \frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & 0 & 0 & \frac{2}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & 0 & -\frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

after Gram-Schmidt on:

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

$$28. D = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$P = \begin{pmatrix} 0 & 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} & 0 & \frac{1}{3}\sqrt{3} \\ 0 & \frac{2}{3}\sqrt{\frac{3}{2}} & 0 & \frac{1}{3}\sqrt{3} \\ -\frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} & 0 & \frac{1}{3}\sqrt{3} \end{pmatrix}$$

after Gram-Schmidt on:

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

29. $D = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -7 & 0 \\ 0 & 0 & 0 & -7 \end{pmatrix}$

$P = \begin{pmatrix} \frac{1}{3}\sqrt{3} & 0 & \frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & 0 & 0 & \frac{2}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & 0 & -\frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ 0 & 1 & 0 & 0 \end{pmatrix}$

after Gram-Schmidt on:

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

30. $D = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{3}\sqrt{3} & \frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ 0 & \frac{1}{3}\sqrt{3} & 0 & \frac{2}{3}\sqrt{\frac{3}{2}} \\ 0 & \frac{1}{3}\sqrt{3} & -\frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \end{pmatrix}$

after Gram-Schmidt on:

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

31. $D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix}$

$P = \begin{pmatrix} \frac{1}{3}\sqrt{3} & \frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & 0 & \frac{2}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & -\frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \end{pmatrix}$

after Gram-Schmidt on:

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

32. $D = \begin{pmatrix} -5 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$P = \begin{pmatrix} \frac{1}{3}\sqrt{3} & \frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & 0 & \frac{2}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & -\frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \end{pmatrix}$

after Gram-Schmidt on:

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

33. $D = \begin{pmatrix} 7 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}$

$P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} & \frac{1}{3}\sqrt{3} & 0 \\ 0 & \frac{2}{3}\sqrt{\frac{3}{2}} & \frac{1}{3}\sqrt{3} & 0 \\ -\frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} & \frac{1}{3}\sqrt{3} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

after Gram-Schmidt on:

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

34. $D = \begin{pmatrix} 10 & 0 & 0 & 0 \\ 0 & 10 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

$P = \begin{pmatrix} \frac{1}{3}\sqrt{3} & 0 & \frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & 0 & 0 & \frac{2}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & 0 & -\frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ 0 & 1 & 0 & 0 \end{pmatrix}$

after Gram-Schmidt on:

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

35. First Derivative:

$$(-4x - 2y, -2x - 4y + \sin(y))$$

Second Derivative:

$$\begin{pmatrix} -4 & -2 \\ -2 & \cos(y) - 4 \end{pmatrix}$$

Characteristic Polynomial:

$$x^2 + 7x + 8$$

maximum

36. First Derivative:

$$(8x + 4y + 4, 4x + 8y - \sin(y + 1) + 8)$$

Second Derivative:

$$\begin{pmatrix} 8 & 4 \\ 4 & -\cos(y + 1) + 8 \end{pmatrix}$$

Characteristic Polynomial:

$$x^2 - 15x + 40$$

minimum

37. First Derivative:

$$(8x + 4y - \sin(x + 2) + 16, 4x + 8y + 8)$$

Second Derivative:

$$\begin{pmatrix} -\cos(x + 2) + 8 & 4 \\ 4 & 8 \end{pmatrix}$$

Characteristic Polynomial:

$$x^2 - 15x + 40$$

minimum

38. First Derivative:

$$(-4x - 4y + \sin(x), -4x - 4y)$$

Second Derivative:

$$\begin{pmatrix} \cos(x) - 4 & -4 \\ -4 & -4 \end{pmatrix}$$

Characteristic Polynomial:

$$x^2 + 7x - 4$$

neither

39. First Derivative:

$$(-8x - 4y + \sin(x - 1), -4x - 8y - 12)$$

Second Derivative:

$$\begin{pmatrix} \cos(x - 1) - 8 & -4 \\ -4 & -8 \end{pmatrix}$$

Characteristic Polynomial:

$$x^2 + 15x + 40$$

maximum

40. First Derivative:

$$(-4x - 4y + 16, -4x - 4y + \sin(y - 2) + 16)$$

Second Derivative:

$$\begin{pmatrix} -4 & -4 \\ -4 & \cos(y - 2) - 4 \end{pmatrix}$$

Characteristic Polynomial:

$$x^2 + 7x - 4$$

neither

41. First Derivative:

$$(-8x - 2y - 2, -2x - 8y + \sin(y + 1) - 8)$$

Second Derivative:

$$\begin{pmatrix} -8 & -2 \\ -2 & \cos(y + 1) - 8 \end{pmatrix}$$

Characteristic Polynomial:

$$x^2 + 15x + 52$$

maximum

42. First Derivative:

$$(4x + 4y + 8, 4x + 4y - \sin(y) + 8)$$

Second Derivative:

$$\begin{pmatrix} 4 & 4 \\ 4 & -\cos(y) + 4 \end{pmatrix}$$

Characteristic Polynomial:

$$x^2 - 7x - 4$$

neither

43. First Derivative:

$$(2x + 2z - 8, 8y + z - 2, 2x + y + 8z - \sin(z - 2) - 20)$$

Second Derivative:

$$\begin{pmatrix} 2 & 0 & 2 \\ 0 & 8 & 1 \\ 2 & 1 & -\cos(z - 2) + 8 \end{pmatrix}$$

Characteristic Polynomial:

$$x^3 - 17x^2 + 81x - 78$$

minimum

44. First Derivative:

$$(-8x - y + 9, -x - 8y - 4z + \sin(y - 1) + 1, -4y - 2z)$$

Second Derivative:

$$\begin{pmatrix} -8 & -1 & 0 \\ -1 & \cos(y - 1) - 8 & -4 \\ 0 & -4 & -2 \end{pmatrix}$$

Characteristic Polynomial:

$$x^3 + 17x^2 + 69x - 18$$

neither

45. First Derivative:

$$(-2x - 2z + 4, -4y - z, -2x - y - 4z + \sin(z) + 4)$$

Second Derivative:

$$\begin{pmatrix} -2 & 0 & -2 \\ 0 & -4 & -1 \\ -2 & -1 & \cos(z) - 4 \end{pmatrix}$$

Characteristic Polynomial:

$$x^3 + 9x^2 + 21x + 6$$

maximum

46. First Derivative:

$$(-4x - y - 2, -x - 4y - 4z + \sin(y + 2) - 4, -4y - 2z - 6)$$

Second Derivative:

$$\begin{pmatrix} -4 & -1 & 0 \\ -1 & \cos(y + 2) - 4 & -4 \\ 0 & -4 & -2 \end{pmatrix}$$

Characteristic Polynomial:

$$x^3 + 9x^2 + 9x - 42$$

neither

47. First Derivative:

$$(4x + y - 1, x + 4y + 2z - \sin(y - 1) - 4, 2y + 2z - 2)$$

Second Derivative:

$$\begin{pmatrix} 4 & 1 & 0 \\ 1 & -\cos(y - 1) + 4 & 2 \\ 0 & 2 & 2 \end{pmatrix}$$

Characteristic Polynomial:

$$x^3 - 9x^2 + 21x - 6$$

minimum

48. First Derivative:

$$(2x + 2z, 4y + z, 2x + y + 4z - \sin(z))$$

Second Derivative:

$$\begin{pmatrix} 2 & 0 & 2 \\ 0 & 4 & 1 \\ 2 & 1 & -\cos(z) + 4 \end{pmatrix}$$

Characteristic Polynomial:

$$x^3 - 9x^2 + 21x - 6$$

minimum

49. First Derivative:

$$(-2x - 2z, -4y - z + 8, -2x - y - 4z + \sin(z) + 2)$$

Second Derivative:

$$\begin{pmatrix} -2 & 0 & -2 \\ 0 & -4 & -1 \\ -2 & -1 & \cos(z) - 4 \end{pmatrix}$$

Characteristic Polynomial:

$$x^3 + 9x^2 + 21x + 6$$

maximum

50. First Derivative:

$$(4x + 4y + z - \sin(x + 1) + 10, 4x + 2y + 8, x + 4z - 7)$$

Second Derivative:

$$\begin{pmatrix} -\cos(x + 1) + 4 & 4 & 1 \\ 4 & 2 & 0 \\ 1 & 0 & 4 \end{pmatrix}$$

Characteristic Polynomial:

$$x^3 - 9x^2 + 9x + 42$$

neither

Inner Products

7.6

7.6.1 Inner Products from Positive Definite Symmetric Matrices	957
7.6.2 Hermitian Inner Product	958
7.6.3 An Integral Inner Product	961
7.6.4 Orthonormal Bases	963
7.6.5 Introduction to Fourier Series	964
7.6.6 Fourier Series Example and π	972
7.6.7 Gram-Schmidt and Polynomials	973
7.6.8 Exercises	979
7.6.9 Solutions	983

Questions to Guide Your Study:

- *What is an inner product?*
- *What is a Hermitian inner product?*
- *What is an example of an inner product between functions?*
- *What are some examples of orthonormal sets of functions?*
- *What is a Fourier series and does it do?*
- *How do you apply a Gram Schmidt process with respect to an inner product?*

7.6.1 Inner Products from Positive Definite Symmetric Matrices

Inner Product

An inner product on \mathbb{R}^n is a positive definite symmetric bilinear transformation $T : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ given by:

$$T(u, v) = u \diamond v$$

Wow! That is a lot of words. Let's look at some examples. Take a symmetric matrix like

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

The matrix A represents a bilinear transformation

$$T(u, v) = u^T A v$$

Because A is symmetric, then:

$$T(u, v) = u^T A v = v^T A u = T(v, u)$$

Let's try this out:

$$(1 \ -1) \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 4 = (2 \ 1) \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Now the characteristic polynomial of A is $p(x) = x^2 - 3x + 1$. Since $p(-x) = x^2 + 3x + 1$ has no sign changes, the matrix A is positive definite so that $v^T A v > 0$ all of the time. For instance,

$$(1 \ -1) \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 1 > 0$$

Therefore, the matrix A thought of as a bilinear transformation gives an inner product.

Example 1. If we define an inner product \diamond by the matrix A , then $u \diamond v = u^T A v$. So:

$$(1, -1) \diamond (2, 1) = 4$$

Inner Products from Matrices

Any positive definite symmetric matrix gives an inner product.

Example 2. The regular dot product \bullet between vectors in \mathbb{R}^n is the inner product determined by the matrix $\text{id}_{n \times n}$.

Recall that the dot product gives us a notion of length of a vector:

$$|v| = \sqrt{v \bullet v}$$

Because an inner product \diamond is positive definite, then $v \diamond v > 0$

Therefore, we can compute the length of a vector with respect to an inner product \diamond in a similar way.

Norm From an Inner Product

We let the norm or *length* of a vector with respect to an inner product \diamond be given by

$$|v|_{\diamond} = \sqrt{v \diamond v}$$

Example 3. Letting \diamond be given by the matrix A above, then:

$$|(1, 3)|_{\diamond} = \sqrt{\begin{pmatrix} 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix}} = \sqrt{17}$$

7.6.2 Hermitian Inner Product

We turn our attention to vector spaces where the scalars are complex—things like \mathbb{C}^3 or \mathbb{C}^5 .

Complex Vector Space

A vector space with scalars in \mathbb{C} is called a complex vector space

If we were to try to use the normal dot product to define the vector length of $v = (i, i)$ in \mathbb{C}^2 , we would think

$$\sqrt{v \bullet v} = \sqrt{i^2 + i^2} = \sqrt{-2} \quad \text{This does not make sense!}$$

Hence, we need to define the inner product in \mathbb{C}^n differently. We begin with some definitions.

Hermitian Adjoint

The Hermitian adjoint A^* of a matrix A with entries in \mathbb{C} is $A^* = \overline{A}^T$ where \overline{A} means that we have taken the complex conjugate of each entry.

Hermitian Matrix

This is the analog to a matrix being symmetric—but when we have complex entries. A matrix is called Hermitian if $A = A^*$.

Example 4. All symmetric matrices with real entries are Hermitian.

Conjugate Linear

A function $f : V \rightarrow W$ between complex vector spaces is called conjugate linear if it is additive and if $f(a \cdot v) = \bar{a} \cdot f(v)$. So when the scalar comes out, we take a conjugate of it. It is *conjugate scalable*.

Hermitian Inner Product

Let V be a complex vector space. A Hermitian Inner Product is a “positive definite” and “Hermitian” function $T : V \times V \rightarrow \mathbb{C}$ which is linear in the first component and *conjugate linear* in the second component. The word “positive definite” simply means that $T(v, v) > 0$ and “Hermitian” means that $T(u, v) = \overline{T(v, u)}$. We will write $u \square v = T(u, v)$ to signify a Hermitian inner product.

Hermitian Inner Products from Matrices

Take any positive definite Hermitian matrix A . Then we can define a Hermitian inner product:

$$u \square v = u^T A \bar{v}$$

Note: if we wanted the Hermitian inner product to be conjugate linear in the first component, then we could instead define the Hermitian inner product as $u^ A v$.*

Standard Hermitian Inner Product

The matrix $A = \text{id}_{n \times n}$ defines the standard Hermitian product.

Example 5. Let \square denote the standard Hermitian Inner Product.

$$(i, 1) \square (2, i+2) = \begin{pmatrix} i & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -i+2 \end{pmatrix} = i \cdot 2 + 1 \cdot (-i+2) = 4 - i$$

$$(i, i) \square (i, i) = \begin{pmatrix} i & i \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -i \\ -i \end{pmatrix} = i \cdot (-i) + i \cdot (-i) = 1 + 1 = 2$$

Hermitian Norm of a Vector

Given a vector v in a complex vector space v , we can define the norm

$$|v|_{\square} = \sqrt{v \square v}$$

Example 6. Letting \square denote the standard Hermitian inner product,

$$|(i, i)|_{\square} = \sqrt{\begin{pmatrix} i & i \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -i \\ -i \end{pmatrix}} = \sqrt{2}$$

Though we do not go into depth here in this text, we mention how our work to orthogonally diagonalize real symmetric matrices generalizes to complex Hermitian matrices.

Unitary Matrix

A Hermitian matrix A whose columns are orthonormal with respect to the standard Hermitian inner product is called *unitary*. It is the analog to an orthogonal matrix.

Theorem 7.6.1

Hermitian matrices are diagonalizable with a matrix U which is unitary.

Proof. The proof given in this text easily generalizes. \square

7.6.3 An Integral Inner Product

If we subdivide the interval $[0, 1]$ into n equal pieces and then take a right hand rule Riemann sum for a continuous function $f(x)$, we have a list of rectangle areas for $f(x)$ over than interval. This is a way that we can turn a function into a tuple—a tuple of rectangle areas. We can do this with two continuous functions both with a right hand rule and both with partitioning $[0, 1]$ into n equal pieces. So we have two n tuples in \mathbb{R}^n . We can take the dot product between these two tuples in \mathbb{R}^n . We could repeat this for a different value of n . As $n \rightarrow \infty$, this dot product of rectangle areas for two functions f and g gets closer and closer to a number—it limits to something: *a new kind of an inner product. This inner product is defined by an integral!*

$C[0, 1]$

Let $C[0, 1]$ denote the vector space consisting of continuous functions $[0, 1] \rightarrow \mathbb{R}$.

Inner product on $C[0, 1]$

Let $f, g \in C[0, 1]$. Then, we can define an inner product $f \diamond g = \int_0^1 f(x)g(x) dx$.

Proof. Define $T(f, g) = f \diamond g$. One can check that $T(f, g) = T(g, f)$ so that it is symmetric.

Now let's check to see if T is positive definite. This amounts to checking if $T(f, f) = \int f(x)^2 dx > 0$ for continuous $f(x)$ that is not the zero function on $[0, 1]$. Since f is not the zero function, then there exists some $a \in [0, 1]$ so that $f(a)^2 > 0$. We use the continuity of $g(x) = f(x)^2$. Choose $\epsilon > 0$ so that $g(a) - \epsilon > 0$. Then there exists δ so that $(a - \delta, a + \delta) \subset g^{-1}((g(a) - \epsilon, g(a) + \epsilon))$. This means that the integral

$\int_{a-\delta}^{a+\delta} g(x) dx \geq (2\delta)(g(a) - \epsilon) > 0$. Since $g(x) = f(x)^2 > 0$, we then have that

$$\int_0^1 f(x)^2 dx > 0$$

That T is bilinear amounts from the fact that multiplication is bilinear and taking an integral is linear. Therefore, \diamond gives us an inner product. \square

Example 7. Using this inner product,

$$x \diamond (x+1) = \int_0^1 \underbrace{x^2 + x}_{x \cdot (x+1)} dx = \frac{x^3}{3} + \frac{x^2}{2} \Big|_0^1 = \frac{5}{6}$$

Example 8.

$$|x|_\diamond = \sqrt{\int_0^1 x^2 dx} = \sqrt{\frac{1}{3}}$$

Example 9. Using the trigonometric identity $\frac{1}{2} \sin(2a) = \sin a \cos b$,

$$\sin(2\pi x) \diamond \cos(2\pi x) = \int_0^1 \sin(2\pi x) \cos(2\pi x) dx = \int_0^1 \frac{1}{2} \sin(4\pi x) dx = 0$$

Hence, $\sin(2\pi x)$ and $\cos(2\pi x)$ are orthogonal with respect to the inner product \diamond .

Orthogonality

With respect to an inner product \diamond , two vectors v and w are orthogonal if $v \diamond w = 0$.

Distance

We define the distance between two vectors v and w with respect to \diamond as $|v - w|_\diamond$.

Example 10. The distance between x and 1 with respect to \diamond is

$$|x - 1|_\diamond = \sqrt{\int_0^1 (x - 1)^2 dx} = \sqrt{\frac{1}{3}}$$

7.6.4 Orthonormal Bases

When we apply the Gram Schmidt process using projections, suppose that we start with a collection of vectors $v_1, v_2, v_3, \dots, v_n$. Our end goal is to turn these vectors into a collection of vectors $w_1, w_2, w_3, \dots, w_n$ which are orthogonal to each other. At step k , we compute:

$$w_k = v_k - \left(\underbrace{\text{proj}_{w_1} v_k + \text{proj}_{w_2} v_k + \cdots + \text{proj}_{w_{k-1}} v_k}_{\text{The projection of } v_k \text{ onto } \langle w_1, \dots, w_{k-1} \rangle} \right)$$

Now suppose that at each step we also try to guarantee that w_j has length 1. Then,

$$\text{proj}_{w_j} v_k = \frac{w_k \bullet v_k}{w_j \bullet w_j} = w_k \bullet v_k$$

Projection onto a subspace

Suppose that W is a subspace of V and that $\{w_1, \dots, w_k\}$ is an orthonormal basis for W . Then, the projection of a vector v onto W is:

$$(v \bullet w_1)w_1 + (v \bullet w_2)w_2 + \cdots + (v \bullet w_k)w_k$$

Example 11. Take $v_1 = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ and $v_2 = (-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$. We will consider the projection of the vector $(2, 3)$ onto $\langle v_1, v_2 \rangle = \mathbb{R}^2$. The vector $(2, 3)$ is already in \mathbb{R}^2 so this projection should be $(2, 3)$ again but written with respect to v_1 and v_2 .

$$(2, 3) \bullet v_1 = \frac{5}{\sqrt{2}} \quad (2, 3) \bullet v_2 = \frac{1}{\sqrt{2}}$$

Hence,

$$(2, 3) = \frac{5}{\sqrt{2}}v_1 + \frac{1}{\sqrt{2}}v_2$$

Let

$$f \diamond g = \int_0^1 fg \, dx$$

Inner Product Projection onto a Subspace

Suppose that W is a subspace of V and that $\{w_1, \dots, w_k\}$ is an orthonormal basis for W with respect to \diamond . Then, the projection of a vector f onto W is:

$$(f \diamond w_1)w_1 + (f \diamond w_2)w_2 + \cdots + (f \diamond w_k)w_k$$

Corollary 7.6.2 Parseval's Identity

Suppose that $f = a_1w_1 + \cdots + a_kw_k$ where $\{w_1, \dots, w_k\}$ is an orthonormal basis for W with respect to \diamond . Then,

$$|f|_\diamond^2 = a_1^2 + a_2^2 + \cdots + a_k^2$$

This is like a generalized Pythagorean Identity a.k.a. Parseval's Identity.

Proof. Using the orthonormality of $\{w_1, \dots, w_k\}$, we have:

$$\int_0^1 f \cdot f \, dx = \sum_{i,j} \int_0^1 a_i a_j w_i w_j \, dx = \sum_{i,j} a_i a_j (w_i \diamond w_j) = \sum_i a_i^2$$

□

Note: usually the length $|f|_\diamond$ is denoted as $|f|_2$ and called the “ L^2 norm” of a function.

7.6.5 Introduction to Fourier Series

Physicists and Engineers often want waves to add and cancel each other in a certain way. They use Fourier Series.

We discuss Fourier series here from a linear algebra perspective. We also discuss the ideas of convergence

which are associated with Fourier series. The ideas presented are more of an essay on the subject to help the reader gain an intuitive understanding and appreciation for some of the mathematics involved. That being the case, there are no exercises in this section on the analysis of Fourier series.

Here is an example of an infinite orthonormal set of functions (thought of as vectors).

An Infinite Orthonormal Set

The functions 1 , $\sqrt{2} \cos(2n\pi x)$ for each $n \in \mathbb{N}$ and $\sqrt{2} \sin(2n\pi x)$ for each $n \in \mathbb{N}$ together make up an infinite orthonormal set. Call this infinite collection \mathcal{C} . Let S_N denote the subcollection of \mathcal{C} consisting of functions 1 , $\sqrt{2} \cos(2n\pi x)$, and $\sqrt{2} \sin(2n\pi x)$ for $n \leq N$.

Example 12. Let $n \in \mathbb{N}$ (that is, n is a positive integer.) Then,

$$|\sqrt{2} \sin(2n\pi x)|_\diamond = 1$$

That is, $\sqrt{2} \sin(2n\pi x)$ is a unit “vector.” We check this using the trigonometric identity $\sin^2(x) = \frac{1}{2} - \frac{\cos(2x)}{2}$:

$$\int_0^1 (\sqrt{2} \sin(2n\pi x))^2 dx = 2 \cdot \int_0^1 \frac{1}{2} - \underbrace{\frac{\cos(4n\pi x)}{2}}_{\text{this integrates to 0 by its periodicity}} dx = 2 \cdot \frac{1}{2} \cdot 1 = 1$$

this integrates to 0 by
its periodicity

Fourier Series and Closeness

Let $f \in C[0, 1]$. As $N \rightarrow \infty$, the projection of f onto the span $\langle S_N \rangle$ gets arbitrarily “close” to f . This “limiting projection” is called the Fourier series of f . Yet we will define “closeness” in a \diamond sense. That is, given any positive distance $\epsilon > 0$, there exists N such that

$$\left| f - \sum_{w \in S_N} (f \diamond w)w \right|_\diamond < \epsilon$$

Proof. [10, p. 92] \square

What does this even really mean? Sums of cosine and sine waves are getting closer to the function?
But how?

The sum of cosine and sine waves $\sum_{w \in S_N} (f \diamond w)w$ as $N \rightarrow \infty$ may not even converge to a single function according to the result we just cited!

We simply know that the additional wave oscillations as we keep adding eventually only *significantly* change things on smaller and smaller sets—but these small sets can wander and change at a moments notice.

Let's step away from continuous functions in our discussion.

Class of Functions

Suppose that g and h are functions $[0, 1] \rightarrow \mathbb{R}$, which although possibly not continuous, have well-defined lengths $|g|_\diamond$ and $|h|_\diamond$ which are finite. We say that f and g are in the same class of functions with respect to \diamond if $|f - g|_\diamond = 0$.

Our result above really says that a sequence of function classes limits to a *unique* function class.
There is one and only one limit to this sequence when thought of as a class.

Converging to a Class of Functions

We let “ \mathcal{S} ” be the whole “class” of functions g such that

$$\left| g - \sum_{w \in S_N} (f \diamond w)w \right|_\diamond$$

limits to 0 as $N \rightarrow \infty$. In fact:

$$f \underset{\text{in a } \diamond}{\sim} g$$

sense

for all $g \in \mathcal{S}$.

Theorem 7.6.3

We have $|f - g|_\diamond = 0$ if and only if $f(x) = g(x)$ for all x except for x in a set for which when we integrate over it we get 0. That is, the area between the points of this set and the function is 0.

That is, they are equal to each other everywhere except on a very small set.

Proof. When we integrate $(f - g)^2 \geq 0$, we will get something ≥ 0 . By way of contradiction, if $(f - g)(x) > 0$ on a set which has “measure” bigger than zero, we will have a nonzero integral. See [4] for details on how to define such a measurement. \square

Two functions in the same class only differ from each other on a “very small set.”

Real Hilbert Space

Suppose our vectors are not simply functions but classes of functions where two functions are in the same class if and only if $|f - g|_\diamond = 0$. Every function in a class has the same \diamond length. Take all such classes that have finite \diamond length. Then, \diamond becomes a nice inner product on such a space of vectors. Not only that, but all sequences of vectors “which seem to be limiting” (explained below) in a \diamond sense actually do limit and that limit is in this vector space.

This vector space of *all* such classes of functions $f : [0, 1] \rightarrow \mathbb{R}$ of any kind that we can integrate (in a Lebesgue sense—explained below) so that \diamond is calculable and $|f|_\diamond$ is finite *is an example of a Hilbert Space—a special kind of a vector space where we can talk about limits of vectors!*

Let’s address the phrase “which seem to be limiting”

This means for a sequence f_n that for each $\epsilon > 0$, there exists a point in our sequence N , such that if $n, m > N$, then $|f_n - f_m|_\diamond < \epsilon$. The sequence elements are getting closer together. Such a sequence is called a **Cauchy sequence** and is useful for describing a sequence which seems like it should have a limit without actually referring to the limit itself in the description. A vector space is **complete** with respect to \diamond if every Cauchy sequence has a limit in that vector space. Hilbert spaces are complete inner product vector spaces.

What are these small sets to which we are referring? We know $|f - g|_\diamond = 0$ if and only if $f(x) \neq g(x)$ on a very small set.

For an example of a “small set” to which we are referring, imagine that we are finding the area under a function via integration that is 0 everywhere except at $x = \frac{1}{2}$ and $\frac{3}{4}$ where it is equal to 1. We are considering two infinitely thin rectangles of height 1. The area is 0. The set $\{\frac{1}{2}, \frac{3}{4}\}$ is an example of a “small set.” But our small sets do not have to be finite. They can even live with extremely high density within the interval $[0, 1]$.

For instance, consider removing all numbers in the interval $[0, 1]$ that have a 4 somewhere in their decimal expansion. If we remove just the numbers that have a 4 in the first decimal place, the resulting lengths of what is left add up to $\frac{9}{10}$ of what we had. Now omit from these all numbers that have a 4 in the second decimal place. This yields again $\frac{9}{10}$ of what we had at the previous step. Continuing this process on forever, the limiting resulting sum of lengths is 0. Such a set is not one you would normally integrate over using a Riemann integral normally taught in a calculus course. Riemann integrals happen over unions of intervals. The set we are referring to is a complicated mess as the result of a limiting process. However, when we change our definition of an integral to something called a “Lebesgue” integral, we can integrate over such a set—but no matter what function we integrate on such a set we will always get 0. Our set is what we call a “Lebesgue measure 0 set.”

Another example of a “Lebesgue measure 0 set” comes from considering base 3 decimal expansions where we have replaced any instance of an infinite repetition of 0’s with a repetition of 2’s in the same way in base 10 we can replace 1 with .9999 ···. Then, if we omit all numbers in $[0, 1]$ that have a 1 in this type of expansion, it is like we are taking out “middle thirds.” This type of “Lebesgue measure 0 set” is called the [Cantor set](#).

Lebesgue Integral

This is another way of defining integration. Instead of considering a limit of rectangle sums under a curve with decreasing rectangle width, we use a limit of sums of y_i values in the codomain multiplied by the measure of the preimage of $[y_i, y_{i+1}]$. Our limit happens as these codomain intervals decrease in length. The idea of how to measure sets and describe what kinds of sets are measurable is inherent in this type of integration. Riemann integrals are defined over unions of subintervals in the domain only. *The two types of integrals agree perfectly where they are both defined.* Yet Lebesgue integrals are necessary in our definition of \diamond so that we can have a Hilbert space where Cauchy sequences have limits. This in particular implies that the wave sums converge. Not only that, we know that our wave sums converge to our function (in a \diamond sense).

Equality in a \diamond sense

Let f and g be two functions $[0, 1] \rightarrow \mathbb{R}$ we can integrate. We say that f and g are equal in a \diamond sense if $f(x) \neq g(x)$ only for x values in a subset of $[0, 1]$ that has Lebesgue measure 0.

Lebesgue Measure 0 Set

This is a set over which any Lebesgue integral evaluates to 0.

Theorem 7.6.4 Fourier Series

The Fourier series of f where $|f|_\diamond$ is finite is the projection of f onto \mathcal{C} which is infinite dimensional. The function f is equal to its projection *in a \diamond sense*.

Proof. See [4]. □

Fourier Series is simply a Gram-Schmidt-type projection!

This equality means that f is in the span of \mathcal{C} so that we can use Parseval's (generalized Pythagorean) Identity given above:

Corollary 7.6.5 Parseval's Identity Infinite Version

$$|f|_{\diamond}^2 = \sum_{w \in \mathcal{C}} (f \diamond w)^2$$

This is an infinite Pythagorean Theorem for functions thought of as vectors and lengths thought of with respect to \diamond .

Proof. See [4]. □

Disappointing

Still, our convergence result is a little disappointing. Our sums eventually stabilize toward a class of \diamond 's version of “no change”—which is pretty wobbly. True, it is a nice setup if we want to work in a vector space and do linear algebra. What if we want to converge to a specific function? What if we want our infinite wave sum to match our function exactly at a point? But we could go further—what if we would like our wave sums to get closer to our function as a whole at a uniform rate???

There are many easy examples of functions with discontinuities so that $\sum_{w \in S_N} (f \diamond w)w$ actually converges to the function at most points. Just think of a step function with horizontal lines and jumps. We try to approximate the step function with a sum of waves which themselves are continuous. The wave sums $\sum_{w \in S_N} (f \diamond w)w$ will successfully converge “pointwise” to the function at each point along each horizontal step. As soon as we come to a jump, however, the y value that the wave sums will converge to will be right in the middle of the jump. This should make sense since the wave has to be connected. Yet we can add and cancel waves as much as we want inside of any of the horizontal regions until the wave is actually approximating the step. Notice that the wave sum at N will be different than f at all of the jumps.

Pointwise Convergence

We say that our sine and cosine wave sums converge pointwise to f if $\sum_{w \in S_N} (f \diamond w)w$ limits to $f(x)$ as $N \rightarrow \infty$ specifically at each point x .

Convergence in a \diamond sense does not guarantee pointwise convergence—not even on all points but a Lebesgue measure 0 set!

Consider taking the following sequence of functions. The first function f_1 is equal to 1 on $[0, \frac{1}{2}]$ and 0 elsewhere. Call $[0, \frac{1}{2}]$ the 1-interval of f_1 . For all the functions in the sequence that we build, suppose that they are identically 0 off of their 1-interval. We will just be moving the 1-intervals and sometimes shortening them as we progress through the sequence. Let f_2 have a 1-interval of $[0, \frac{1}{2}]$. The functions f_1 and f_2 have given us two 1-intervals overlapping only at endpoints that have moved across $[0, 1]$ each of length $\frac{1}{2}$. Now we repeat this process for 1-intervals of length $\frac{1}{4}$. There are four subintervals overlapping only at endpoints from left to right of length $\frac{1}{4}$ that go across $[0, 1]$. Let f_3, f_4, f_5 , and f_6 take these on as their 1-interval respectively. For instance, f_3 has a 1-interval of $[0, \frac{1}{4}]$ and f_4 has a 1-interval of $[\frac{1}{4}, \frac{1}{2}]$. We keep this up for 1-intervals of size $\frac{1}{8}, \frac{1}{16}$, etc. This sequence is like a “type writer” going back and forth where the piece that goes back and forth gets thinner at an exponential rate. The integral and for sure the \diamond length of f_n goes to 0. This means that f_n converges in a \diamond sense to the zero function. *But the convergence is so wobbly!* For a while we could have $f_n(x) = 0$ repeatedly. Yet eventually as the type writer moves across, again we will always have even for a moment $f_m(x) = 1$ for some $m > n$. So, for our fixed x value, *there is no limit of $f_n(x)$.*

Yet even with this type writer sequence, what if we just chose one just one function f_m for each pass and make a new sequence out of that. This sequence would actually converge pointwise to the 0 function at all points *except* for a Lebesgue measure 0 set. This is because the measure of the points that will evaluate to 1 sometime in the future after a step m is no more than adding together fractions $\frac{1}{2^{m+1}} + \frac{1}{2^{m+2}} + \dots$ As a geometric series, this sum is $\frac{1}{2^m}$. The measure of points where convergence will not be pointwise is heading swiftly to 0.

This same type of idea can be applied to our sequence of wave sums $\sum_{w \in S_N} (f \diamond w)w$. Even when we are just converging to f in a \diamond sense, it is possible to thin out our sequence to reduce the wobble and get *pointwise convergence at every point except on a Lebesgue measure 0 set*.

Still, there is a condition such that if a function satisfies it, then the wave sums will converge to f pointwise *at every point!*.

Bounded Variation

A function is said to have bounded variation on $[0, 1]$ if it does not oscillate too much or have an infinite asymptote. Technically we say that all the sums $\sum_{i=1}^n |f(x_{i+1}) - f(x_i)|$ where $0 = x_1 < x_2 < \dots \leq x_{n-1} < x_n = 1$ are smaller than some fixed bounding number.

Theorem 7.6.6 Pointwise Convergence

The wave sums $\sum_{w \in S_N} (f \diamond w)w$ for any function f in $C[0, 1]$ (so f is *continuous*) of bounded variation will converge pointwise to f . The wave sums will not necessarily get there uniformly—but eventually at each point things get close.

Proof. See [4]. □

What about if we want our wave sums to get close to our function in a uniform way?

 L^∞ -norm

We let the L^∞ norm of a function $[0, 1] \rightarrow$ to be:

$$|f|_\infty = \max\{f(x) : x \in [0, 1]\}$$

The measure of how close two functions f and g are to each other is given by $|f - g|_\infty$ which is the maximum distance that they are apart.

Uniform Convergence

We say that the wave sums converge uniformly to f if the maximum distance between $f(x)$ and $\sum_{w \in S_N} (f \diamond w)w$ (for any $x \in [0, 1]$) limits to 0. That is, $|f - \sum_{w \in S_N} (f \diamond w)w|_\infty \rightarrow 0$.

Uniform convergence is stronger than pointwise convergence. If a sequence of functions converges uniformly, then it will necessarily converge pointwise as well at each point in the domain.

Theorem 7.6.7 Uniform Convergence

Suppose that $f : [0, 1] \rightarrow \mathbb{R}$ is a function such that the usual distance between $f(x)$ and $f(y)$ does not exceed a constant multiple of a fixed positive power of the distance between the inputs x and y no matter which x and y we choose in $[0, 1]$. That is, $|f(x) - f(y)| \leq C|x - y|^t$ for some $t > 0$ for all $x, y \in [0, 1]$. Then, we are guaranteed that the wave sums $\sum_{w \in S_N} (f \diamond w)w$ converge to f uniformly.

Proof. See [5]. □

Uniform convergence means that the waves are getting close to the function together and not sporadically. So as N gets larger and larger, the wave sums appear more and more like the function f without any funny spikes along the way.

7.6.6 Fourier Series Example and π

Example 13. Let's compute the Fourier series of the function $f(x) = \frac{1}{2} - x$ over the interval $[0, 1]$. We are guaranteed pointwise convergence since this function is of bounded variation and continuous (no jumps). All we are doing is computing a lot of inner products. We will see how this Fourier series leads to a nice formula for π . First,

$$\left(\frac{1}{2} - x\right) \diamond 1 = \int_0^1 \left(\frac{1}{2} - x\right) dx = 0 \quad (\text{since area under } x\text{-axis equals area above}).$$

Now let's compute $(\frac{1}{2} - x) \diamond \sqrt{2} \cos(2n\pi x)$. In the integral, let's use the substitution $u = (\frac{1}{2} - x)$:

$$\sqrt{2} \int_{-\frac{1}{2}}^{\frac{1}{2}} u \cdot \cos \underbrace{\underbrace{2n\pi \cdot \left(\frac{1}{2} - u\right)}_{\pi \cdot n - 2n\pi u}}_{= \pm \cos(2n\pi u) \text{ an even function}} du = 0$$

Odd Function

So the coefficients of 1 and $\sqrt{2} \cos(2n\pi x)$ for $n \in \mathbb{N}$ are all 0. We only need to check the coefficients of $\sqrt{2} \sin(2n\pi x)$ which are given as $(\frac{1}{2} - x) \diamond \sqrt{2} \sin(2n\pi x)$. We do this by tabular integration by parts:

(+)	($\frac{1}{2} - x$)	
(-)	-1	
		integrate

This becomes

$$\left(\frac{1}{2} - x\right) \cdot \frac{-1}{n\pi\sqrt{2}} \cos(2n\pi x) \Big|_0^1 - \underbrace{\int_0^1 \frac{1}{n\pi\sqrt{2}} \cos(2n\pi x) dx}_{\text{By periodicity} = 0}$$

$$= \frac{1}{2\sqrt{2}} \cdot \frac{1}{n\pi} + \frac{1}{2\sqrt{2}} \cdot \frac{1}{n\pi} = \frac{1}{\sqrt{2}} \cdot \frac{1}{n\pi}$$

Therefore,

$$\left(\frac{1}{2} - x\right) = \sum_{n \in \mathbb{N}} \left(\frac{1}{\sqrt{2}} \cdot \frac{1}{n\pi} \right) \sqrt{2} \cdot \sin(2n\pi x)$$

Now, setting $x = \frac{1}{4}$, we have:

$$\left(\frac{1}{2} - \frac{1}{4}\right) = \frac{1}{\pi} \sum_{n \in \mathbb{N}} \frac{1}{n} \sin\left(2n\pi \cdot \frac{1}{4}\right)$$

$$\frac{\pi}{4} = \sum_{n \in \mathbb{N}} \frac{1}{n} \cdot \sin\left(n \cdot \frac{\pi}{2}\right)$$

Note that

$$\sin\left(n \cdot \frac{\pi}{2}\right) = \begin{cases} 0, & n \text{ is even} \\ 1, & n \text{ is 1 more than a multiple of 4} \\ -1, & n \text{ is 1 less than a multiple of 4} \end{cases}$$

So, we arrive at:

Leibniz Formula for π

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \dots$$

7.6.7 Gram-Schmidt and Polynomials

Example 14. Consider the collection of polynomials $1, x, x^2, \dots$. This is an infinite collection of linearly independent functions. For instance, try as you might you can not add up any linear combination of $1, x$ and get something that is quadratic like x^2 (*assuming that we are just letting x be free—not describing any matrix action or anything like as we have done sometimes*).

Let's start the Gram Schmidt process on this collection and try to come up with an orthonormal basis. Once in hand, one can approximate functions by linear combinations of this orthonormal basis much like as for Fourier series (i.e. when we use \mathcal{C}). The method of finding coefficients is the same—just using \diamond .

Let $v_i = x^i$. Then set $w_0 = 1$. We compute

$$w_1 = x - \frac{x \diamond 1}{1 \diamond 1} \cdot 1 = x - \frac{1}{2}$$

$$\begin{aligned}
w_2 &= x^2 - \underbrace{\frac{x^2 \diamond (x - \frac{1}{2})}{(x - \frac{1}{2}) \diamond (x - \frac{1}{2})}}_{\frac{\int_0^1 x^2 \cdot (x - \frac{1}{2}) dx}{\int_0^1 (x - \frac{1}{2})^2 dx}} \cdot x - \underbrace{\frac{x^2 \diamond 1}{1 \diamond 1} \cdot 1}_{\frac{\int_0^1 x^2 \cdot 1 dx}{\int_0^1 1 \cdot 1 dx}} \\
&= x^2 - \frac{\frac{1}{12}}{\frac{1}{12}} \left(x - \frac{1}{2} \right) - \frac{\frac{1}{3}}{1} \cdot 1 = x^2 - x + \frac{1}{6}
\end{aligned}$$

We can now turn w_0 , w_1 , and w_2 into an orthonormal collection by dividing by their lengths:

$$\begin{aligned}
\frac{w_0}{|w_0|_\diamond} &= 1 & \frac{w_1}{|w_1|_\diamond} &= \frac{x - \frac{1}{2}}{\int_0^1 (x - \frac{1}{2})^2 dx} = \frac{x - \frac{1}{2}}{\sqrt{\frac{1}{12}}} = \sqrt{12} \cdot \left(x - \frac{1}{2} \right) \\
\frac{w_2}{|w_2|_\diamond} &= \frac{x^2 - x + \frac{1}{6}}{\int_0^1 (x^2 - x + \frac{1}{6})^2 dx} = \frac{x^2 - x + \frac{1}{6}}{\sqrt{\frac{1}{180}}} = \sqrt{180} \cdot \left(x^2 - x + \frac{1}{6} \right)
\end{aligned}$$

Key Concepts from this Section

- **inner product:** (page 957) An inner product on \mathbb{R}^n is a positive definite symmetric bilinear transformation $T : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ given by:

$$T(u, v) = u \diamond v$$

- **inner products from matrices:** (page 957) Any positive definite symmetric matrix gives an inner product.

- **norm from an inner product:** (page 958) We let the norm or *length* of a vector with respect to an inner product \diamond be given by

$$|v|_\diamond = \sqrt{v \diamond v}$$

- **complex vector space:** (page 958) A vector space with scalars in \mathbb{C} is called a complex vector space
- **hermitian adjoint:** (page 959) The Hermitian adjoint A^* of a matrix A with entries in \mathbb{C} is $A^* = \overline{A}^T$ where \overline{A} means that we have taken the complex conjugate of each entry.
- **hermitian matrix:** (page 959) This is the analog to a matrix being symmetric—but when we have complex entries. A matrix is called Hermitian if $A = A^*$.
- **conjugate linear:** (page 959) A function $f : V \rightarrow W$ between complex vector spaces is called conjugate linear if it is additive and if $f(a \cdot v) = \bar{a} \cdot f(v)$. So when the scalar comes out, we take a conjugate of it. It is *conjugate scalable*.
- **hermitian inner product:** (page 959) Let V be a complex vector space. A Hermitian Inner Product is a “positive definite” and “Hermitian” function $T : V \times V \rightarrow \mathbb{C}$ which is linear in the first component and

conjugate linear in the second component. The word “positive definite” simply means that $T(v, v) > 0$ and “Hermitian” means that $T(u, v) = \overline{T(v, u)}$. We will write $u \square v = T(u, v)$ to signify a Hermitian inner product.

- **hermitian inner products from matrices:** (page 959) Take any positive definite Hermitian matrix A . Then we can define a Hermitian inner product:

$$u \square v = u^T A \bar{v}$$

- **standard hermitian inner product:** (page 960) The matrix $A = \text{id}_{n \times n}$ defines the standard Hermitian product.

- **hermitian norm of a vector:** (page 960) Given a vector v in a complex vector space V , we can define the norm

$$|v|_{\square} = \sqrt{v \square v}$$

- **unitary matrix:** (page 961) A Hermitian matrix A whose columns are orthonormal with respect to the standard Hermitian inner product is called *unitary*. It is the analog to an orthogonal matrix.

- **theorem 7.6.1 :** (page 961) Hermitian matrices are diagonalizable with a matrix U which is unitary.

- **$C[0, 1]$:** (page 961) Let $C[0, 1]$ denote the vector space consisting of continuous functions $[0, 1] \rightarrow \mathbb{R}$.

- **inner product on $C[0, 1]$:** (page 961) Let $f, g \in C[0, 1]$. Then, we can define an inner product $f \diamond g = \int_0^1 f(x)g(x) dx$.

- **orthogonality:** (page 962) With respect to an inner product \diamond , two vectors v and w are orthogonal if $v \diamond w = 0$.

- **distance:** (page 962) We define the distance between two vectors v and w with respect to \diamond as $|v - w|_{\diamond}$.

- **projection onto a subspace:** (page 963) Suppose that W is a subspace of V and that $\{w_1, \dots, w_k\}$ is an orthonormal basis for W . Then, the projection of a vector v onto W is:

$$(v \bullet w_1)w_1 + (v \bullet w_2)w_2 + \cdots + (v \bullet w_k)w_k$$

- **inner product projection onto a subspace:** (page 964) Suppose that W is a subspace of V and that $\{w_1, \dots, w_k\}$ is an orthonormal basis for W with respect to \diamond . Then, the projection of a vector f onto W is:

$$(f \diamond w_1)w_1 + (f \diamond w_2)w_2 + \cdots + (f \diamond w_k)w_k$$

- **corollary 7.6.2 parseval's identity:** (page 964) Suppose that $f = a_1 w_1 + \dots + a_k w_k$ where $\{w_1, \dots, w_k\}$ is an orthonormal basis for W with respect to \diamond . Then,

$$|f|_{\diamond}^2 = a_1^2 + a_2^2 + \dots + a_k^2$$

This is like a generalized Pythagorean Identity a.k.a. Parseval's Identity.

- **an infinite orthonormal set:** (page 965) The functions $1, \sqrt{2} \cos(2n\pi x)$ for each $n \in \mathbb{N}$ and $\sqrt{2} \sin(2n\pi x)$ for each $n \in \mathbb{N}$ together make up an infinite orthonormal set. Call this infinite collection \mathcal{C} . Let S_N denote the subcollection of \mathcal{C} consisting of functions $1, \sqrt{2} \cos(2n\pi x)$, and $\sqrt{2} \sin(2n\pi x)$ for $n \leq N$.
- **fourier series and closeness:** (page 965) Let $f \in C[0, 1]$. As $N \rightarrow \infty$, the projection of f onto the span $\langle S_N \rangle$ gets arbitrarily “close” to f . This “limiting projection” is called the Fourier series of f . Yet we will define “closeness” in a \diamond sense. That is, given any positive distance $\epsilon > 0$, there exists N such that

$$\left| f - \sum_{w \in S_N} (f \diamond w) w \right|_{\diamond} < \epsilon$$

- **class of functions:** (page 966) Suppose that g and h are functions $[0, 1] \rightarrow \mathbb{R}$, which although possibly not continuous, have well-defined lengths $|g|_{\diamond}$ and $|h|_{\diamond}$ which are finite. We say that f and g are in the same class of functions with respect to \diamond if $|f - g|_{\diamond} = 0$.
- **converging to a class of functions:** (page 966) We let “ \mathcal{S} ” be the whole “class” of functions g such that

$$\left| g - \sum_{w \in S_N} (f \diamond w) w \right|_{\diamond}$$

limits to 0 as $N \rightarrow \infty$. In fact:

$$f \underset{\text{in a } \diamond}{\underbrace{\sim}} g$$

in a \diamond
sense

for all $g \in \mathcal{S}$.

- **theorem 7.6.3 :** (page 966) We have $|f - g|_{\diamond} = 0$ if and only if $f(x) = g(x)$ for all x except for x in a set for which when we integrate over it we get 0. That is, the area between the points of this set and the function is 0. That is, they are equal to each other everywhere except on a very small set.
- **real hilbert space:** (page 967) Suppose our vectors are not simply functions but classes of functions where two functions are in the same class if and only if $|f - g|_{\diamond} = 0$. Every function in a class has the same \diamond length. Take all such classes that have finite \diamond length. Then, \diamond becomes a nice inner product

on such a space of vectors. Not only that, but all sequences of vectors “which seem to be limiting” (explained below) in a \diamond sense actually do limit and that limit is in this vector space.

This vector space of *all* such classes of functions $f : [0, 1] \rightarrow \mathbb{R}$ of any kind that we can integrate (in a Lebesgue sense—explained below) so that \diamond is calculable and $|f|_\diamond$ is finite *is an example of a Hilbert Space—a special kind of a vector space where we can talk about limits of vectors!*

- **cauchy sequence:** (page 967) A sequence f_n is called Cauchy if for each $\epsilon > 0$, there exists a point in our sequence N , such that if $n, m > N$, then $|f_n - f_m|_\diamond < \epsilon$.
- **complete:** (page 967) A vector space is called complete with respect to \diamond if every Cauchy sequence has a limit in that vector space. Hilbert spaces are complete inner product vector spaces.
- **cantor set:** (page 968) This is an example of a Lebesgue measure 0 set. Consider base 3 decimal expansions of numbers in $[0, 1]$ where we have replace any instance of an infinite repetition of 0's with a repetition of 2's in the same way in base 10 we can replace 1 with .9999... Then, if we omit all numbers in $[0, 1]$ that have a 1 in this type of expansion, it is like we are taking out “middle thirds.”
- **lebesgue integral:** (page 968) This is another way of defining integration. Instead of considering a limit of rectangle sums under a curve with decreasing rectangle width, we use a limit of sums of y_i values in the codomain multiplied by the measure of the preimage of $[y_i, y_{i+1}]$. Our limit happens as these codomain intervals decrease in length. The idea of how to measure sets and describe what kinds of sets are measurable is inherent in this type of integration. Riemann integrals are defined over unions of subintervals in the domain only. *The two types of integrals agree perfectly where they are both defined.* Yet Lebesgue integrals are necessary in our definition of \diamond so that we can have a Hilbert space where Cauchy sequences have limits. This in particular implies that the wave sums converge. Not only that, we know that our wave sums converge to our function (in a \diamond sense).
- **equality in a \diamond sense:** (page 968) Let f and g be two functions $[0, 1] \rightarrow \mathbb{R}$ we can integrate. We say that f and g are equal in a \diamond sense if $f(x) \neq g(x)$ only for x values in a subset of $[0, 1]$ that has Lebesgue measure 0.
- **lebesgue measure 0 set:** (page 968) This is a set over which any Lebesgue integral evaluates to 0.
- **theorem 7.6.4 fourier series:** (page 968) The Fourier series of f where $|f|_\diamond$ is finite is the projection of f onto \mathcal{C} which is infinite dimensional. The function f is equal to its projection *in a \diamond sense.*
- **corollary 7.6.5 parseval's identity infinite version:** (page 969)

$$|f|_\diamond^2 = \sum_{w \in \mathcal{C}} (f \diamond w)^2$$

This is an infinite Pythagorean Theorem for functions thought of as vectors and lengths thought of with respect to \diamond .

- **pointwise convergence:** (page 969) We say that our sine and cosine wave sums converge pointwise to f if $\sum_{w \in S_N} (f \diamond w)w$ limits to $f(x)$ as $N \rightarrow \infty$ specifically at each point x .
- **bounded variation:** (page 970) A function is said to have bounded variation on $[0, 1]$ if it does not oscillate too much or have an infinite asymptote. Technically we say that all the sums $\sum_{i=1}^m |f(x_{i+1}) - f(x_i)|$ where $0 = x_1 < x_2 < \dots \leq x_{n-1} < x_n = 1$ are smaller than some fixed bounding number.
- **theorem 7.6.6 pointwise convergence:** (page 970) The wave sums $\sum_{w \in S_N} (f \diamond w)w$ for any function f in $C[0, 1]$ (so f is *continuous*) of bounded variation will converge pointwise to f . The wave sums will not necessarily get there uniformly—but eventually at each point things get close.
- **L^∞ -norm:** (page 971) We let the L^∞ norm of a function $[0, 1] \rightarrow$ to be:

$$\|f\|_\infty = \max\{f(x) : x \in [0, 1]\}$$

- **uniform convergence:** (page 971) We say that the wave sums converge uniformly to f if the maximum distance between $f(x)$ and $\sum_{w \in S_N} (f \diamond w)w$ (for any $x \in [0, 1]$) limits to 0. That is, $\|f - \sum_{w \in S_N} (f \diamond w)w\|_\infty \rightarrow 0$.
- **theorem 7.6.7 uniform convergence:** (page 971) Suppose that $f : [0, 1] \rightarrow \mathbb{R}$ is a function such that the usual distance between $f(x)$ and $f(y)$ does not exceed a constant multiple of a fixed positive power of the distance between the inputs x and y no matter which x and y we choose in $[0, 1]$. That is, $|f(x) - f(y)| \leq C|x - y|^t$ for some $t > 0$ for all $x, y \in [0, 1]$. Then, we are guaranteed that the wave sums $\sum_{w \in S_N} (f \diamond w)w$ converge to f uniformly.
- **leibniz formula for π :** (page 973)

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \dots$$

7.6.8 Exercises

When a Form Defines an Inner Product

Determine which of the following bilinear forms determine an inner product. Explain.

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

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

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

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

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

6. $\begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}$

7. $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$

8. $\begin{pmatrix} 4 & 4 \\ 4 & 4 \end{pmatrix}$

9. $\begin{pmatrix} 0 & 4 \\ 1 & 1 \end{pmatrix}$

10. $\begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix}$

Practice with Inner Products

11. $\diamond : \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$

$u = (-2, -3) \quad v = (3, 1) \quad w = (1, -3)$

Compute: $u \diamond ((-2)v - w)$

12. $\diamond : \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$

$u = (2, -2) \quad v = (-3, -2) \quad w = (1, 3)$

Compute: $u \diamond (w + v)$

13. $\diamond : \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$

$u = (3, 2) \quad v = (-2, 3) \quad w = (3, -3)$

Compute: $u \diamond ((-2)v - w)$

14. $\diamond : \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$

$u = (-2, -2) \quad v = (-3, 1) \quad w = (2, 1)$

Compute: $u \diamond ((-2)v - w)$

15. $\diamond : \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$
 $u = (3, -3) \quad v = (-2, -2) \quad w = (2, 2)$
 Compute: $u \diamond ((-3)v - w)$

16. $\diamond : \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$
 $u = (-2, 3) \quad v = (1, -2) \quad w = (1, 2)$
 Compute: $(-3)u \diamond (w + (-2)v)$

17. $\diamond : \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$
 $u = (1, 2) \quad v = (-3, 3) \quad w = (-2, 1)$
 Compute: $u \diamond v - 3w \diamond v$

18. $\diamond : \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$
 $u = (-2, 3) \quad v = (-2, -3) \quad w = (1, 2)$
 Compute: $(-2)u \diamond (w + v)$

19. $\diamond : \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$
 $u = (-3, -3) \quad v = (2, -3) \quad w = (2, 2)$
 Compute: $u \diamond (3v - w)$

20. $\diamond : \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$
 $u = (1, 1) \quad v = (-3, -2) \quad w = (-3, -3)$
 Compute: $u \diamond v - (-3)w \diamond v$

Computing Lengths with Respect to Inner Products

Compute $|u|_\diamond$ for each of the following.

21. $\diamond : \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$
 $u = (-3, 1)$

22. $\diamond : \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$
 $u = (-3, 2)$

23. $\diamond : \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$
 $u = (2, 3)$

24. $\diamond : \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$
 $u = (-2, 1)$

25. $\diamond : \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$
 $u = (2, 3)$

26. $\diamond : \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$
 $u = (-3, -3)$

27. $\diamond : \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$
 $u = (-3, 1)$

28. $\diamond : \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$
 $u = (2, -2)$

29. $\diamond :$
$$\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$$
$$u = (-3, 2)$$

30. $\diamond :$
$$\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$$
$$u = (2, 3)$$

31. $f \diamond g = \int_0^1 fg \, dx :$
$$u = -2x + 1$$

32. $f \diamond g = \int_0^1 fg \, dx :$
$$u = -3x + 1$$

33. $f \diamond g = \int_0^1 fg \, dx :$
$$u = 2$$

34. $f \diamond g = \int_0^1 fg \, dx :$
$$u = x - 2$$

Gram-Schmidt with an Integral Inner Product

Apply Gram Schmidt to convert each of the following into a collection of functions which are orthogonal to each other with respect to the following inner product:

$$f \diamond g = \int_0^1 f \cdot g \, dx$$

35. $1, x^4, x^6$

36. $1, x, x^3$

37. $1, x^2, x^6$

38. $1, x, x^4$

39. $1, x^2, x^4$

40. $1, x, x^2$

41. $1, x, x^3$

42. $1, x^2, x^5$

43. $1, x, x^2$

44. $1, x^4, x^6$

Orthonormal Functions

Use Gram Schmidt and rescaling to convert the following into orthonormal collections with respect to the inner product:

$$f \diamond g = \int_0^1 f \cdot g \, dx$$

45. 1, x^4 , x^6

46. 1, x , x^3

47. 1, x , x^2

48. 1, x^3 , x^6

49. 1, x , x^6

50. 1, x^2 , x^6

51. 1, x^4 , x^5

52. 1, x^3 , x^4

53. 1, x , x^3

54. 1, x^2 , x^3

7.6.9 Solutions

- 1.** This symmetric matrix is not positive definite. Consider its characteristic polynomial: $x^2 - 2x$.
- 2.** The matrix is not even symmetric.
- 3.** The matrix is not even symmetric.
- 4.** This symmetric matrix is not positive definite. Consider its characteristic polynomial: $x^2 - x - 1$.
- 5.** yes
- 6.** This symmetric matrix is not positive definite. Consider its characteristic polynomial: $x^2 - 6x$.
- 7.** yes
- 8.** This symmetric matrix is not positive definite. Consider its characteristic polynomial: $x^2 - 8x$.
- 9.** This symmetric matrix is not positive definite. Consider its characteristic polynomial: $x^2 - 2x - 15$.
- 10.** yes
- 11.** 101
- 12.** -6
- 13.** -23
- 14.** -6
- 15.** 0
- 16.** -75
- 17.** -24
- 18.** 6
- 19.** 63
- 20.** 200

21. $\sqrt{14}$

22. $\sqrt{15}$

23. $2\sqrt{22}$

24. $2\sqrt{2}$

25. $3\sqrt{7}$

26. $3\sqrt{10}$

27. $3\sqrt{2}$

28. $2\sqrt{2}$

29. $\sqrt{15}$

30. $3\sqrt{7}$

31. $\sqrt{\frac{1}{3}}$

32. 1

33. 2

34. $\sqrt{\frac{7}{3}}$

35. 1,

$$\begin{aligned}x^4 - \frac{1}{5}, \\x^6 - \frac{135}{154}x^4 + \frac{5}{154}\end{aligned}$$

36. 1,

$$\begin{aligned}x - \frac{1}{2}, \\x^3 - \frac{9}{10}x + \frac{1}{5}\end{aligned}$$

37. 1,

$$\begin{aligned}x^2 - \frac{1}{3}, \\x^6 - \frac{5}{7}x^2 + \frac{2}{21}\end{aligned}$$

38. 1,

$$\begin{aligned}x - \frac{1}{2}, \\x^4 - \frac{4}{5}x + \frac{1}{5}\end{aligned}$$

39. 1,

$$\begin{aligned}x^2 - \frac{1}{3}, \\x^4 - \frac{6}{7}x^2 + \frac{3}{35}\end{aligned}$$

40. 1,

$$\begin{aligned}x - \frac{1}{2}, \\x^2 - x + \frac{1}{6}\end{aligned}$$

41. 1,

$$\begin{aligned}x - \frac{1}{2}, \\x^3 - \frac{9}{10}x + \frac{1}{5}\end{aligned}$$

42. 1,

$$\begin{aligned}x^2 - \frac{1}{3}, \\x^5 - \frac{25}{32}x^2 + \frac{3}{32}\end{aligned}$$

43. 1,

$$\begin{aligned}x - \frac{1}{2}, \\x^2 - x + \frac{1}{6}\end{aligned}$$

44. 1,

$$\begin{aligned}x^4 - \frac{1}{5}, \\x^6 - \frac{135}{154}x^4 + \frac{5}{154}\end{aligned}$$

45. 1,

$$\begin{aligned}\frac{15}{4}x^4 - \frac{3}{4}, \\ \frac{13}{24}\sqrt{\frac{1}{13}}(154x^6 - 135x^4 + 5)\end{aligned}$$

46. 1,

$$\begin{aligned}3\sqrt{\frac{1}{3}}(2x - 1), \\ \frac{7}{3}\sqrt{\frac{1}{7}}(10x^3 - 9x + 2)\end{aligned}$$

47. 1,

$$\begin{aligned}3\sqrt{\frac{1}{3}}(2x - 1), \\ 5\sqrt{\frac{1}{5}}(6x^2 - 6x + 1)\end{aligned}$$

48. 1,

$$\begin{aligned}\frac{7}{3}\sqrt{\frac{1}{7}}(4x^3 - 1), \\ \frac{13}{9}\sqrt{\frac{1}{13}}(35x^6 - 28x^3 + 2)\end{aligned}$$

49. 1,

$$\begin{aligned}3\sqrt{\frac{1}{3}}(2x - 1), \\ \frac{13}{15}\sqrt{\frac{1}{13}}(28x^6 - 18x + 5)\end{aligned}$$

50. 1,

$$\begin{aligned}\frac{5}{2}\sqrt{\frac{1}{5}}(3x^2 - 1), \\ \frac{13}{8}\sqrt{\frac{1}{13}}(21x^6 - 15x^2 + 2)\end{aligned}$$

51. 1,

$$\begin{aligned}\frac{15}{4}x^4 - \frac{3}{4}, \\ \frac{11}{4}\sqrt{\frac{1}{11}}(48x^5 - 45x^4 + 1)\end{aligned}$$

52. 1,

$$\begin{aligned}\frac{7}{3}\sqrt{\frac{1}{7}}(4x^3 - 1), \\ 30x^4 - 28x^3 + 1\end{aligned}$$

53. 1,

$$\begin{aligned}3\sqrt{\frac{1}{3}}(2x - 1), \\ \frac{7}{3}\sqrt{\frac{1}{7}}(10x^3 - 9x + 2)\end{aligned}$$

54. 1,

$$\begin{aligned}\frac{5}{2}\sqrt{\frac{1}{5}}(3x^2 - 1), \\ \frac{7}{2}\sqrt{\frac{1}{7}}(16x^3 - 15x^2 + 1)\end{aligned}$$

Chapter 7 Selected Review Questions

Section 7.1

Can you rewrite a vector v in $\mathbb{R}[x]^3$ as a vector in \mathbb{R}^3 *without polynomial entries* if x is given by a matrix?

1. $(-x^2 + 1, x^2, 2)$

2. $(-x + 2, -x, x + 1)$

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

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

Can you use the characteristic polynomial and generalized synthetic division to find a matrix powers?

3. $\begin{pmatrix} 0 & 2 \\ 1 & -1 \end{pmatrix}^7$

4. $\begin{pmatrix} 0 & -2 \\ 1 & -1 \end{pmatrix}^7$

Can you find a nonrecursive formula for a_n using a system of equations to determine a matrix power?

5. $a_{n+2} = 2a_n + (-1)a_{n+1}$

$$a_0 = 2, \quad a_1 = -2$$

6. $a_{n+2} = 6a_n + (1)a_{n+1}$

$$a_0 = -1, \quad a_1 = 2$$

Section 7.2

Can you find the characteristic polynomial of a matrix using sums of determinants of central submatrices?

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

8. $\begin{pmatrix} 0 & 0 & 1 \\ -1 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$

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

10.
$$\begin{pmatrix} 2 & 0 & 0 & 1 \\ -1 & 0 & -1 & 1 \\ 2 & 2 & -1 & 2 \\ 2 & 2 & 0 & 0 \end{pmatrix}$$

Given an incidence matrix, can you determine the number of spanning trees of the digraph using the technique in the text?

11.
$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ -1 & -1 & 0 & 1 \\ 0 & 1 & -1 & -1 \end{pmatrix}$$

12.
$$\begin{pmatrix} -1 & 1 & 1 & 0 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

Section 7.3

Can you find minimal polynomials of matrices?

13.
$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

14.
$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

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

16.
$$\begin{pmatrix} 0 & 2 & -1 \\ 0 & 0 & 0 \\ 0 & 2 & -1 \end{pmatrix}$$

Can you find invariant subspaces that turn up in the column process of computing the minimal polynomial?

17.
$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & -1 & 1 \\ -1 & 0 & -2 \end{pmatrix}$$

18.
$$\begin{pmatrix} -1 & 1 & 2 \\ 0 & -2 & -2 \\ 0 & 0 & -1 \end{pmatrix}$$

Section 7.4

Can you diagonalize a matrix using kernels? If A denotes the matrix, find U and a diagonal matrix D so that $D = U^{-1}AU$.

19. $\begin{pmatrix} -1 & -2 & -6 \\ 1 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}$

20. $\begin{pmatrix} 1 & -2 & 10 \\ 1 & -1 & 5 \\ 0 & 1 & -1 \end{pmatrix}$

Can you diagonalize a matrix using ranges? If A denotes the matrix, find U and a diagonal matrix D so that $D = U^{-1}AU$.

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

22. $\begin{pmatrix} 1 & 0 & -2 \\ 1 & -1 & -1 \\ 0 & 0 & -1 \end{pmatrix}$

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

24. $\begin{pmatrix} -4 & 9 \\ -2 & 5 \end{pmatrix}$

Section 7.5

Can you orthogonally diagonalize a matrix? If A denotes the matrix, find an orthogonal matrix U and a diagonal matrix D so that $D = U^{-1}AU$.

25. $\begin{pmatrix} -2 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & -1 \end{pmatrix}$

26. $\begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & -1 \end{pmatrix}$

27. $\begin{pmatrix} 4 & 1 & 1 \\ 1 & 4 & 1 \\ 1 & 1 & 4 \end{pmatrix}$

28. $\begin{pmatrix} -3 & 4 & 4 & 0 \\ 4 & -3 & 4 & 0 \\ 4 & 4 & -3 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}$

Can you determine whether a function has a maximum, minimum or neither at a critical point using the second derivative matrix?

29. $f(x, y) = 2x^2 + 2xy + 2y^2 - 10x - 8y + \cos(x - 2) + 13$
with critical point: $(2, 1)$

30. $f(x, y) = -4x^2 - 2xy - 4y^2 - 2x - 8y - \cos(x) - 4$
with critical point: $(0, -1)$

31. $f(x, y) = -x^2 - 2y^2 - 4xz - yz - 2z^2 - 2x + 8y - 2z - \cos(z) - 9$

with critical point: $(-1, 2, 0)$

32. $f(x, y) = 4x^2 + xy + 4y^2 + 2yz + z^2 + 16x + 2y + \cos(y) + 16$

with critical point: $(-2, 0, 0)$

Can you determine if a matrix is positive definite, negative definite or neither just by looking at the characteristic polynomial?

33. $x^3 - 17x^2 + 69x + 18$

34. $x^3 + 17x^2 + 81x + 78$

35. $x^3 - 17x^2 + 81x - 78$

Can you find at which angle which simple conic was rotated by to have a given equation?

36. $\frac{25}{2}x^2 + 7xy + \frac{25}{2}y^2 = 144$

37. $-4\sqrt{3}xy + 3x^2 + 7y^2 = 9$

Section 7.6

Can you determine when and why a matrix either defines or does not define an inner product?

38.
$$\begin{pmatrix} 0 & 2 \\ 1 & 4 \end{pmatrix}$$

39.
$$\begin{pmatrix} 0 & 2 \\ 1 & 4 \end{pmatrix}$$

Can you perform arithmetic with inner products? Assuming that \diamond is the inner product defined by the given matrix, evaluate the expression.

40. $\diamond : \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$
 $u = (3, -3) \quad v = (-2, 2) \quad w = (1, 3)$
Compute: $u \diamond ((-3)v - w)$

41. $\diamond : \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$
 $u = (1, 1) \quad v = (-2, 3) \quad w = (2, 2)$
Compute: $u \diamond (v - w)$

Can you find lengths of vectors with respect to inner products? Compute $|u|_\diamond$ for each of the following.

42. $\diamond : \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$
 $u = (1, 3)$

43. $\diamond : \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$
 $u = (-2, 2)$

44. $f \diamond g = \int_0^1 fg \, dx$:
 $u = x - 3$

45. $f \diamond g = \int_0^1 fg \, dx$:
 $u = x + 1$

Can you apply Gram Schmidt when the inner product is different from the dot product—even when it is defined via integration? Assume that $f \diamond g = \int_0^1 fg \, dx$. Apply Gram Schmidt to the following sets of vectors with respect to \diamond to find an orthonormal collection of functions.

46. $1, x, x^2$

47. $1, x, x^3$

Solutions/Hints

1. $(0, 1, 2)$

2. $(4, -2, 3)$

3. Characteristic Polynomial:

$$x^2 + x - 2$$

Remainder:

$$43x - 42$$

Matrix power:

$$\begin{pmatrix} -42 & 86 \\ 43 & -85 \end{pmatrix}$$

4. Characteristic Polynomial:

$$x^2 + x + 2$$

Remainder:

$$7x + 10$$

Matrix power:

$$\begin{pmatrix} 10 & -14 \\ 7 & 3 \end{pmatrix}$$

5. $a_n = \left(\frac{4}{3}\right)(-2)^n + \frac{2}{3}$

6. $a_n = (-(-2)^n)$

7. $x^3 - x^2 - 5x + 3$

8. $x^3 - 4x^2 + 4x$

9. $x^4 + 2x^3 - 3x^2$

10. $x^4 - x^3 - 4x^2 + 2x - 2$

11. 5

12. 6

13. Minimal polynomial:

$$(x - 1)^2$$

Characteristic polynomial: $(x - 1)^3$

14. Minimal polynomial:

$$(x - 1) \cdot (x + 1)$$

Characteristic polynomial: $(x + 1) \cdot (x - 1)^2$

15. Minimal polynomial:

$$(x + 2)^2$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 + 5x + 6 & x^2 + 4x + 4 \\ -1 & 0 & 0 \\ -1 & -x - 2 & 0 \end{pmatrix}$$

16. Minimal polynomial:

$$x \cdot (x + 1)$$

Possible result of column operations:

$$\begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2}x & x^2 & \frac{1}{2}x^2 + \frac{1}{2}x \\ 1 & -2x & 0 \end{pmatrix}$$

17. Minimal polynomial:

$$(x + 1)^2$$

Invariant Subspaces:

$$\langle(0, 1, 0)\rangle \text{ and } \langle(-1, 0, 0), (0, -1, 1)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} x & x^2 + x & -x^2 - 2x - 1 \\ -1 & 0 & 0 \\ 1 & x + 1 & 0 \end{pmatrix}$$

18. Minimal polynomial:

$$(x + 1) \cdot (x + 2)$$

Invariant Subspaces:

$$\langle(0, 1, -\frac{1}{2})\rangle \quad \text{and}$$

$$\langle(0, 0, 1), (2, -2, -1)\rangle$$

Possible result of column operations:

$$\begin{pmatrix} 1 & 0 & 0 \\ -x - 2 & x + 1 & 0 \\ 0 & -\frac{1}{2}x - \frac{1}{2} & x^2 + 3x + 2 \end{pmatrix}$$

$$\begin{aligned} \mathbf{19.} \quad D &= \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \\ U &= \begin{pmatrix} 4 & -2 & -2 \\ -3 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \mathbf{20.} \quad D &= \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -2 \end{pmatrix} = \\ U &= \begin{pmatrix} 4 & -5 & -4 \\ 3 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \mathbf{21.} \quad D &= \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2 \end{pmatrix} = \\ U &= \begin{pmatrix} 4 & -3 & -3 \\ 0 & 2 & -2 \\ 0 & 1 & 1 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \mathbf{22.} \quad D &= \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \\ U &= \begin{pmatrix} 0 & -2 & 2 \\ 1 & -1 & 1 \\ 0 & -2 & 0 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \mathbf{23.} \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} &= \\ \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} & \end{aligned}$$

$$\begin{aligned} \mathbf{24.} \quad \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix} &= \\ \begin{pmatrix} -1 & 3 \\ 2 & -3 \end{pmatrix} \begin{pmatrix} -4 & 9 \\ -2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \frac{2}{3} & \frac{1}{3} \end{pmatrix} & \end{aligned}$$

$$\begin{aligned} \mathbf{25.} \quad D &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix} \\ P &= \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix} \end{aligned}$$

26. $D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$

 $P = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \end{pmatrix}$

27. $D = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

 $P = \begin{pmatrix} \frac{1}{3}\sqrt{3} & \frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & 0 & \frac{2}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & -\frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \end{pmatrix}$

after Gram-Schmidt on:

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

28. $D = \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & -7 & 0 \\ 0 & 0 & 0 & -7 \end{pmatrix}$

 $P = \begin{pmatrix} \frac{1}{3}\sqrt{3} & 0 & \frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & 0 & 0 & \frac{2}{3}\sqrt{\frac{3}{2}} \\ \frac{1}{3}\sqrt{3} & 0 & -\frac{1}{2}\sqrt{2} & -\frac{1}{3}\sqrt{\frac{3}{2}} \\ 0 & 1 & 0 & 0 \end{pmatrix}$

after Gram-Schmidt on:

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

29. First Derivative:

$(4x + 2y - \sin(x - 2) - 10, 2x + 4y - 8)$

Second Derivative:

$$\begin{pmatrix} -\cos(x - 2) + 4 & 2 \\ 2 & 4 \end{pmatrix}$$

Characteristic Polynomial:

$x^2 - 7x + 8$

minimum

30. First Derivative:

$(-8x - 2y + \sin(x) - 2, -2x - 8y - 8)$

Second Derivative:

$$\begin{pmatrix} \cos(x) - 8 & -2 \\ -2 & -8 \end{pmatrix}$$

Characteristic Polynomial:

$x^2 + 15x + 52$

maximum

31. First Derivative:

$$(-2x - 4z - 2, -4y - z + 8, -4x - y - 4z + \sin(z) - 2)$$

Second Derivative:

$$\begin{pmatrix} -2 & 0 & -4 \\ 0 & -4 & -1 \\ -4 & -1 & \cos(z) - 4 \end{pmatrix}$$

Characteristic Polynomial:

$$x^3 + 9x^2 + 9x - 42$$

neither

32. First Derivative:

$$(8x + y + 16, x + 8y + 2z - \sin(y) + 2, 2y + 2z)$$

Second Derivative:

$$\begin{pmatrix} 8 & 1 & 0 \\ 1 & -\cos(y) + 8 & 2 \\ 0 & 2 & 2 \end{pmatrix}$$

Characteristic Polynomial:

$$x^3 - 17x^2 + 81x - 78$$

minimum

33. neither

34. negative definite

35. positive definite

36. $\theta = -45^\circ$

$$9x^2 + 16y^2 = 144$$

37. $\theta = +30^\circ$

$$x^2 + 9y^2 = 9$$

38. The matrix is not even symmetric.

39. yes

40. 42

41. -9

42. $\sqrt{26}$

43. $2\sqrt{2}$

44. $\sqrt{\frac{19}{3}}$

45. $\sqrt{\frac{7}{3}}$

46. 1,

$$\begin{aligned}x - \frac{1}{2}, \\x^2 - x + \frac{1}{6}\end{aligned}$$

47. 1,

$$\begin{aligned}x - \frac{1}{2}, \\x^3 - \frac{9}{10}x + \frac{1}{5}\end{aligned}$$

Part III

Number Theory and Other Applications of Linear Algebra

Differential Equations and More on Rotations

8

Differential Equations

8.1

8.1.1 Exercises	1009
8.1.2 Solutions	1010

Questions to Guide Your Study:

- *What are some examples of differential equations? What are they?*
- *How is solving a “linear differential equation” the same as finding the fiber of a linear transformation?*
- *How can we determine the dimension of the kernel of linear transformation which describes a differential equation?*
- *How can diagonalization of a matrix help to solve a simple differential equation given by a matrix?*

Real Analytic Functions on an interval

A function is said to be real analytic on an interval (a, b) if it can be expressed as a power series

$$\sum_{n=0}^{\infty} a_n(x - c)^n$$

for $c \in (a, b)$ that converges on the interval (a, b) .

C^n Functions

A function is said to be C^n on an interval (a, b) if it and its derivatives down to the n th derivative are all continuous functions on that interval.

$C^\omega[a, b]$

The notion of being a real analytic function is stronger than even being a C^∞ function (i.e. having all derivatives that are continuous and defined). *This is because if a function has a powers series representation that is well defined over an open interval, it has derivatives of all orders that are well defined and continuous on that open interval.* Without going into detail, we provide a little rationale: for any $c \in (a, b)$, one can write $f(x)$ nearby c as a sum of terms $a_m(x - c)^m$. The m th derivative on plugging in c to see things vanish is $m!a_m$.

The symbol ω sometimes is used to denote “something that is more than all of the counting numbers $1, 2, 3, \dots$ ” That is, something that is more than ∞ . *This notation here however only signifies that we have something stronger than C^∞ nothing else...* So we use the notation $C^\omega(a, b)$ to denote all of the real analytic functions over an interval (a, b) .

The set $C^\omega(a, b)$ is a vector space!

Linear Operator

Define L to be the function $C^\omega(a, b) \rightarrow C^\omega(a, b)$ given by:

$$L(f) = c_1 f'' + c_2 f' + c_3 f$$

for real constants c_1, c_2, c_3 . This is an example of a linear transformation. It is additive and scalable.

We have a neat way of expressing the fibers of such a linear operator.

Theorem 8.1.1

Let $c \in (a, b)$. Every element f in $L^{-1}(g)$ is uniquely representable within that fiber by the values $(f(c), f'(c))$. That is, no other function h in that fiber has $(h(c), h'(c)) = (f(c), f'(c))$. Also, for any pair of values (t, w) , there is $f \in L^{-1}(g)$ such that $(f(c), f'(c)) = (t, w)$. That is, every element in the fiber is expressible uniquely by an element in \mathbb{R}^2 .

Proof. Suppose that

$$f(x) = \sum_{n=0}^{\infty} a_n (x - c)^n$$

Then,

$$f'(x) = \sum_{n=0}^{\infty} (n+1)a_{n+1}(x-c)^n$$

since the exponent of a term $a_{n+1}x^{n+1}$ has been reduced by 1 and the coefficient has been multiplied by $(n+1)$.

Also:

$$f''(x) = \sum_{n=0}^{\infty} (n+1)(n+2)a_{n+2}(x-c)^n$$

since the exponent of a term $(n+2)a_{n+2}(x-c)^{n+1}$ in $f'(x)$ has been reduced by 1 and the coefficient has been multiplied by $(n+1)$. Therefore,

$$\begin{aligned} L(f) &= c_1 \sum_{n=0}^{\infty} (n+1)(n+2)a_{n+2}(x-c)^n + c_2 \sum_{n=0}^{\infty} (n+1)a_{n+1}(x-c)^n + c_3 \sum_{n=0}^{\infty} a_n(x-c)^n \\ &= \sum_{n=0}^{\infty} (c_1(n+1)(n+2)a_{n+2} + c_2(n+1)a_{n+1} + c_3a_n)(x-c)^n \end{aligned}$$

Now if

$$g(x) = \sum_{n=0}^{\infty} b_n(x-c)^n$$

then

$$c_1(n+1)(n+2)a_{n+2} + c_2(n+1)a_{n+1} + c_3a_n = b_n$$

so that we could solve for a_{n+2} uniquely in terms of a_{n+1} , a_n , and b_n . Knowing the values of a_0 , a_1 and all of the b_n , we uniquely determine all of the other a_n . Note that $f(c) = a_0$ and $f'(c) = a_1$ □

Not all of the fibers of L are vector spaces—only the fiber over the zero function (i.e. vector) is.

Not only this, but the functions *add the same way* as our ordered pairs in \mathbb{R}^2 add together. Indeed, $f \mapsto (f(c), f'(c))$ is an isomorphism from $L^{-1}(0)$ to \mathbb{R}^2 .

We can therefore think about $L^{-1}(0)$ as \mathbb{R}^2 . It is spanned by two linearly independent functions (i.e. vectors).

Homogeneous Linear Differential Equation

Finding the functions that live in $L^{-1}(0)$ is the same as finding the functions f that satisfy the equation

$$c_1f''(x) + c_2f'(x) + c_3f(x) = 0$$

for all $x \in (a, b)$. This type of equation is called a homogeneous system of equations.

Nonhomogeneous Linear Differential Equation

Finding the functions that live in $L^{-1}(g)$ is the same as finding the functions f that satisfy the equation

$$c_1 f''(x) + c_2 f'(x) + c_3 f(x) = g(x)$$

for all $x \in (a, b)$. This type of equation is called a nonhomogeneous system of equations.

The solutions to a nonhomogeneous system of equations are given as a fiber of a linear transformation and simply represent a shift of the fiber $L^{-1}(0)$. So to solve such a system:

- Find a particular solution.
- Find a basis for $L^{-1}(0)$.

This is exactly what we do when we solve a system of equations. We find one solution vector from the reduced row echelon form of the augmented matrix. Then we add this vector to the kernel. We find vectors that span the kernel. The kernel is the fiber over zero of a matrix function.

What if $L(f) = c_1 f' + f$? Then $L^{-1}(0)$ then knowing a_0 in the power series for f is enough to determine f from the power series relationships. So, $L^{-1}(0)$ is representable as the one-dimensional vector space \mathbb{R} where every real number denotes a_0 and uniquely determines an element in $L^{-1}(0)$.

We want to be able to use matrix techniques. We will show how diagonalization can be used to help solve a “mixed” linear differential equation where we are solving not just for one function, but a *pair of functions*.

Example 1. For instance, suppose that $D = C^\omega(a, b) \times C^\omega(a, b)$ and we have a linear operator

$$L : C^\omega(a, b) \times C^\omega(a, b) \rightarrow C^\omega(a, b) \times C^\omega(a, b) \quad L(f, g) = (4f - 3g - f', 2f - g - g')$$

Suppose that $c \in (a, b)$ and let

$$f(x) = \sum_{n=0}^{\infty} a_n(x - c)^n \quad g(x) = \sum_{n=0}^{\infty} b_n(x - c)^n$$

Then in order for $(f, g) \in L^{-1}(0, 0)$, when we compare the coefficients of $(x - c)^n$ with

$$0 = \sum_{n=0}^{\infty} 0(x - c)^n$$

we have:

$$4a_n - 3b_n - (n + 1)a_{n+1} = 0 \quad 2a_n - b_n - (n + 1)b_{n+1} = 0$$

These recurrences tell us that knowledge of a_n and b_n can be determined solely from knowledge of (a_0, b_0) . Note that $a_0 = f(c)$ and $b_0 = g(c)$. Hence, $(f, g) \mapsto (f(c), g(c))$ is an isomorphism from $L^{-1}(0, 0)$ to \mathbb{R}^2 . So, solving this mixed differential system of equations yields a span of two ordered pairs in D . This system can be written as:

$$\underbrace{\begin{pmatrix} 4 & -3 \\ 2 & -1 \end{pmatrix}}_A \cdot \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} f' \\ g' \end{pmatrix}$$

Now notice that the trace of this matrix is 3 and that the determinant is 2 so that the characteristic polynomial is

$$x^2 - 3x + 2 = (x - 1)(x - 2)$$

The first column of $x - 1$ (as a matrix) is $\begin{pmatrix} 3 \\ 2 \end{pmatrix}$ which gives an eigenvector for $x = 2$. The first column of $x - 2$ is $\begin{pmatrix} 2 \\ 2 \end{pmatrix}$ which gives an eigenvector for $x = 1$ so that if f_1 and g_1 are functions such that

$$\begin{pmatrix} f \\ g \end{pmatrix} = \underbrace{\begin{pmatrix} 2 & 3 \\ 2 & 2 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} f_1 \\ g_1 \end{pmatrix}}_v$$

then we can write:

$$\begin{pmatrix} f' \\ g' \end{pmatrix} = \underbrace{\begin{pmatrix} 2 & 3 \\ 2 & 2 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} f'_1 \\ g'_1 \end{pmatrix}}_{v'}$$

so that our equation is of the form:

$$AUv = Uv' \implies U^{-1}AUv = v'$$

Realize that

$$U^{-1}AU = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

so that our system has now become

$$\begin{aligned} f_1 &= f'_1 \\ 2f_2 &= f'_2 \end{aligned}$$

This system *is a lot simpler* and we will explain how to solve it.

First of all, the solution of $f'_1 - f_1 = 0$ is the kernel of $f_1 \mapsto f'_1 - f_1$ which from the discussion above is spanned by a single function. We just need to find one solution. One should remember that the derivative of e^x is e^x . Hence, $f_1(x) = e^x$ is a function (i.e. vector) whose span covers all solutions of $f'_1 - f_1 = 0$. Similarly, we notice that $f_2(x) = e^{2x}$ is a spanning solution for f_2 in $2f_2 = f'_2$. Therefore, the solutions (f_1, f_2) to our simplified system are all ordered pairs (f_1, f_2) such that:

$$(f_1, f_2) \in \{ c_1(e^x, 0) + c_2(0, e^{2x}) : c_1, c_2 \in \mathbb{R} \}$$

This means that:

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}}_{U^{-1}AU} \cdot \underbrace{\begin{pmatrix} c_1e^x \\ c_2e^{2x} \end{pmatrix}}_v = \underbrace{\begin{pmatrix} c_1e^x \\ 2c_2e^{2x} \end{pmatrix}}_{v'}$$

Remember that

$$\begin{pmatrix} f \\ g \end{pmatrix} = \underbrace{\begin{pmatrix} 2 & 3 \\ 2 & 2 \end{pmatrix}}_U \cdot \underbrace{\begin{pmatrix} c_1e^x \\ c_2e^{2x} \end{pmatrix}}_v$$

so that the general solution (f, g) of our original system is given by:

$$f(x) = 2c_1e^x + 3c_2e^{2x} \quad g(x) = 2c_1e^x + 2c_2e^{2x}$$

where c_1 and c_2 are free to vary. Another way of writing this is:

$$(f, g) = c_1 \cdot (2e^x, 2e^x) + c_2 \cdot (3e^{2x}, 2e^{2x})$$

That is, the solution can be expressed as an \mathbb{R} -span:

$$L^{-1}(0, 0) = \langle (2e^x, 2e^x), (3e^{2x}, 2e^{2x}) \rangle$$

Let's take something in this span and check it in the differential equation. What about the following:

$$(2e^x, 2e^x) - (3e^{2x}, 2e^{2x}) = (2e^x - 3e^{2x}, 2e^x - 2e^{2x})$$

We have:

$$\underbrace{\begin{pmatrix} 4 & -3 \\ 2 & -1 \end{pmatrix}}_A \cdot \begin{pmatrix} 2e^x - 3e^{2x} \\ 2e^x - 2e^{2x} \end{pmatrix} = \begin{pmatrix} 2e^x - 6e^{2x} \\ 2e^x - 4e^{2x} \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} \frac{d}{dx}(2e^x - 3e^{2x}) \\ \frac{d}{dx}(2e^x - 2e^{2x}) \end{pmatrix}$$

Solution to $f' = rf$

The general solution to $f' = rf$ where $r \in \mathbb{R}$ and $f : (a, b) \rightarrow \mathbb{R}$ is given by:

$$f(x) = e^{rx}$$

Differential Equation Diagonalization

To solve a differential equation of the form $Aw = w'$ where A is a 2×2 matrix, $w = (f, g)$, and $w' = (f', g')$:

- Find U so that $U^{-1}AU = \begin{pmatrix} r_1 & 0 \\ 0 & r_2 \end{pmatrix}$. Let u_1 and u_2 be the columns of U so that $U = \begin{pmatrix} u_1 & u_2 \end{pmatrix}$.
- The solution of the differential equation is the \mathbb{R} -span:

$$\langle e^{r_1 x} \cdot u_1, e^{r_2 x} \cdot u_2 \rangle$$

Example 2. Suppose that we would like to solve the system:

$$\underbrace{\begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix}}_A \cdot \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} f' \\ g' \end{pmatrix}$$

Notice that $\text{tr}(A) = 0$ and $\det(A) = -1$ so that the characteristic polynomial of A is $x^2 - 1 = (x + 1)(x - 1)$. We could take the first column u_1 of U to correspond to the eigenvalue $x = 1$ as a rescaling of the second column of $x + 1$ yielding $\frac{1}{2} \cdot (2, 2) = (1, 1)$. We can take the second column u_2 of U to correspond to the eigenvalue $x = -1$ as a rescaling of the first column of $x - 1$ yielding $\frac{1}{-2} \cdot (-2, 0) = (1, 0)$. Hence, the

solutions are described by the \mathbb{R} -span:

$$\langle e^x \cdot (1, 1), e^{-x} \cdot (1, 0) \rangle$$

Indeed, one can check that:

$$\begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} e^x + e^{-x} \\ e^x \end{pmatrix} = \begin{pmatrix} e^x - e^{-x} \\ e^x \end{pmatrix} \stackrel{\leq}{=} \begin{pmatrix} \frac{d}{dx}(e^x + e^{-x}) \\ \frac{d}{dx}(e^x) \end{pmatrix}$$

Key Concepts from this Section

- **real analytic functions on an interval:** (page 1000) A function is said to be real analytic on an interval (a, b) if it can be expressed as a power series

$$\sum_{n=0}^{\infty} a_n(x - c)^n$$

for $c \in (a, b)$ that converges on the interval (a, b) .

- **C^n functions:** (page 1000) A function is said to be C^n on an interval (a, b) if it and its derivatives down to the n th derivative are all continuous functions on that interval.
- **$C^\omega[a, b]$:** (page 1000) The notion of being a real analytic function is stronger than even being a C^∞ function (i.e. having all derivatives that are continuous and defined). *This is because if a function has a powers series representation that is well defined over an open interval, it has derivatives of all orders that are well defined and continuous on that open interval.* Without going into detail, we provide a little rationale: for any $c \in (a, b)$, one can write $f(x)$ nearby c as a sum of terms $a_m(x - c)^m$. The m th derivative on plugging in c to see things vanish is $m!a_m$.

The symbol ω sometimes is used to denote “something that is more than all of the counting numbers $1, 2, 3, \dots$ ” That is, something that is more than ∞ . *This notation here however only signifies that we have something stronger than C^∞ nothing else...* So we use the notation $C^\omega(a, b)$ to denote all of the real analytic functions over an interval (a, b) .

- **linear operator:** (page 1001) Define L to be the function $C^\omega(a, b) \rightarrow C^\omega(a, b)$ given by:

$$L(f) = c_1 f'' + c_2 f' + c_3 f$$

for real constants c_1, c_2, c_3 . This is an example of a linear transformation. It is additive and scalable.

- **theorem 8.1.1 :** (page 1001) Let $c \in (a, b)$. Every element f in $L^{-1}(g)$ is uniquely representable within that fiber by the values $(f(c), f'(c))$. That is, no other function h in that fiber has $(h(c), h'(c)) = (f(c), f'(c))$. Also, for any pair of values (t, w) , there is $f \in L^{-1}(g)$ such that $(f(c), f'(c)) = (t, w)$. That is, every element in the fiber is expressible uniquely by an element in \mathbb{R}^2 .
- **homogeneous linear differential equation:** (page 1002) Finding the functions that live in $L^{-1}(0)$ is the same as finding the functions f that satisfy the equation

$$c_1 f''(x) + c_2 f'(x) + c_3 f(x) = 0$$

for all $x \in (a, b)$. This type of equation is called a homogeneous system of equations.

- **nonhomogeneous linear differential equation:** (page 1002) Finding the functions that live in $L^{-1}(g)$ is the same as finding the functions f that satisfy the equation

$$c_1 f''(x) + c_2 f'(x) + c_3 f(x) = g(x)$$

for all $x \in (a, b)$. This type of equation is called a nonhomogeneous system of equations.

- **solution to $f' = rf$:** (page 1006) The general solution to $f' = rf$ where $r \in \mathbb{R}$ and $f : (a, b) \rightarrow \mathbb{R}$ is given by:

$$f(x) = e^{rx}$$

- **differential equation diagonalization:** (page 1006) To solve a differential equation of the form $Aw = w'$ where A is a 2×2 matrix, $w = (f, g)$, and $w' = (f', g')$:

- Find U so that $U^{-1}AU = \begin{pmatrix} r_1 & 0 \\ 0 & r_2 \end{pmatrix}$. Let u_1 and u_2 be the columns of U so that $U = \begin{pmatrix} u_1 & u_2 \end{pmatrix}$.
- The solution of the differential equation is the \mathbb{R} -span:

$$\langle e^{r_1 x} \cdot u_1, e^{r_2 x} \cdot u_2 \rangle$$

8.1.1 Exercises

Systems of Differential Equations

Find the vector space of pairs (f, g) that solve the system of differential equations. Write the system in matrix form and use the technique of this section.

$$\begin{aligned} \text{1. } f + 3g &= f' \\ -f - 3g &= g' \end{aligned}$$

$$\begin{aligned} \text{2. } 7f + 15g &= f' \\ -3f - 7g &= g' \end{aligned}$$

$$\begin{aligned} \text{3. } -7f + 15g &= f' \\ -3f + 7g &= g' \end{aligned}$$

$$\begin{aligned} \text{4. } -g &= f' \\ g &= g' \end{aligned}$$

$$\begin{aligned} \text{5. } 4f + 9g &= f' \\ -2f - 5g &= g' \end{aligned}$$

$$\begin{aligned} \text{6. } -f + 3g &= f' \\ -f + 3g &= g' \end{aligned}$$

$$\begin{aligned} \text{7. } -4f - g &= f' \\ 6f + g &= g' \end{aligned}$$

$$\begin{aligned} \text{8. } f - g &= f' \\ -3f - g &= g' \end{aligned}$$

$$\begin{aligned} \text{9. } f + 3g &= f' \\ -f - 3g &= g' \end{aligned}$$

$$\begin{aligned} \text{10. } 2f - g &= f' \\ g &= g' \end{aligned}$$

$$\begin{aligned} \text{11. } -3f - g &= f' \\ 3f + g &= g' \end{aligned}$$

$$\begin{aligned} \text{12. } -3f - g &= f' \\ 3f + g &= g' \end{aligned}$$

$$\begin{aligned} \text{13. } -2f - 3g &= f' \\ -g &= g' \end{aligned}$$

$$\begin{aligned} \text{14. } f - g &= f' \\ -f + g &= g' \end{aligned}$$

8.1.2 Solutions

1. $\langle 1 \cdot (3, -1), 1 \cdot (1, -1) \rangle$

2. $\langle e^{(2x)} \cdot (3, -1), e^{(2x)} \cdot (5, -3) \rangle$

3. $\langle e^{(2x)} \cdot (5, 3), e^{(2x)} \cdot (3, 1) \rangle$

4. $\langle e^x \cdot (1, -1), e^x \cdot (1, 0) \rangle$

5. $\langle e^x \cdot (3, -1), e^x \cdot (3, -2) \rangle$

6. $\langle e^{(2x)} \cdot (1, 1), e^{(2x)} \cdot (3, 1) \rangle$

7. $\langle e^{(-x)} \cdot (1, -3), e^{(-x)} \cdot (1, -2) \rangle$

8. $\langle e^{(2x)} \cdot (1, -1), e^{(2x)} \cdot (1, 3) \rangle$

9. $\langle 1 \cdot (3, -1), 1 \cdot (1, -1) \rangle$

10. $\langle e^{(2x)} \cdot (1, 0), e^{(2x)} \cdot (1, 1) \rangle$

11. $\langle 1 \cdot (1, -3), 1 \cdot (1, -1) \rangle$

12. $\langle 1 \cdot (1, -3), 1 \cdot (1, -1) \rangle$

13. $\langle e^{(-x)} \cdot (3, -1), e^{(-x)} \cdot (1, 0) \rangle$

14. $\langle e^{(2x)} \cdot (1, -1), e^{(2x)} \cdot (1, 1) \rangle$

Quaternion Rotations

8.2

8.2.1 Introduction to Quaternions	1011
8.2.2 Rotations	1015
8.2.3 Specific Rotation Computations	1020
8.2.4 Euler's Theorem (Proof)	1024
8.2.5 Exercises	1029
8.2.6 Solutions	1030

Questions to Guide Your Study:

- *What is a quaternion and how it describe a vector in \mathbb{R}^4 ?*
- *How does quaternion multiplication work and how is it related to the cross product of two vectors in \mathbb{R}^3 ?*
- *What is a rotation in \mathbb{R}^n and how can we describe it via a matrix?*
- *How do you use quaternion multiplication to rotate a vector about a given axis at a given degree?*
- *How do you prove that a rotations in three-dimensions will always have an axis of rotation?*

8.2.1 Introduction to Quaternions

We will consider four operations that we can apply to a vector $(a, b, c, d) \in \mathbb{R}^4$.

- Let 1 be a “do nothing operator” on a vector (a, b, c, d) .
- Let i be the operator that switches $a \leftrightarrow b$ and $c \leftrightarrow d$ but then puts a negative on one of them as follows:

$$i : (a, b, c, d) \mapsto (-b, a, -d, c)$$

Notice that $(a, b, c, d) \bullet (-b, a, -d, c) = 0$.

- Let j be the operator that switches $a \leftrightarrow c$ and $b \leftrightarrow d$ but then puts a negative on one of them as follows:

$$j : (a, b, c, d) \mapsto (-c, d, a, -b)$$

Notice that $(a, b, c, d) \bullet (-c, d, a, -b) = 0$.

- Let k be the composition of these two operators:

$$(a, b, c, d) \xrightarrow{j} (-c, d, a, -b) \xrightarrow{i} (-d, -c, b, a)$$

$i \circ j = k$

These operators combined with their negatives form a closed group. All of these “orthogonal operators” $\pm i$, $\pm j$, $\pm k$, we will call *imaginary* operators. If the first component of our vectors corresponds to the real axis \mathbb{R} , then these operators take an element on it like $(a, 0, 0, 0)$ and cast it into a realm which is purely orthogonal to it—orthogonal to what is real.

Further, if we think of $1, i, j, k$ as standard basis vectors, we can form a four dimensional \mathbb{R} vector space. If we include multiplication (composition) of these operators, this vector space becomes a ring. This multiplication is not commutative.

Quaternion Ring

The ring of quaternions over the reals is the \mathbb{R} vector space generated by the symbols $1, i, j$, and k that follows the following multiplication:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

This ring may be expressed as:

$$\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

Quaternion

A quaternion is any element $a + bi + cj + dk$ of this ring.

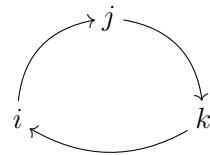
In general, we will think of any vector $(a, b, c, d) \in \mathbb{R}^4$ as:

$$(a, b, c, d) = a \cdot \mathbf{1}(1, 0, 0, 0) + b \cdot i(1, 0, 0, 0) + c \cdot j(1, 0, 0, 0) + d \cdot k(1, 0, 0, 0)$$

or we can just think of an element of the quaternion ring as a vector in and of itself.

Quaternion multiplication is very useful for a quick calculation of a three-dimensional rotation. The primary goal of this section is to discuss how this is done and to prove it. Specifically, we define what is meant by a rotation generally, how it can be described in terms of matrices, and how there is a nice matrix connection to quaternions.

Think of quaternion multiplication by considering the diagram:



If we go with the arrows, the result is positive. If we go against, the result is negative. For instance, $i \cdot j = k$, but $j \cdot i = -k$. Using this, we can combine the operation with addition:

$$(2i + 3j) \cdot k = 2i \cdot k + 3j \cdot k = -2j + 3i$$

When we multiply like this we are *composing* the operator $2i + 3j$ with the operator k . Yet, if we plug $(1, 0, 0, 0)$ into this composed operation, we just get the vector corresponding to $-2j + 3i$ which is $(0, 3, -2, 0)$. So really, this operator math can be thought of as vector math.

Imaginary Part

The imaginary part of a quaternion $q = a + bi + cj + dk$ is

$$\text{Im}(q) = bi + cj + dk$$

Real Part

The real part of a quaternion $q = a + bi + cj + dk$ is

$$\text{Re}(q) = a$$

Imaginary Quaternion

An imaginary quaternion is one of the form $bi + cj + dk$ so that $a = 0$.

An imaginary quaternion has no real part.

Example 1. $i + j - 3k$ is an imaginary quaternion.

By their very construction and definition as a sum of orthogonal operators, the multiplication of an imaginary quaternion to a quaternion $q = a + bi + cj + dk$ produces something that is orthogonal by dot product to q .

Example 2. Here is an example:

$$(2i + j + 3k) \cdot (i + 4j + 5k) = -23 - 7i - 7j + 7k$$

using the multiplication of the operators. We know that $-23 - 7i - 7j + 7k$ thought of as $(-23, -7, -7, 7)$ is orthogonal to $(i + 4j + 5k)$ thought of as $(0, 1, 4, 5)$ because it was obtained by applying a sum of orthogonal operators $(2i + j + 3k)$ to $(0, 1, 4, 5)$. *You can verify this by checking that the dot product is 0.*

Conjugate Quaternion

Let $q = a + bi + cj + dk$. Then we define the conjugate \bar{q} as

$$\bar{q} = a - bi - cj - dk$$

Theorem 8.2.1

Let u, w be the vectors in \mathbb{R}^3 describing the imaginary quaternions p and q . Then $\text{Im}(p \cdot q)$ is given by $u \times w$.

Proof. Note that i, j, k with multiplication behave just like dx, dy , and dz with the wedge product \wedge except $dx \wedge dx = dy \wedge dy = dz \wedge dz = 0$ instead of -1 . But with quaternion multiplication taking the imaginary part of something real like -1 is just 0 as well. Hence the imaginary part of $p \cdot q$ is the cross product which is defined by the wedge product. \square

Theorem 8.2.2

Let q and p be quaternions, then:

$$\overline{q \cdot p} = \overline{p} \cdot \overline{q}$$

Proof. Let q_r and p_r be the real parts respectively of q and p . Let q_i and p_i be the imaginary parts of q and p respectively. We simply compute:

$$(q_r + q_i) \cdot (p_r + p_i) = q_r p_r + q_r p_i + q_i p_r + q_i p_i$$

and take its conjugate:

$$q_r p_r - q_r p_i - q_i p_r + q_i p_i$$

and compare it to:

$$(p_r - p_i) \cdot (q_r - q_i) = p_r q_r - p_r q_i - p_i q_r + p_i q_i$$

Notice that

$$p_i q_i = p_i \times q_i = -q_i \times p_i = -q_i p_i$$

so that the two computations we are comparing yield the same result. \square

To explore quaternion multiplication visually, see the following SageMath activity:



8.2.2 Rotations

Even though quaternions are four-dimensional, we will use them to describe three-dimensional rotations. First, what is a rotation?

Rotation

A rotation with respect to a given basis in \mathbb{R}^4 is given by a linear transformation describable by an orthogonal square matrix with respect to that basis which has a determinant of +1.

We recall what an orthogonal matrix is:

Orthogonal Matrix

An orthogonal matrix is one whose columns make up an orthonormal set.

We also recall a result about orthogonal matrices:

Theorem 8.2.3

Let U be an orthogonal square matrix. Then $U^T = U^{-1}$

Proof. Just think about matrix multiplication in terms of dot products. \square

Corollary 8.2.4

The determinant of an orthogonal matrix is ± 1 .

Proof. Let M be an orthogonal matrix. Then $M^T M = \text{id}$ so that $\det(M) = \det(M^T)$ is a square root of 1. That is, it is ± 1 . \square

Theorem 8.2.5

Let U be a $n \times n$ orthogonal square matrix and v a column vector in \mathbb{R}^n . Then

$$|v| = |U \cdot v|$$

Proof. Note that $|v|^2 = v^T v$ and

$$|Uv|^2 = v^T \underbrace{U^T U}_\text{id} v = v^T v$$

Since vector lengths are positive and $|v|^2 = |Uv|^2$, then $|v| = |Uv|$. \square

Isometry

An isometry is a function that preserves distances.

Theorem 8.2.6

An orthogonal matrix is an isometry.

A determinant of $+1$ is like *preserving orientation*. Being orthogonal produces an isometry. So intuitively, our definition of rotation should make sense.

Unit Quaternion

A unit quaternion is one in which its length as a vector in \mathbb{R}^4 is 1.

Theorem 8.2.7

Let w be a unit imaginary quaternion. Then $w^2 = -1$.

Proof. The imaginary part of w^2 is $w \times w = 0$. We know via direct computation that if $w = ai + bj + ck$ that this real part is $-a^2 - b^2 - c^2$ for real numbers a, b, c . This quantity is -1 since by assumption $a^2 + b^2 + c^2 = 1$. \square

Theorem 8.2.8

Let u be a unit quaternion. Then

$$u\bar{u} = 1.$$

Proof. Suppose that $u = a + bi + cj + dk$. Then

$$u\bar{u} = (a + (bi + cj + dk))(a - (bi + cj + dk))$$

which is a difference of two squares:

$$= a^2 - (bi + cj + dk)^2$$

The imaginary part of $(bi + cj + dk)^2$ is given by $(b, c, d) \times (b, c, d) = (0, 0, 0)$. The real part is: $b^2i^2 + c^2j^2 +$

$d^2 k^2 = -b^2 - c^2 - d^2$. Hence, we get:

$$u\bar{u} = a^2 + b^2 + c^2 + d^2$$

which is the square of the length of u thought of as a vector in \mathbb{R}^4 . Since u is a unit quaternion, this is 1.

□

SO(n)

We let $SO(n)$ denote the group of $n \times n$ matrices that describe rotations on \mathbb{R}^n . It is called the *special orthogonal group* on \mathbb{R}^n . It consists of $n \times n$ matrices that are orthogonal and of determinant +1.

Theorem 8.2.9

$SO(n)$ is a group.

Proof. Let A and B be $n \times n$ orthogonal matrices each of determinant 1. Then,

$$(AB)(AB)^T = \underbrace{ABB^T}_{\text{id}} \underbrace{A^T}_{\text{id}}$$

so that $(AB)^T$ is the inverse of AB . This shows that the columns of AB are orthogonal to each other each with length 1. That is, AB is orthogonal. Also $\det(AB) = \det(A) \cdot \det(B) = 1$. Hence, $SO(n)$ is closed under multiplication. If $A \in SO(n)$, then it is clear that $A^T \in SO(n)$. Yet A^T is the inverse of A so that $SO(n)$ is closed under taking inverses. This is enough to show that $SO(n)$ is a subgroup of the group of $n \times n$ invertible (i.e. inverse admitting) matrices. □

Lemma 8.2.10

The multiplication action of a *unit* quaternion on the left is given by a matrix in column interpretation in $SO(4)$. That is, it is a four-dimensional rotation.

Proof. We think of e_1 as 1, e_2 as i , e_3 as j and e_4 as k . Now we track their destinations as we multiply by

$q = a + bi + cj + dk$ on the left. We get a matrix via a column interpretation:

$$M = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}$$

Note that the length of each column is the same as the first which is 1 and that all of these columns are orthogonal to each other. Since M is an orthogonal matrix, its determinant is ± 1 . We *just* need to show that the determinant of M is positive and we are done. To do this, we can use our kitty-corner technique with 2×2 submatrices to realize that all six *signed* products are *positive squares*. This is left as an exercise to the reader. \square

Lemma 8.2.11

A similar argument shows that the multiplication action by a unit quaternion on the right is also given by a matrix in column interpretation in $SO(4)$. We express the destinations as columns again.

Corollary 8.2.12

Let u and w be unit quaternions. Then uw is again a unit quaternion.

Proof. The multiplication of the two quaternions can be given by the multiplication of the matrix for u on the left of the matrix for w both in column interpretation. This matrix product is an orthogonal matrix and hence an isometry. Plugging in the column vector e_1 into this product in column interpretation should give the output uw which has the same length as the input e_1 which is 1. \square

Conjugating by Unit Quaternions

We say that we conjugate q by the unit quaternion u when we compute $uq\bar{u}$.

Theorem 8.2.13

Let u be a unit quaternion. Then, $q \mapsto uq\bar{u}$ defines a rotation with input q expressible as a matrix

$$M = \begin{pmatrix} 1 & 0's \\ 0's & A \end{pmatrix}$$

where $A \in SO(3)$.

Proof. Notice that the determinant of such an M is $+1$ by multiplying the determinants of the diagonal blocks and that the columns are all orthonormal. Hence, such a matrix M as described in the theorem is in $SO(4)$.

Now, we show that $q \mapsto uq\bar{u}$ really gives us such a matrix. We think of e_1 as 1 , e_2 as i , e_3 as j and e_4 as k .

The destination of e_1 is $u \cdot 1 \cdot \bar{u} = 1$. So, $e_1 \mapsto e_1$. In a column interpretation for M , this gives us our first column of M .

The destination of e_2 is $u \cdot i \cdot \bar{u}$. Let's show that this results in *an imaginary quaternion*. Now, switching the multiplication order to $u \cdot \bar{u} \cdot i$ does not change the real part. Let's see why. In the product $u \cdot i \cdot \bar{u}$ after distributing and expanding we have products like jik (having i in the middle) which is imaginary. Switching the order in this product will keep it imaginary. From a product like aii where a is real, switching the order of multiplication changes nothing. Hence, the real part of changing the order as proposed remains the same. Notice that $\underbrace{u \cdot \bar{u}}_1 \cdot i = i$ has a real part of 0 so that $u \cdot i \cdot \bar{u}$ also has a zero real part.

The same holds true for the destinations of e_3 and e_4 . This tells us that M is of the form

$$\begin{pmatrix} 1 & 0's \\ 0's & A \end{pmatrix}$$

Note that multiplication by u on the left: $q \mapsto uq$ is given by a matrix in $SO(4)$. Take this output as the vector form of uq and plug it in as a column into the matrix function giving the action of multiplication of u on the right. The overall effect is to plug q in as a column vector into a matrix function given by the product of two matrices in $SO(4)$. Since $SO(4)$ is a group, this product is still in $SO(4)$. This means that $M \in SO(4)$ which forces the determinant of A to be $+1$ and its columns to be orthogonal so that $A \in SO(3)$ thus giving the theorem. \square

8.2.3 Specific Rotation Computations

We will prove in the next subsection that every three-dimensional rotation as we have defined it has an axis of rotation. To be an axis of rotation means that any vector along it is an eigenvector with eigenvalue 1 . That is, if A describes the rotation, then $Av = 1 \cdot v$ so that v remains fixed.

In our current setup, when we conjugate by a unit quaternion u to rotate in four-dimensions, then if we rotate u itself we have: $u \cdot \underbrace{u \cdot \bar{u}}_1 = u$ so that $u \mapsto u$. That is, u is fixed by the four dimensional rotation. We have already seen that the matrix M for this four-dimensional rotation is of the form

$$\begin{pmatrix} 1 & 0's \\ 0's & A \end{pmatrix}$$

with A giving a three-dimensional rotation on purely imaginary quaternions (the space of such things is \mathbb{R}^3).

Since the real part of u has absolute value less than 1 , we can write it as $\cos(\theta)$ for some $\theta \in [0, 2\pi]$. Factoring $\sin(\theta)$ out of the imaginary part, we write u as $u = \cos(\theta) + \sin(\theta) \cdot w$ where $w = bi + cj + dk$

is an imaginary quaternion. Then,

$$\begin{aligned} 1 &= |u| = \cos^2(\theta) + \sin^2(\theta)b^2 + \sin^2(\theta)c^2 + \sin^2(\theta)d^2 \\ &= \cos^2(\theta) + \sin^2(\theta)(b^2 + c^2 + d^2) = 1 \end{aligned}$$

This computation forces $b^2 + c^2 + d^2 = 1$ so that w is an imaginary quaternion of length 1.

Let's compute:

$$\begin{pmatrix} 1 & 0's \\ 0's & A \end{pmatrix} \cdot \underbrace{\begin{pmatrix} \cos(\theta) \\ \sin(\theta)w \end{pmatrix}}_u = \underbrace{\begin{pmatrix} \cos(\theta) \\ \sin(\theta)w \end{pmatrix}}_u$$

Notice that

$$\begin{pmatrix} 1 & 0's \\ 0's & A \end{pmatrix} \cdot \begin{pmatrix} \cos(\theta) \\ 0's \end{pmatrix} = \begin{pmatrix} \cos(\theta) \\ 0's \end{pmatrix}$$

This forces:

$$\begin{pmatrix} 1 & 0's \\ 0's & A \end{pmatrix} \cdot \begin{pmatrix} 0 \\ \sin(\theta)w \end{pmatrix} = \begin{pmatrix} 0 \\ \sin(\theta)w \end{pmatrix}$$

This is also equal to

$$\begin{pmatrix} 0 \\ A \cdot (\sin(\theta)w) \end{pmatrix}$$

That is, $\sin(\theta)w$ thought of as a vector is an eigenvector of A with an eigenvalue of 1. Since w is in the same eigenspace, then:

The vector (b, c, d) corresponding to w is an eigenvector of A with eigenvalue 1. It is the axis of rotation of the three-dimensional rotation A .

Theorem 8.2.14

Using the above notation, rotation by conjugating by u is through an angle of 2θ . This angle is counterclockwise when we look down the tip of the arrow of w down to its tail.

Proof. Let's first think of a quaternion q and a unit quaternion u such that $uq\bar{u} = q$ so that q comes back to itself again. Then multiplying by u on the left of each side, $uq = qu$. The question comes: when do two quaternions commute with each other? The imaginary part of uq is given by $u \times q$ and the imaginary part of qu is $q \times u$. We know that $u \times q = -(q \times u)$. But this equality is also saying that $u \times q = q \times u$ so that $u \times q = -(u \times q)$ which forces $u \times q = q \times u = 0$. That means that *only real quaternions commute with each other*. Since $|u| = 1$, then if $uq\bar{u} = q$ and we write $u = \cos(\theta) + \sin(\theta)w$ as above, then $u = \cos(\theta)$ is completely real. The smallest positive value of θ for which this occurs is π making $u = -1$. This forces $\theta = \pi$. That is, when $\theta = \pi$, then the rotation is precisely 2π . Now what if we performed rotation u on q and

then follow it by rotation $u_1 = \cos(\phi) + \sin(\phi)w$ about the same axis. The effect would be:

$$u_1(uq\bar{u})\bar{u_1} = (u_1u)q(\bar{u_1}\bar{u})$$

so that composing two rotations about w corresponds to multiplying the two quaternions u and u_1 that describe those rotations. Using the fact that $w^2 = -1$, we have that the outcome of the following multiplication:

$$uu_1 = (\cos(\theta) + \sin(\theta)w) \cdot (\cos(\phi) + \sin(\phi)w)$$

is the same as if we replaced w with i and were multiplying two complex numbers on the unit circle. We know that such a multiplication adds the angles together so that:

$$uu_1 = \cos(\theta + \phi) + \sin(\theta + \phi) \cdot w$$

In particular, we know that the rotation given by $\theta = \frac{\pi}{n}$ composed with itself n times yields the rotation for $\theta = \pi$ which is a rotation of 2π around w . The only rotation that does this is one that rotates by an angle of $\frac{2\pi}{n}$. In such a way we have a map $\mathbb{Q} \cap [0, 1] \rightarrow [0, 2\pi]$ defined as $x \mapsto 2x\pi$ where $\theta = \pi x$ for a rational number x describes a rotation by an angle of $2\pi x$.

The set $\mathbb{Q} \cap [0, 1]$ is dense in $[0, 1]$ meaning that every point in $[0, 1]$ can be realized as a limit of a sequence of rational numbers. A set is called “closed” in an analytic sense if it contains all of its “limit points.” The smallest closed set that contains a set is called the *closure* of that set. The set $[0, 1]$ is closed. We can say that $[0, 1]$ is the closure of the set $\mathbb{Q} \cap [0, 1]$. Our mapping $x \mapsto 2x\pi$ sends x to $\theta = \pi x$ which is then sent to a quaternion rotation in $SO(3)$ and then to the angle of the actual rotation. This overall mapping is a “continuous mapping” since each step can be formed with continuous matrix entries formed from trigonometric functions and inverse trigonometric functions (details omitted).

Dually, the mapping that goes from x to $2\pi x$ defined simply by *giving a rotation angle* is also continuous. These two functions match at rational numbers in $[0, 1]$. The difference of these functions is then a continuous function which is identically 0 at all rational numbers in $[0, 1]$.

One way of defining what is known as a “continuous map” is as a map where the preimage of any closed set is again closed. The preimage of 0 contains $\mathbb{Q} \cap [0, 1]$ —but it must be closed!—so the preimage must contain the closure of this set which is all of $[0, 1]$. That is, this difference function is identically 0 on all of $[0, 1]$ meaning that the our quaternion conjugation defined by θ gives a rotation of 2θ around the vector w for any value of θ .

Further, let’s prove that our angle is counterclockwise when we look down the tip of the arrow of w down to its tail. We assume that our rotation is less than π in our computation (it will not be confused with clockwise). This means that our θ will be larger than 0 and less than or equal to $\frac{\pi}{2}$. Assume that $q \perp w$ and that q is imaginary. Let’s write $u = c + sw$ where c and s are real number scalars denoting $\cos(\theta)$ and $\sin(\theta)$ and w is a unit imaginary quaternion. Then q rotates to

$$(c + sw) \cdot q \cdot (c - sw)$$

Multiplying this out, using the fact that $w^2 = -1$, we have:

$$c^2q + s^2q - csqw + cswq$$

Then using $c^2 + s^2 = 1$, we have the imaginary quaternion:

$$q + cs(wq - qw)$$

It is imaginary since wq and qw have the same real part which cancels out. Let's consider the vector which $q + cs(wq - qw)$ represents. Let's call it v . What we need to show is that $(q \times v) \bullet w > 0$ since there is a positive counterclockwise angle from q to v if $q \times v$ is in the same direction as w when we look down to the tail of w from its tip. So, first we consider $(q \times v)$. This is the imaginary part of $q(q + cs(wq - qw))$. Computing, noting that $cs > 0$ because $0 < \theta \leq \frac{\pi}{2}$:

$$q(q + cs(wq - qw)) = \underbrace{q^2}_{\text{real}} + \underbrace{cs}_{>0} \cdot (qwq - q^2w)$$

Notice that $-q^2 = |q|^2$ since the real part of q^2 where $q = ai + bj + ck$ is $-a^2 - b^2 - c^2$ and the imaginary part is $q \times q = 0$. Since $cs > 0$, we can ignore it. Hence, we are really looking at the imaginary part of the following where we remember that qw is real since $q \perp w$:

$$\underbrace{qw}_{\text{real}} q + |q|^2 w$$

When we take a dot product with w , the part $(qw)q$ goes away since $q \perp w$. All we are left with is $|q|^2 w \bullet w = |q|^2 |w|^2 > 0$ which is what we wanted to show. \square

Example 3. Let's rotate the vector $(1, 2, 3)$ around an axis $(1, 1, 1)$ counterclockwise by an angle of 60° . We take θ to be half of 60° so $\theta = 30^\circ$. Then

$$u = \cos(30) + \sin(30) \cdot \underbrace{\left(\frac{1}{\sqrt{2}} \cdot i + \frac{1}{\sqrt{2}} \cdot j + \frac{1}{\sqrt{2}} \cdot k \right)}_{\text{This represents our axis}}$$

This represents our axis
 $(1, 1, 1)$ where we have
 rescaled it to a unit
 length: $\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right)$

Multiplying out

$$u \cdot \underbrace{(i + 2j + 3k)}_{\text{This represents our vector } (1, 2, 3)} \cdot \bar{u}$$

This represents our vector $(1, 2, 3)$

we get $2i + j + 3k$ which corresponds to the vector $(2, 1, 3)$.



See the following SageMath activity to explore an interactive model of rotations by quaternions:

8.2.4 Euler's Theorem (Proof)

Theorem 8.2.15 Euler's Theorem

Given any three-dimensional rotation matrix, the rotation it describes has an axis of rotation.

We work toward a proof of this fact in this subsection using matrices. We will need some facts covered in the section on inner products.

Lemma 8.2.16

Given any square matrix M with real entries, we may find a unitary matrix W (i.e. the Hermitian inner product version of orthogonal—see the section on inner products) such that W^*MW is upper triangular where W^* is the Hermitian adjoint of W .

Proof. Further, let's find an upper triangular matrix T with possibly complex values such that M is similar to T . The characteristic polynomial of M has a root in \mathbb{C} since it can completely factor in $\mathbb{C}[x]$ by the fundamental theorem of algebra (discussed in section 8.3). Let's call this root t_1 and note that it is an eigenvalue for M . Let v be an associated eigenvector of length 1 and let C represent columns making an orthonormal basis for v^\perp . Then, setting $U = (v \ C)$, we have $U^{-1}MU$ has $(t_1, 0)$'s as its first column so that:

$$U^{-1}MU = \begin{pmatrix} t_1 & * \\ 0's & B_1 \end{pmatrix}$$

We can repeat this same process for B_1 with an eigenvalue t_2 to find a matrix \tilde{U} so that $\tilde{U}^{-1}B_1\tilde{U}$ is of this

form. Then, let $U_1 = \begin{pmatrix} 1 & * \\ 0's & \tilde{U} \end{pmatrix}$ so that:

$$U_1^{-1}U^{-1}MUU_1 = \begin{pmatrix} t_1 & * & * \\ 0 & t_2 & * \\ 0's & 0's & B_1 \end{pmatrix}$$

Continuing this process, we have found a unitary matrix $W = UU_1 \cdots U_r$ such that $W^{-1}MW$ is upper triangular. \square

Orthogonal matrices are unitary meaning their columns form an orthonormal collection of vectors with respect to the Hermitian inner product—this is because the usual inner product on \mathbb{R}^n is just a special case of the Hermitian inner product.

All $n \times n$ unitary matrices with entries in \mathbb{C} make up a group.

These ideas tell us that W^*MW (with W as in the lemma) is unitary since M is orthogonal. It is also upper triangular.

Let D be the unitary matrix W^*MW . Then $D^*D = D^*D = \text{id}$. This means that the Hermitian length of the first column is the same as the length of the first row. Since T is upper triangular, the first column only has one nonzero entry—and it is shared with the first row. The length is the sum of squares of the length of each complex entry. Hence, all other entries in the first row are forced to 0. This causes the second column to have only one nonzero entry. Continuing inductively we find that D is actually a diagonal matrix.

The matrix W actually diagonalized M to give D where D is again unitary.

Since D is a diagonal matrix and unitary, the length of each column is 1. In particular, for the i th column we have one nonzero entry. If we call it d , then the length of the i th column is computed as $0^2 + 0^2 + \cdots + |d|^2 + \cdots + 0^2 = 1$ so that $|d| = 1$. We have that d is a complex number that is on the unit circle in the complex plane. As roots of the characteristic polynomial, these always come in pairs if they are complex. When these pairs are multiplied, we get the square of their length—so 1. If in particular, M is a 3×3 matrix, one of the eigenvalues must be real and equal to +1 since the determinant—the product of the diagonal entries is 1. Even if all of the eigenvalues were real, we could not have -1 for every eigenvalue for then we would get a determinant of -1. Hence, one of the eigenvalues is guaranteed to be 1. What does this mean? There is an eigenvector which is fixed by the rotation—it is the axis of rotation!

Key Concepts from this Section

- **quaternion ring:** (page 1012) The ring of quaternions over the reals is the \mathbb{R} vector space generated by the symbols 1, i , j , and k that follows the following multiplication:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

This ring may be expressed as:

$$\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

- **quaternion:** (page 1012) A quaternion is any element $a + bi + cj + dk$ of this ring.
- **imaginary part:** (page 1013) The imaginary part of a quaternion $q = a + bi + cj + dk$ is

$$\text{Im}(q) = bi + cj + dk$$

- **real part:** (page 1013) The real part of a quaternion $q = a + bi + cj + dk$ is

$$\text{Re}(q) = a$$

- **imaginary quaternion:** (page 1014) An imaginary quaternion is one of the form $bi + cj + dk$ so that $a = 0$.
- **conjugate quaternion:** (page 1014) Let $q = a + bi + cj + dk$. Then we define the conjugate \bar{q} as

$$\bar{q} = a - bi - cj - dk$$

- **theorem 8.2.1 :** (page 1014) Let u, w be the vectors in \mathbb{R}^3 describing the imaginary quaternions p and q . Then $\text{Im}(p \cdot q)$ is given by $u \times w$.
- **theorem 8.2.2 :** (page 1015) Let q and p be quaternions, then:

$$\overline{q \cdot p} = \bar{p} \cdot \bar{q}$$

- **rotation:** (page 1015) A rotation with respect to a given basis in \mathbb{R}^4 is given by a linear transformation describable by an orthogonal square matrix with respect to that basis which has a determinant of +1.

- **orthogonal matrix:** (page 1016) An orthogonal matrix is one whose columns make up an orthonormal set.
- **theorem 8.2.3 :** (page 1016) Let U be an orthogonal square matrix. Then $U^T = U^{-1}$
- **corollary 8.2.4 :** (page 1016) The determinant of an orthogonal matrix is ± 1 .
- **theorem 8.2.5 :** (page 1016) Let U be a $n \times n$ orthogonal square matrix and v a column vector in \mathbb{R}^n . Then

$$|v| = |U \cdot v|$$

- **isometry:** (page 1016) An isometry is a function that preserves distances.
- **theorem 8.2.6 :** (page 1017) An orthogonal matrix is an isometry.
- **unit quaternion:** (page 1017) A unit quaternion is one in which its length as a vector in \mathbb{R}^4 is 1.
- **theorem 8.2.7 :** (page 1017) Let w be a unit imaginary quaternion. Then $w^2 = -1$.
- **theorem 8.2.8 :** (page 1017) Let u be a unit quaternion. Then

$$u\bar{u} = 1.$$

- **$SO(n)$:** (page 1018) We let $SO(n)$ denote the group of $n \times n$ matrices that describe rotations on \mathbb{R}^n . It is called the *special orthogonal group* on \mathbb{R}^n . It consists of $n \times n$ matrices that are orthogonal and of determinant +1.
- **theorem 8.2.9 :** (page 1018) $SO(n)$ is a group.
- **lemma 8.2.10 :** (page 1018) The multiplication action of a *unit* quaternion on the left is given by a matrix in column interpretation in $SO(4)$. That is, it is a four-dimensional rotation.
- **lemma 8.2.11 :** (page 1019) A similar argument shows that the multiplication action by a unit quaternion on the right is also given by a matrix in column interpretation in $SO(4)$. We express the destinations as columns again.
- **corollary 8.2.12 :** (page 1019) Let u and w be unit quaternions. Then uw is again a unit quaternion.
- **conjugating by unit quaternions:** (page 1019) We say that we conjugate q by the unit quaternion u when we compute $uqu\bar{u}$.
- **theorem 8.2.13 :** (page 1019) Let u be a unit quaternion. Then, $q \mapsto uqu\bar{u}$ defines a rotation with input q expressible as a matrix

$$M = \begin{pmatrix} 1 & 0's \\ 0's & A \end{pmatrix}$$

where $A \in SO(3)$.

- **theorem 8.2.14 :** (page 1021) Using the above notation, rotation by conjugating by u is through an angle of 2θ . This angle is counterclockwise when we look down the tip of the arrow of w down to its tail.
- **theorem 8.2.15 euler's theorem:** (page 1024) Given any three-dimensional rotation matrix, the rotation it describes has an axis of rotation.
- **lemma 8.2.16 :** (page 1024) Given any square matrix M with real entries, we may find a unitary matrix W (i.e. the Hermitian inner product version of orthogonal—see the section on inner products) such that W^*MW is upper triangular where W^* is the Hermitian adjoint of W .

8.2.5 Exercises

Rotating Vectors

Rotate the vector v counterclockwise by an angle of θ around an axis of w . Assume that the angle is counterclockwise when viewed from the tip of w looking down to its tail.

1. $v = (2, 2, 2)$, $w = (-1, 1, -1)$, $\theta = -\frac{1}{2}\pi$

2. $v = (-2, 2, 1)$, $w = (0, 1, 0)$, $\theta = \frac{3}{2}\pi$

3. $v = (2, -1, 1)$, $w = (1, -1, 1)$, $\theta = -\frac{1}{2}\pi$

4. $v = (-1, 2, -2)$, $w = (1, 1, 1)$, $\theta = -\frac{3}{2}\pi$

5. $v = (-2, 1, 1)$, $w = (0, 1, 0)$, $\theta = -\pi$

6. $v = (-2, 1, -1)$, $w = (0, 0, 1)$, $\theta = -\frac{1}{3}\pi$

7. $v = (-1, 1, -1)$, $w = (1, 1, 1)$, $\theta = -\pi$

8. $v = (2, 1, 1)$, $w = (1, -1, 1)$, $\theta = \frac{2}{3}\pi$

9. $v = (-2, -1, -1)$, $w = (-1, 1, -1)$, $\theta = -\frac{1}{3}\pi$

10. $v = (-2, 2, 1)$, $w = (-1, 1, -1)$, $\theta = \frac{2}{3}\pi$

11. $v = (-1, -1, 1)$, $w = (0, 0, 1)$, $\theta = \frac{1}{3}\pi$

12. $v = (2, -1, -2)$, $w = (1, 1, 1)$, $\theta = \frac{2}{3}\pi$

13. $v = (1, -2, -2)$, $w = (1, 0, 0)$, $\theta = -\pi$

14. $v = (1, -2, -1)$, $w = (0, 0, 1)$, $\theta = \frac{1}{2}\pi$

15. $v = (-2, -1, 1)$, $w = (1, 1, 1)$, $\theta = \frac{1}{3}\pi$

16. $v = (1, 1, -1)$, $w = (0, 0, 1)$, $\theta = \frac{3}{2}\pi$

8.2.6 Solutions

1. $\approx (-1.64, -0.667, 2.98)$

2. $\approx (-1.00, 2.00, -2.00)$

3. $\approx (1.33, -1.91, 0.756)$

4. $\approx (-2.64, 0.244, 1.40)$

5. $\approx (2.00, 1.00, -1.00)$

6. $\approx (-0.134, 2.23, -1.00)$

7. $\approx (0.333, -1.67, 0.333)$

8. $\approx (-1.00, -1.00, 2.00)$

9. $\approx (-0.333, -0.667, -2.33)$

10. $\approx (1.00, 2.00, -2.00)$

11. $\approx (0.366, -1.37, 1.00)$

12. $\approx (-2.00, 2.00, -1.00)$

13. $\approx (1.00, 2.00, 2.00)$

14. $\approx (2.00, 1.00, -1.00)$

15. $\approx (-0.333, -2.33, 0.667)$

16. $\approx (1.00, -1.00, -1.00)$

Number Theory

9

Matrices in Modular Arithmetic

9.1

9.1.1 \mathbb{Z} -modules	1033
9.1.2 Chinese Remainder Theorem	1044
9.1.3 Arithmetic With Bar Notation	1057
9.1.4 Classifying \mathbb{Z} -modules	1058
9.1.5 Multiplicative Groups and Exponents	1060
9.1.6 Exercises	1071
9.1.7 Solutions	1073

Questions to Guide Your Study:

- *What is a \mathbb{Z} -module and what are some ways of thinking about \mathbb{Z} -module quotients?*
- *What is the Chinese Remainder Theorem and how is it useful for solving systems of congruences?*
- *What are some quick matrix techniques for solving systems of congruences?*
- *What are the principles of modular arithmetic (in and out principles) and how do they come from cosets?*
- *What are the different types of \mathbb{Z} -modules are possible?*
- *What are some ways of finding multiplicative inverses in modular arithmetic?*

9.1.1 \mathbb{Z} -modules

\mathbb{Z} -module

A \mathbb{Z} -module is the same thing as a vector space *except* the scalars come from \mathbb{Z} . Some common examples are

- \mathbb{Z} the integers themselves.
- $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ which consists of pairs of integers (x, y) like $(2, 7)$ or $(-1543, 78)$.
- $\mathbb{Z}^3 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ which consists of triples of integers (x, y, z) like $(5, 3, 2)$ or $(99, -375, -100)$.

Free \mathbb{Z} -module (finitely generated)

We will call a (finitely generated) \mathbb{Z} -module that can be described (at least isomorphically) as \mathbb{Z}^m for some m a free (finitely generated) \mathbb{Z} -module. We say “finitely generated” to mean that the module is the \mathbb{Z} -span of finitely many elements. We will not call the elements of a \mathbb{Z} -module vectors—just elements.

All finitely generated vector spaces with scalars in \mathbb{R} can isomorphically be thought of as \mathbb{R}^m for some m . They are *all* free \mathbb{R} -modules. *But not all finitely generated \mathbb{Z} modules are free.* We will see some examples shortly!

Submodule

A submodule is to a module what a subspace is to a vector space.

\mathbb{Z} -Rank of a \mathbb{Z} -module

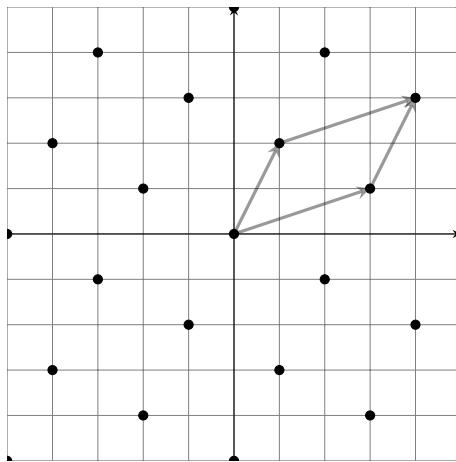
The \mathbb{Z} -rank of a module is the size of the smallest set of elements whose \mathbb{Z} -span is the whole module. It is like dimension—but we give it a different name because *rank alone cannot determine if a submodule is equal to the module—but dimension in a vector space would be enough!*

Example 1. Let's look at an example of a submodule of \mathbb{Z}^2 . Let $A = \langle (3, 1), (1, 2) \rangle_{\mathbb{Z}}$ where the \mathbb{Z} implies that we are taking a span with respect to \mathbb{Z} . Then A is a submodule of \mathbb{Z}^2 . The rank of A is 2 and the rank of $\mathbb{Z}^2 = \langle e_1, e_2 \rangle_{\mathbb{Z}}$ is also 2.

Generators

We say that that $(3, 1)$ and $(1, 2)$ generate A over \mathbb{Z} if A is the \mathbb{Z} -span of $(3, 1)$ and $(1, 2)$.

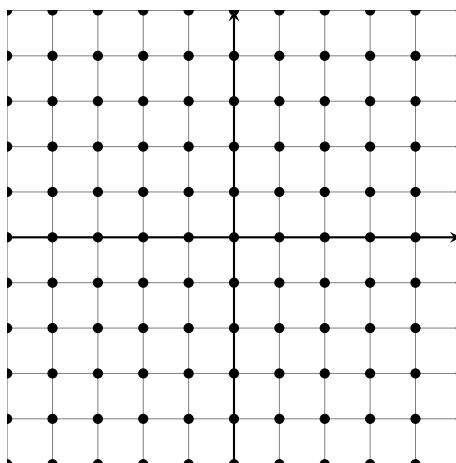
Let's see visually why $A \neq \mathbb{Z}^2$. The submodule A can be pictured as points in \mathbb{Z}^2 as follows:



Fundamental Parallelogram

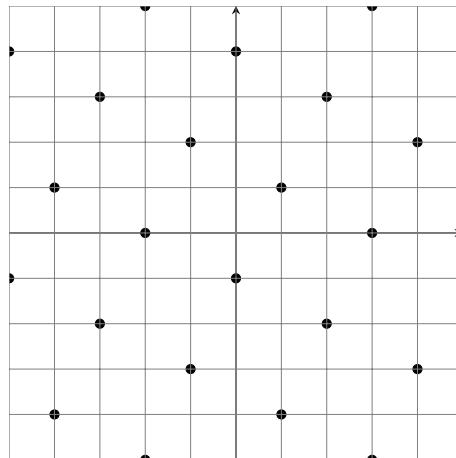
We have represented a fundamental parallelogram that describes the submodule A in the illustration above.

Yet \mathbb{Z}^2 is represented by points in the following way:

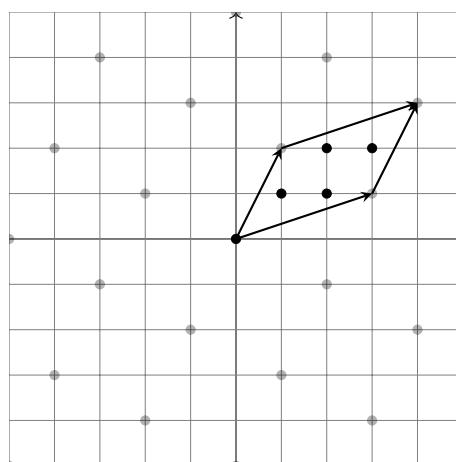


Just like we can shift a subspace (like looking at parallel planes), we can shift a submodule.

Example 2. The following picture represents a shift of the submodule A :



We can count how many shifts of A there are in \mathbb{Z}^2 by capturing one point of each shift in a fundamental parallelogram that describes A .



What is a good way to computationally determine how many shifts there are of a submodule?

\mathbb{Z} -module Homomorphism (Map)

An additive function that is scalable with respect to scalars in \mathbb{Z} is not called a linear transformation—that is reserved when we are dealing with vector spaces and scalars from a field. Here in this case, we say that we are dealing with a \mathbb{Z} -module map—yet most commonly a \mathbb{Z} -module homomorphism.

\mathbb{Z} -module homomorphisms $\mathbb{Z}^m \rightarrow \mathbb{Z}^n$ are represented by matrices just like linear transformations $\mathbb{R}^m \rightarrow \mathbb{R}^n$ are. The main difference is that the matrix entries of the \mathbb{Z} -module homomorphism *must* be integers.

\mathbb{Z} -module Isomorphism

A \mathbb{Z} -module isomorphism is a \mathbb{Z} -module homomorphism which has an inverse function which is also a \mathbb{Z} -module homomorphism.

Invertible integers

Multiplication by an integer is a \mathbb{Z} -module homomorphism. But it is not an isomorphism unless the inverse which is multiplication by the multiplicative inverse of the integer is also multiplication by an integer. The only integers whose multiplicative inverses are again integers are:

$$\begin{array}{c} -1 \\ \quad \quad \quad 1 \end{array}$$

\mathbb{Z} -basis

A \mathbb{Z} -basis for a \mathbb{Z} -module K is a minimal collection of elements whose \mathbb{Z} -span is all of K . There is no collection that spans the whole space with a fewer number of elements in it.

Changing the \mathbb{Z} -basis does not add or subtract points from the \mathbb{Z} -module—it keeps the module the same.

\mathbb{Z} Row and Column Operations

Let a matrix M represent a \mathbb{Z} -module homomorphism. A row or column operation turned into a column interpretation matrix represents a \mathbb{Z} -module isomorphism *as long as rescaling only happens by invertible integers.*

Theorem 9.1.1

A \mathbb{Z} -module isomorphism $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ bijectively sends the shifts of a submodule A to the shifts of the submodule $f(A)$.

Proof. Let f be the isomorphism. We can describe a shift of A by $w + A$ for some $w \in \mathbb{Z}^2$. First notice that since f is additive, $f(w + A) = f(w) + f(A)$ so that f really does give a function from shifts of A to shifts of $f(A)$. Suppose that we have two distinct shifts of A and that w is one and v is the other. Note that $w + a \neq v$ no matter which $a \in A$ we choose. Because f is additive and bijective, $f(w) + f(a) \neq f(v)$ no matter which $f(a) \in f(A)$ we choose. That is, $f(w)$ and $f(v)$ are in distinct shifts of $f(A)$. This means that the two distinct shifts $w + A$ and $v + A$ are sent to two distinct shifts $f(w) + f(A)$ and $f(v) + f(A)$. So the map of shifts is injective. Since f is surjective, a shift $r + f(A)$ is the image of the shift $w + A$ for some w where $f(w) = r$. So the map of shifts is surjective. We have a bijective mapping between shifts. \square

Let's apply \mathbb{Z} -module isomorphisms to \mathbb{Z}^2 that change our fundamental parallelogram to a rectangle. *It is easier to count points in a rectangle!*

Theorem 9.1.2

Let A be the \mathbb{Z} -span of $u, v \in \mathbb{Z}^2$. Make a matrix with u and v as columns: $M = \begin{pmatrix} u & v \end{pmatrix}$. Then, let B be the \mathbb{Z} -span of the the columns of $R \cdot M \cdot C$ where R represents a row operations matrix and C represents a column operations matrix where the only rescalings if any are by invertible integers. Then the shifts of A are in bijective correspondence with the shifts of B .

Proof. Think of what happens:

- The matrix C is an isomorphism so that the span of the columns of MC is the same as the span of the columns of M .
- Then, R is an isomorphism f that sends A to $f(A)$ given as the span of the columns of RMC .
- This isomorphism bijectively sends the shifts of A to the shifts of $f(A)$.

\square

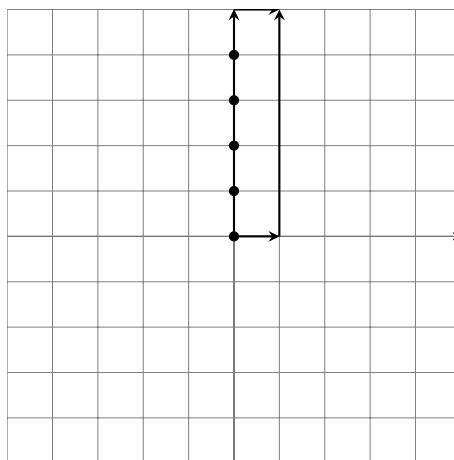
Example 3. Start with the submodule A we have above which is the span of $(3, 1)$ and $(1, 2)$. Put these ordered pairs into the columns of a matrix:

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

Performing only airdrops and switches and rescaling by -1 , we have:

$$\begin{array}{ccc} \left(\begin{array}{cc} 3 & 1 \\ 1 & 2 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & 2 \\ -3 \cdot 1 & -3 \cdot 2 \\ 3 & 1 \end{array} \right) \\ \left(\begin{array}{cc} -2 \cdot 1 & 2 \\ 1 & -2 \cdot 0 \\ 0 & -5 \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & 0 \\ -1 \cdot 0 & -1 \cdot -5 \end{array} \right) \\ & & \left(\begin{array}{cc} 1 & 0 \\ 0 & 5 \end{array} \right) \end{array}$$

We can represent a point in each shift in the fundamental parallelogram of the \mathbb{Z} -span of $(1, 0)$ and $(0, 5)$ as follows:



There are 5 distinct shifts.

Cosets

These shifts are called cosets of the submodule A in \mathbb{Z}^2

Notice how we included points on one boundary but not the other. That is because the points on opposite sides are a $(1, 0)$ shift apart. *We are trying to just capture one point from each shift.*

Corollary 9.1.3

The absolute value of the determinant of M counts the number of cosets of A in \mathbb{Z}^2 if A is a \mathbb{Z} -rank 2 submodule of \mathbb{Z}^2 .

Proof. In section 7.3 we discussed how the Euclidean algorithm can be used with our type of row and column operations to make a diagonal matrix. That is, with the Euclidean algorithm applied to integers instead of polynomials, we can choose R and C according to our parameters so that the columns of $R \cdot M \cdot C$ make a rectangular parallelogram (i.e. a rectangle). The area of the rectangle counts the desired points. This area is the absolute value of the determinant:

$$\det(R \cdot M \cdot C)$$

Yet the determinants of $\det(R)$ and $\det(C)$ are invertible integers since their inverses must also be \mathbb{Z} -module isomorphisms representable as integer matrices:

$$\det(R^{-1}) = \frac{1}{\det(R)} \in \mathbb{Z} \quad \det(C^{-1}) = \frac{1}{\det(C)} \in \mathbb{Z}$$

This means that the absolute value of $\det(M)$ counts the number of distinct shifts. □

Example 4. We take the determinant:

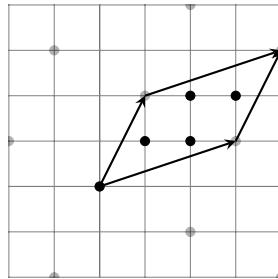
$$\det \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} = 5$$

This counts how many distinct cosets there are of A in \mathbb{Z}^2

Quotient Module

We define a \mathbb{Z} -module \mathbb{Z}^2/A . Call it the *quotient module* of \mathbb{Z}^2 with A . The elements in this \mathbb{Z} -module are the cosets of A in \mathbb{Z}^2 . Each element is a shift of a submodule. This is exactly how we thought about quotient vector spaces. The cosets of \mathbb{Z}^2/A can be labeled or determined from a set of representatives from each shift in a fundamental parallelogram describing A .

Example 5. For our running example, we can think of the points of \mathbb{Z}^2/A as being the points inside of the illustrated fundamental parallelogram:



Cosets, Addition, and Scalar Multiplication

Each coset of A in \mathbb{Z}^2 can be represented as:

$$(\text{point}) + A$$

where (point) is any point in the coset! It is like we have moved the origin to then (point) and then graphed the points of A from this *new origin*. Any point in the coset gives the same picture. Then, to add two cosets:

$$\left((\text{point 1}) + A \right) + \left((\text{point 2}) + A \right) = ((\text{point 1}) + (\text{point 2})) + A$$

To rescale:

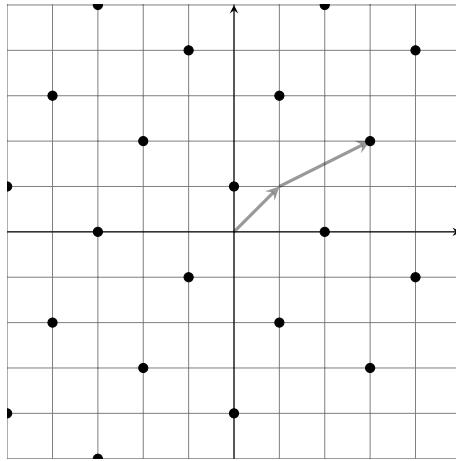
$$m \cdot \left((\text{point 1}) + A \right) = m \cdot (\text{point}) + A$$

Let's label the cosets of A as:

$$\underbrace{(0, 0) + A}_{\text{just } A} \quad (1, 1) + A \quad (2, 1) + A \quad (2, 2) + A \quad (3, 2) + A$$

where the points $(0, 0), (1, 1), (2, 1), (2, 2), (3, 2)$ were the points in the fundamental parallelogram of A .

Example 6. To add two cosets (i.e. two shifts) of A together is just like performing one shift and then the other:



$$((1,1) + A) + ((2,1) + A) = \underbrace{(3,2)}_{(1,1)+(2,1)} + A$$

We have shifted A to start from $(1, 1)$ and then we shifted $(2, 1)$ further so that it starts from $(3, 2)$.

This quotient \mathbb{Z} -module does not isomorphically look like \mathbb{Z}^m for any m at all: *it only has 5 elements.* It is an example of a \mathbb{Z} -module which is not free.

Example 7. Consider the quotient \mathbb{Z} -module $\mathbb{Z}/5\mathbb{Z}$. The set $5\mathbb{Z}$ is “all integers multiplied by 5” or just simply “all multiples of 5.” This set is a \mathbb{Z} -module: *it is closed under addition and also \mathbb{Z} -scalar multiplication.* The \mathbb{Z} -module $5\mathbb{Z}$ is a submodule of the \mathbb{Z} -module \mathbb{Z} itself. (In other words, $5\mathbb{Z}$ is a subset of \mathbb{Z} whose addition and multiplication are borrowed from \mathbb{Z} itself.) The elements of $\mathbb{Z}/5\mathbb{Z}$ are the cosets of $5\mathbb{Z}$:

$$5\mathbb{Z} \quad 1 + 5\mathbb{Z} \quad 2 + 5\mathbb{Z} \quad 3 + 5\mathbb{Z} \quad 4 + 5\mathbb{Z}$$

Bar Notation for Quotients

In our example of $\mathbb{Z}/5\mathbb{Z}$, let $a \in \mathbb{Z}$. Then, \bar{a} is the coset of $5\mathbb{Z}$ that a is an element of. In particular, $a \in a + 5\mathbb{Z}$.

Example 8. In the quotient $\mathbb{Z}/5\mathbb{Z}$,

$$\bar{0} = \bar{5} = \bar{10}$$

$$\bar{3} = \bar{8} = \bar{-2}$$

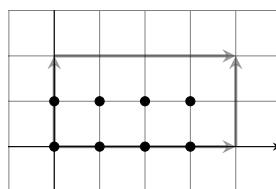
In this example, $\bar{a} = \bar{b}$ if and only if a and b are a multiple of 5 apart.

The quotient $\mathbb{Z}/5\mathbb{Z}$ is an example of a \mathbb{Z} -module which is not free.

Example 9. Our row and column operations which did not rescale past (-1) were additive and \mathbb{Z} -scalable bijections that changed \mathbb{Z}^2/A to *isomorphically* look like

$$\underbrace{\mathbb{Z}/\mathbb{Z}}_{\text{one element}} \times \underbrace{\mathbb{Z}/5\mathbb{Z}}_{(1 \text{ shift})}$$

Example 10. Let $C = \langle (4, 0), (0, 2) \rangle$. The \mathbb{Z} -module \mathbb{Z}^2/C gives an addition structure to the points within the following rectangle where we do not take points on opposite sides of the rectangle since they are shifts of each other across this fundamental rectangle (parallelogram).



Each point illustrated represents a distinct coset—a distinct shift of C . Moving from one of these points 4 units in the x -direction will take us back to the same coset. Likewise, moving 2 units in the y direction will take us back to the same coset. *It is like* values on the x axis are the same if they are a multiple of 2 apart (i.e. represent the same coset in $\mathbb{Z}/2\mathbb{Z}$) and values on the y -axis are the same if they are a multiple of 4 apart. This rectangle of points can be thought of as:

$$\underbrace{\mathbb{Z}/4\mathbb{Z}}_{x\text{-axis}} \times \underbrace{\mathbb{Z}/2\mathbb{Z}}_{y\text{-axis}}$$

Example 11. Let $\overline{}$ be the bar notation for cosets of $4\mathbb{Z}$ in \mathbb{Z} and $\overline{}$ be the bar notation for cosets of $2\mathbb{Z}$ in \mathbb{Z} . Then $(\overline{a}, \overline{b})$ for $a, b \in \mathbb{Z}$ is an element of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and uniquely describes one of the points in our rectangle. If we let $\underline{}$ be the bar notation for cosets in C , then both $(\overline{a}, \overline{b})$ and $(\underline{a}, \underline{b})$ represent the same point in our rectangle for every $a, b \in \mathbb{Z}$ which means that they both describe the same points in \mathbb{Z}^2 .

Let's think of how to add the two points together:

$$\left(\begin{smallmatrix} \textcolor{red}{1} \\ \textcolor{green}{2} \end{smallmatrix} \right) + \left(\begin{smallmatrix} \textcolor{red}{1} \\ \textcolor{green}{3} \end{smallmatrix} \right)$$

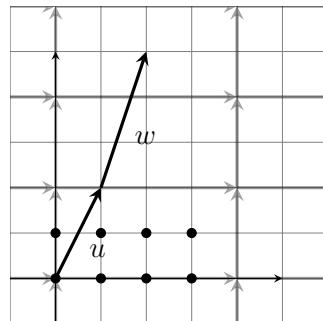
We can think in terms of cosets of C :

$$\begin{aligned} \overline{(1, 2)} + \overline{(1, 3)} &= ((1, 2) + C) + ((1, 3) + C) = ((1, 2) + (1, 3)) + C = (2, 5) + C \\ &= \overline{(2, 5)} = \left(\begin{smallmatrix} \textcolor{red}{2} \\ \textcolor{green}{5} \end{smallmatrix} \right) \end{aligned}$$

Now $2 \in 2 + 4\mathbb{Z} = \textcolor{red}{2}$ and $5 \in 1 + 2\mathbb{Z} = \textcolor{green}{1}$ so that:

$$\left(\begin{smallmatrix} \textcolor{red}{1} \\ \textcolor{green}{2} \end{smallmatrix} \right) + \left(\begin{smallmatrix} \textcolor{red}{1} \\ \textcolor{green}{3} \end{smallmatrix} \right) = \left(\begin{smallmatrix} \textcolor{red}{2} \\ \textcolor{green}{1} \end{smallmatrix} \right)$$

In a picture, it is like we are adding vectors in \mathbb{Z}^2 to get $(2, 5)$ and then shifting back by something in C to get back to the fundamental rectangle. *But also, the arrow addition in \mathbb{Z}^2 that yields $(2, 5)$ takes us to a point in a shift of the fundamental rectangle which corresponds to $(2, 1)$:*



This addition that we have in \mathbb{Z}^2/C which is the same as $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ helps turn the collection of cosets into a \mathbb{Z} -module itself!

Scalar multiplication by a positive integer just means repeated addition. Scalar multiplication by a negative integer just means repeated addition of an additive inverse.

The idea of \mathbb{Z} scalars distributing over addition is the same thing as being able to reorder our addition $a + b = b + a$. The ideas of a group where the addition is commutative and being a \mathbb{Z} -module *are the same!*

$$2 \cdot (a + b) = (a + b) + (a + b) = (a + a) + (b + b) = 2a + 2b$$

Theorem 9.1.4

Quotients of \mathbb{Z} -modules are \mathbb{Z} -modules with a well-defined addition among the cosets.

Theorem 9.1.5

\mathbb{Z} -modules are simply groups where the group operation is commutative. We have been focusing on the group operation of addition so far.

9.1.2 Chinese Remainder Theorem

We can think of the quotient $\mathbb{Z}/m\mathbb{Z}$ which is a collection of m cosets also as a quotient \mathbb{Z}^2/A where $A = \langle(1, 0), (0, m)\rangle$. *The $(1, 0)$ causes the first component to be ignored!*

Notice that inside of A is *everything* like $(\star, 0)$. So A in the first component is all of \mathbb{Z} . In the first component *there is only one shift of A* —just the whole first component—all of \mathbb{Z} itself. Therefore, the first component *is ignored* in the quotient. Yet in the second component, we have m shifts of $m\mathbb{Z}$:

$$m\mathbb{Z} \quad 1 + m\mathbb{Z} \quad 2 + m\mathbb{Z} \quad \dots \quad (m - 1) + m\mathbb{Z}.$$

Notice that there are the same number of cosets described by $\mathbb{Z}/ab\mathbb{Z}$ as there are described by $\mathbb{Z}/a \times \mathbb{Z}/b$. Can we create a bijective correspondence between these two \mathbb{Z} -modules which is an additive and scalable—a \mathbb{Z} -module isomorphism?

We have already seen the usefulness of functions that are not just simple correspondences but transfer addition and scalar action from input to output. This whole text has been devoted to them—they are called *linear transformations* for vector spaces and for \mathbb{Z} -modules they are called \mathbb{Z} -module homomorphisms. This is no exception. Correspondences should be given by \mathbb{Z} -module homomorphisms.

The answer is that we can if $\gcd(a, b) = 1$. In order to prove this result, we appeal to the following lemma which is a consequence of working the Euclidean algorithm backwards:

Lemma 9.1.6

If $\gcd(a, b) = 1$, then there exist integers k and t such that $ka + tb = 1$. In other words, 1 is in the \mathbb{Z} -span of a and b . We could even say:

$$\langle a, b \rangle_{\mathbb{Z}} = \langle \gcd(a, b) \rangle_{\mathbb{Z}} \quad a, b \in \mathbb{Z}$$

Proof. Suppose that $a > b$. Then, $a = q_0b + r_0$ where q_0 is the quotient and r_0 is the remainder of dividing b into a . Repeat this process as follows. The last nonzero remainder r_m is $\gcd(a, b)$.

$$\begin{array}{rcl} a & = & q_0 \cdot b + r_0 \\ b & = & q_1 \cdot r_0 + r_1 \\ r_0 & = & q_2 \cdot r_1 + r_2 \\ r_1 & = & q_3 \cdot r_2 + r_3 \\ \vdots & \vdots & \vdots \quad \vdots \quad \vdots \\ r_{m-2} & = & q_m \cdot r_{m-1} + r_m \\ r_{m-1} & = & q_{m+1} \cdot r_m + 0 \end{array}$$

Using these lines, we note that since r_0 is in the span of a and b . This implies that r_1 is also in the span of a and b . This continues on down to $r_m = \gcd(a, b)$. Hence, $\gcd(a, b) \in \langle a, b \rangle$. But also a and b are multiples of $\gcd(a, b)$. This means that $a, b \in \langle \gcd(a, b) \rangle$. Hence,

$$\langle \gcd(a, b) \rangle = \langle a, b \rangle$$

as desired. □

Theorem 9.1.7 Chinese Remainder Theorem (\mathbb{Z} -module version)

Given two integers a and b whose greatest common factor (divisor) is 1, there exists a \mathbb{Z} -module isomorphism:

$$\mathbb{Z}/ab\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

Proof. Let's find a \mathbb{Z} -module isomorphism $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ that takes $A = \langle (1, 0), (0, ab) \rangle$ to $f(A) = \langle (a, 0), (0, b) \rangle$. This function f would send a shift of A to a shift of $f(A)$. We also know already that if

we had such a f that:

$$\mathbb{Z}^2/A = \mathbb{Z}^2/(\mathbb{Z} \times ab\mathbb{Z}) = \mathbb{Z}/ab\mathbb{Z} \quad (\text{just like we discussed above with } m = ab)$$

$$\mathbb{Z}^2/f(A) = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \quad (\text{just like our example with } \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

Further:

$$\begin{aligned} & \underbrace{(x+A) + (y+A)}_{\text{Coset addition in a quotient.}} = (x+y) + A \implies \\ & f((x+y) + A) = \underbrace{\underbrace{f(x+y)}_{= (f(x)+f(y))} + f(A)}_{\text{Coset addition in a quotient.}} = (f(x) + f(A)) + (f(y) + f(A)) \end{aligned}$$

So that f would be additive map from coset collection to coset collection. And lastly:

Since f is a \mathbb{Z} -module isomorphism, it induces a bijection between the coset collections.

All of these facts would give us a \mathbb{Z} -module isomorphism $\mathbb{Z}/ab\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ as we desire.

All we do is row and column operations (only potentially rescaling by invertible integers) on

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

until we arrive at

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

The row operations matrix R would then give us the isomorphism f . The column operations matrix is just taking linear combinations of things in the domain (or equivalently the codomain across the isomorphism) so that we can check if $(a, 0)$ and $(0, b)$ are really in the range. But the isomorphism itself is established by the row operations.

The row operations matrix R gives the isomorphism and the column operations matrix explores what is in the range of R . In particular, *the outcome of the row and column operations gives us two columns that span $f(A)$* .

So, let's perform some operations:

$$\begin{array}{ccc}
 \left(\begin{array}{cc} 1 & 0 \\ +1 \cdot 0 & +1 \cdot ab \\ 0 & ab \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} -(b-1)a \cdot 1 & ab \\ 1 & ab \\ -(b-1)a \cdot 0 & ab \\ 0 & ab \end{array} \right) \\
 \left(\begin{array}{cc} 1 & a \\ -b \cdot 1 & -b \cdot a \\ 0 & ab \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} 1 & a \\ -b & 0 \end{array} \right) \\
 \left(\begin{array}{cc} a & 1 \\ +t \cdot 0 & +t \cdot (-b) \\ 0 & -b \end{array} \right) & \xrightarrow{\quad} & \left(\begin{array}{cc} -k \cdot a & 1 - tb \\ a & 1 - tb \\ -k \cdot 0 & -b \end{array} \right)
 \end{array}$$

We use the fact that $1 - rb - ka = 0$ since $rb + ka = 1$.

$$\left(\begin{array}{cc} a & 1 - rb - ka \\ 0 & -b \end{array} \right) \xrightarrow{\quad} \left(\begin{array}{cc} a & 0 \\ 0 & b \end{array} \right) \xrightarrow{\quad}$$

This is as desired so that $f(A)$ really is the span of $(a, 0)$ and $(0, b)$ as desired. The row operations matrix formed by applying *only* the row operations to the identity matrix is the following where we use the fact that $1 - tb = ka$

$$R = \begin{pmatrix} 1 - tb & 1 + t - tb \\ -b & 1 - b \end{pmatrix} = \begin{pmatrix} 1 - tb & t + ka \\ -b & 1 - b \end{pmatrix}$$

So f will be represented by this row operations matrix. This is a well-defined \mathbb{Z} -module isomorphism. \square

In particular, let's see where this isomorphism takes the coset $(0, 1) + A$. We know that

$$f((0, 1) + A) = f(0, 1) + f(A) = (t + ka, 1 - b) = (t, 1) + \underbrace{(ka, -b)}_{\in f(A)}$$

That is, $(ka, -b) = k \cdot (a, 0) - 1 \cdot (0, b) \in f(A)$. Hence, $(0, 1) + A \mapsto (t, 1) + f(A)$.

So what we have is a \mathbb{Z} -module isomorphism $\mathbb{Z}/ab\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ which is additive.

This map between quotients is induced by f . But let's give it a different name than f . Let's call it \tilde{f} .

Remembering that multiplication by scalars in \mathbb{Z} is the same thing as repeated addition, one could think that there is a definite multiplication structure in $\mathbb{Z}/m\mathbb{Z}$ for a given m . Let $\underline{\quad}$ be used to represent the cosets in the collection $\mathbb{Z}/m\mathbb{Z}$. Then, as an example, $2 \cdot \underline{3} = 2 \cdot (3 + m\mathbb{Z}) = (3 + m\mathbb{Z}) + (3 + m\mathbb{Z}) = (3 + 3) + m\mathbb{Z} = (2 \cdot 3) + m\mathbb{Z} = \underline{2 \cdot 3}$. Yet notice that this is also $\underline{3} \cdot \underline{2}$ by similar reasoning. We could just define $\underline{3} \cdot \underline{2} = \underline{3 \cdot 2}$.

Multiplication for a Ring

In many \mathbb{Z} -modules there is a natural multiplication structure that arises very naturally. In fact in $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ it is perfectly natural just to make this multiplication component-wise so

$(\underline{2}, \underline{3}) \cdot (\underline{4}, \underline{5}) = (\underline{2 \cdot 4}, \underline{3 \cdot 5})$. This multiplication structure, as long as there is a multiplicative identity element can make a \mathbb{Z} -module into a ring. A ring is an additive group that also has a well-defined (commutative and associative) multiplication structure with an multiplicative identity. Multiplicative inverses *are not required*.

The problem with \tilde{f} is that it does not respect this multiplication very well. That is, $\tilde{f}(u \cdot w) \neq \tilde{f}(u) \cdot \tilde{f}(w)$. *it is not multiplicative. The reason \tilde{f} is not multiplicative is because multiplicative maps must send multiplicative identities to multiplicative identities and the our \tilde{f} map does not as we now explain.*

Note that $1 + ab\mathbb{Z}$ is the multiplicative identity of $\mathbb{Z}/ab\mathbb{Z}$. This is the same as $(0, 1) + A$ which describes the multiplicative identity of \mathbb{Z}^2/A (which we thought of as $\mathbb{Z}/ab\mathbb{Z}$). Our map \tilde{f} sent this multiplicative identity element to $(t, 1) + f(A)$. Yet the multiplicative identity should be the shift $(1, 1) + f(A)$. Note that the only way for $(t, 1) - (1, 1) = (t - 1, 0)$ to be in $f(A)$ is for $t - 1$ to be a multiple of a . This means that $(1, 1)$ and $(t, 1)$ *cannot be in the same shift of $f(A)$* and we are out of luck.

So now, we have a new goal of finding a desired isomorphism that will replace \tilde{f} with a map that is multiplicative.

Ring Homomorphism

Given two rings R_1 and R_2 that are \mathbb{Z} -modules, a ring homomorphism $\tilde{f} : R_1 \rightarrow R_2$ between them is a \mathbb{Z} -module homomorphism which is multiplicative.

Theorem 9.1.8 Chinese Remainder Theorem (Ring Version)

Given two integers a and b whose greatest common factor (divisor) is 1, there exists a ring isomorphism:

$$\tilde{f} : \mathbb{Z}/ab\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

Let k and t be integers such that $ka + tb = 1$.

Proof. To find this map \tilde{f} , we go back to our original situation when we were trying to find an isomorphism $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ that would send A to $f(A)$. This time, let's build a matrix that has a determinant of 1: this means that its inverse matrix has all its entries in \mathbb{Z} and so is a \mathbb{Z} -module homomorphism in reverse. Let's also ensure that the multiplicative identity of $\mathbb{Z}/ab\mathbb{Z}$ thought of as $(0, 1)$ in \mathbb{Z}^2/A is sent to $(1, 1) + f(A)$. That is, let's put the second column as $(1, 1)$:

$$f : \begin{pmatrix} ka & 1 \\ -tb & 1 \end{pmatrix}$$

Notice that the determinant is $ka + tb = 1$ as desired. So now all we have to check is if $f(A)$ is really $\langle (a, 0), (0, b) \rangle$. To do this, we just need to check if $f^{-1}(a, 0) \in A$ and $f^{-1}(0, b) \in A$. This is because \mathbb{Z}^2/A has ab cosets and if $f(A)$ were bigger than $\langle (a, 0), (0, b) \rangle$, then $\mathbb{Z}^2/f(A)$ would have less than ab cosets since already $\det \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = ab$. We compute the inverse matrix easily since the determinant is 1:

$$f^{-1} : \begin{pmatrix} 1 & -1 \\ tb & ka \end{pmatrix}$$

$$f^{-1}(a, 0) = \begin{pmatrix} 1 & -1 \\ tb & ka \end{pmatrix} \cdot \begin{pmatrix} a \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ tab \end{pmatrix}$$

Notice that

$$f^{-1}(a, 0) = (a, tab) = a \cdot (1, 0) + t \cdot (0, ab) \in A$$

Similarly,

$$f^{-1}(0, b) = (-b, kab) \in A$$

Remember that f is a map $\mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ and we let \tilde{f} be the corresponding map on quotients $\mathbb{Z}^2/A \rightarrow \mathbb{Z}^2/f(A)$.

Great! But is \tilde{f} which maps bijectively from \mathbb{Z}^2/A to $\mathbb{Z}^2/f(A)$ multiplicative?

We know that all the cosets of \mathbb{Z}^2/A can be represented as $(0, x)$ for an integer x since $(\star, 0) \in A$ for every \star . This means we can always shift any element of \mathbb{Z}^2 via A to an element $(0, x)$. In particular, we can think of $(0, x)$ as representing the coset $\underline{x} \in \mathbb{Z}/ab\mathbb{Z}$. We have:

$$\tilde{f}(\underline{x} \cdot \underline{y}) = \tilde{f}(\underline{xy})$$

Now, $\tilde{f}(\overline{xy})$ comes from

$$f(0, xy) = xy \cdot f(0, 1) = xy \cdot (1, 1) = (xy, xy) = \underbrace{(x, x) \cdot (y, y)}_{\text{component-wise}} = f(0, x) \cdot f(0, y)$$

This tells us,

$$\tilde{f}(\overline{xy}) = \tilde{f}(\overline{x}) \cdot \tilde{f}(\overline{y})$$

Therefore, our mission is accomplished. We have produced a nice *ring isomorphism*

$$\mathbb{Z}/ab\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

□

Corollary 9.1.9

Given two integers a and b whose greatest common factor (divisor) is 1, then the ring homomorphisms \tilde{f} and \tilde{f}^{-1} described in the above theorem are induced by the following matrix functions (in a column interpretation) $\mathbb{Z}^2 \rightarrow \mathbb{Z}^2$:

$$f : \begin{pmatrix} ka & 1 \\ -tb & 1 \end{pmatrix} \quad f^{-1} : \begin{pmatrix} 1 & -1 \\ tb & ka \end{pmatrix}$$

Let k and t be integers such that $ka + tb = 1$.

How is this ring isomorphism \tilde{f} useful?

Example 12. We can use this ring isomorphism to help us solve systems of “coset equations.” That is, suppose that $\overline{}$ represents $\mathbb{Z}/3\mathbb{Z}$ and $\overline{}$ represents $\mathbb{Z}/5\mathbb{Z}$. Then perhaps we have a system of equations like:

$$\begin{array}{l} \overline{x} = \overline{2} \\ \overline{x} = \overline{3} \end{array}$$

where $x \in \mathbb{Z}$. Another way of writing this system is to take the overlines and just put them over “=” to have \equiv instead. Then, to remind us which quotient we are working in we write $\mod 3$ or $\mod 5$. That is, we have:

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \end{aligned}$$

Coset Equations, Systems of Congruences

Coset equations or systems of congruences for cosets of the kind $r + m\mathbb{Z}$ are systems like we have just discussed in the reading:

$$\begin{aligned}x &\equiv 2 \pmod{3} \\x &\equiv 3 \pmod{5}\end{aligned}$$

This means that we are trying to find x so that $x \in (2 + 3\mathbb{Z}) \cap (3 + 5\mathbb{Z})$

Notice that the ring isomorphism f that we have above sends

“ $1 \pmod{3 \cdot 5}$ ” to “ $(1 \pmod{3}, 1 \pmod{5})$ ” *multiplicative identity to multiplicative identity*.

Since, this is a \mathbb{Z} -module map, we can multiply this input and output by the scalar x .

“ $x \pmod{3 \cdot 5}$ ” goes to “ $(x \pmod{3}, x \pmod{5})$ ”

So, think of $\begin{pmatrix} \textcolor{red}{2} & \textcolor{green}{3} \end{pmatrix} = (x \pmod{3}, x \pmod{5})$. Then, the preimage of $\begin{pmatrix} \textcolor{red}{2} & \textcolor{green}{3} \end{pmatrix}$ is the coset $x + 3 \cdot 5 \cdot \mathbb{Z}$. We just need to find this x .

All we need to do is to compute $f^{-1}(2, 3)$ and we will have our solution! To simplify matters, we only need the bottom row of the matrix describing f^{-1} since we are only interested in the second component—the one that describes $(0, ab)$. That is, we compute:

$$\begin{pmatrix} tb & ka \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

to get an element in a coset of $ab\mathbb{Z}$. *That whole coset will uniquely solve the system because of the bijective correspondence between cosets.*

A whole coset of $ab\mathbb{Z}$ solves the system of coset equations.

Corollary 9.1.10

Suppose that $\gcd(a, b) = 1$. The map $\tilde{f}^{-1} : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \rightarrow \mathbb{Z}/ab\mathbb{Z}$ is given as the column interpretation map of the matrix

$$\tilde{f}^{-1} : \begin{pmatrix} tb & ka \end{pmatrix}$$

where $ka + tb = 1$. This map solves a system of equations.

Solving a System of Congruences

Suppose that we would like to solve a system of coset equations:

$$\begin{aligned} x &\equiv p_1 \pmod{a} \\ x &\equiv p_2 \pmod{b} \end{aligned}$$

We find t and k so that $ka + tb = 1$. Then, all solutions are given by:

$$\begin{pmatrix} tb & ka \end{pmatrix} \cdot \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} + ab\mathbb{Z}$$

In our particular situation, we need to find t and k for $a = 3$ and $b = 5$. Just by observation, we have:

$$\underbrace{-1}_{t} \cdot \underbrace{5}_b + \underbrace{2}_k \cdot \underbrace{3}_a = 1$$

Therefore, we compute:

$$f^{-1}(2, 3) = \begin{pmatrix} -5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 3 \end{pmatrix} = 8$$

Therefore, any x in $8 + 15\mathbb{Z}$ will solve the system. You can check: $8 \in 2 + 3\mathbb{Z}$ and $8 \in 3 + 5\mathbb{Z}$. If we add 15 to 8 we get 23. We know that $23 \in 2 + 3\mathbb{Z}$ and $23 \in 3 + 5\mathbb{Z}$.

How can we find this k and t so $ka + tb = 1$?

Example 13. Suppose that we have $a = 13$ and $b = 7$. The lines of the Euclidean algorithm look like:

$$\begin{array}{rcl} 13 & = & 1 \cdot 7 + 6 \\ 7 & = & 1 \cdot 6 + 1 \end{array}$$

Our goal is to write the last remainder (1) as an integer linear combination of 13 and 7. Let's do this one step at a time and try to generalize the idea. Think of the following labels:

$$\begin{array}{rcl} a & = & q_0 \cdot b + r_0 \\ b & = & q_1 \cdot r_0 + r_1 \end{array}$$

Think of shifting pairs $(a, b) \rightarrow (b, r_0) \rightarrow (r_0, r_1)$. Each of these shifts is like a function (even a linear transformation) $\mathbb{Z}^2 \rightarrow \mathbb{Z}^2$. We can write each shift as a matrix! Just think about a line of the algorithm:

$$x = q \cdot y + r$$

This line relates the pair (x, y) to the pair (y, r) . We can write r in terms of x and y :

$$r = x - q \cdot y$$

Hence,

$$(x, y) \mapsto (y, x - q \cdot y)$$

gives us the function (linear transformation) $\mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ we desire. Note that $e_1 = (1, 0) \mapsto (0, 1)$ and $e_2 = (0, 1) \mapsto (1, -q)$. Hence, we can write the matrix in a column interpretation as:

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

to represent the shifting where q is the quotient when y is divided by x . Notice that the second row $(1 \quad -q)$ is used in the multiplication to find r :

$$\begin{pmatrix} 1 & -q \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} b \\ r \end{pmatrix}$$

This row tells us how to write r as a linear combination of x and y . That is, $r = 1 \cdot x - q \cdot y$. Now perform two shifts in our current example:

$$\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}}_{f_1} \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}}_{f_0} = \underbrace{\begin{pmatrix} 1 & -q_0 \\ -q_1 & 1 - q_0 q_1 \end{pmatrix}}_{f_1 \circ f_0}$$

The second row of the product $\begin{pmatrix} -q_1 & 1 - q_0 q_1 \end{pmatrix}$ tells us how to write r_1 in terms of a and b . Let's do this with

numbers realizing that in our current example $q_0 = 1$ and $q_1 = -1$.

$$\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}}_{f_1} \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}}_{f_0} = \underbrace{\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}}_{f_1 \circ f_0}$$

So,

$$-1 \cdot 13 + 2 \cdot 7 = 1$$

Scalars to Make 1

Suppose that $\gcd(a, b) = 1$ and that $a > b$. Let q_0, q_1, \dots, q_r be the quotients in the Euclidean algorithm through to the last nonzero remainder. Suppose that $\begin{pmatrix} k & t \end{pmatrix}$ is the second row of the matrix product:

$$\begin{pmatrix} w & z \\ k & t \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & q_r \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & q_0 \end{pmatrix}$$

Then $ak + bt = 1$.

So when we find k and t , let's remember:

$$\underbrace{\begin{pmatrix} bt & ak \end{pmatrix}}_{\text{bottom row of } f^{-1}} \cdot \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$$

solves the system

$$\begin{aligned} x &\equiv p_1 \pmod{a} \\ x &\equiv p_2 \pmod{b} \end{aligned}$$

if $ak + bt = 1$.

Example 14. Let's use the values of $k = -1$ and $t = 2$ that we found in the last example to solve the system of coset equations:

$$x \equiv 4 \pmod{13}$$

$$x \equiv 5 \pmod{7}$$

We simply compute:

$$\underbrace{\begin{pmatrix} 2 \cdot 7 & -1 \cdot 13 \end{pmatrix}}_{\substack{\text{Bottom row of the ring} \\ \text{isomorphism } f^{-1}}} \cdot \underbrace{\begin{pmatrix} 4 \\ 5 \end{pmatrix}}_{\substack{\text{Coset representative in} \\ \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}}} = 14 \cdot 4 - 13 \cdot 5 = 56 - 65 = -9$$

Notice that -9 is in $4 + 13\mathbb{Z}$ since it is 4 more than $-13 \in 13\mathbb{Z}$ and it is also in $5 + 7\mathbb{Z}$ since it is 5 more than $-14 \in 7\mathbb{Z}$. If we add a multiple of $13 \cdot 7 = 91$, we should again get a solution. Since we get a whole coset of solutions. Notice that 82 is 4 more than $78 = 6 \cdot 13$ and 5 more than $77 = 7 \cdot 11$.

Example 15. What if we had more coset equations? Consider:

$$\begin{aligned} x &\equiv 4 \pmod{13} \\ x &\equiv 5 \pmod{7} \\ x &\equiv 1 \pmod{11} \end{aligned}$$

Notice that we already solved the system that contains the first two coset equations in the last example. The solution we obtained was $-9 \pmod{91}$. Any x that satisfies our current system with three coset equations will lie in the coset $-9 + 91\mathbb{Z}$. In fact, by our Chinese remainder theorem isomorphism, being in this coset is the same as being in $(4+13\mathbb{Z}) \cap (5+7\mathbb{Z})$. *This means that our first two coset equations can be replaced by $x \equiv -9 \pmod{91}$.* Therefore, we simply need to solve:

$$\begin{aligned} x &\equiv -9 \pmod{91} \\ x &\equiv 1 \pmod{11} \end{aligned}$$

We use the Euclidean algorithm with 91 and 11 :

$$\begin{array}{rcl} 91 & = & 8 \cdot 11 + 3 \\ 11 & = & 3 \cdot 3 + 2 \\ 3 & = & 1 \cdot 2 + 1 \end{array}$$

So we compute:

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} = \begin{pmatrix} -3 & 25 \\ 4 & -33 \end{pmatrix}$$

Therefore, using the bottom row:

$$4 \cdot 91 - 33 \cdot 11 = 364 - 363 = 1$$

Using the bottom row of f^{-1} in the ring version of the Chinese Remainder Theorem, we have:

$$\begin{pmatrix} -33 \cdot 11 & 4 \cdot 91 \end{pmatrix} \cdot \begin{pmatrix} -9 \\ 1 \end{pmatrix} = 3631$$

Remember that the solutions repeat themselves every $91 \cdot 11 = 1001$ so that we have $3631 - 3 \cdot 1001 = 628$ is also a solution. Checking: 628 is 1 more than $627 = 57 \cdot 11$ and it is 9 less than $637 = 91 \cdot 7$.

Variations to Finding Scalars

In our process for finding scalars k and t such that $ak + tb = 1$, there are a couple of variations. If $\gcd(a, b) \neq 1$, then the same process finds k and t such that

$$ak + tb = \gcd(a, b)$$

If instead one wishes to use a negative remainder in a step, the matrix at that step is the same except with the second column having the opposite sign:

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

In the end,

$$ak + tb = (\text{last nonzero remainder which could be } (\pm))$$

Example 16. In the last example, we could have shortened our Euclidean algorithm between 11 and 91 as follows:

$$\begin{array}{rcl} 91 & = & 8 \cdot 11 + 3 \\ 11 & = & 4 \cdot 3 - 1 \end{array}$$

$$\begin{pmatrix} 0 & -1 \\ 1 & -4 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} = \begin{pmatrix} -1 & 8 \\ -4 & 33 \end{pmatrix}$$

Notice that we get $-4 \cdot 91 + 33 \cdot 11 = -1$.

9.1.3 Arithmetic With Bar Notation

In and Out Principles

When working with the bar notation in $\mathbb{Z}/m\mathbb{Z}$, we have the following:

- $\overline{a + b} = \overline{a} + \overline{b}$
- $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$
- $\overline{a^m} = \overline{a^m}$

Proof. We have defined coset addition by the addition of coset representatives. Coset representatives are what put under the bar. Coset multiplication we also define as the multiplication of coset representatives. Exponents just capitalize on this idea in a repeated way. \square

Example 17. Working in $\mathbb{Z}/5\mathbb{Z}$, we can write $\overline{67}$ as $\overline{65 + 2}$ where we have purposely chosen a multiple of 5 close to 67. Then,

$$\begin{aligned}\overline{65 + 2} &= \underbrace{\overline{65}}_{= 0} + \overline{2} \\ &= 0\end{aligned}$$

Notice that we can write $\overline{65} = \overline{0}$ since 65 and 0 are in the same coset. Now, we write: $\overline{0} + \overline{2} = \overline{0 + 2} = \overline{2}$.

Simpler Representative Principle

We can always write $\overline{a} = \overline{b}$ if a and b are in the same coset. It is nice if we can choose a small, nice representative.

Example 18. In the last example, we replaced $\overline{67}$ with $\overline{2}$. Both 67 and 2 are in $\overline{2} = 2 + 5\mathbb{Z}$. In other words, $67 + 5\mathbb{Z} = 2 + 5\mathbb{Z}$.

Example 19. Let's compute $\overline{27}^7$ in $\mathbb{Z}/11\mathbb{Z}$. Firstly, we can replace $\overline{25}$ by $\overline{5}$ since 25 is 5 more than a multiple of 11. Next, we rewrite the exponent 7 as a sum of powers of 2:

$$\overline{5}^7 = \overline{5}^{2^2+2+1} = \overline{5}^{2^2} \cdot \overline{5}^2 \cdot \overline{5}^1$$

We compute

$$\overline{5}^2 = \overline{5^2} = \overline{25} = \overline{3} \quad \overline{5}^{2^2} = \overline{5^2}^2 = \overline{3^2} = \overline{9} = \overline{-2}$$

Notice that 9 and -2 are a multiple of 11 apart so that they are in the same coset. Now we have:

$$\begin{aligned} & \underbrace{\overline{5}^{2^2}}_{\overline{-2}} \cdot \underbrace{\overline{5}^2}_{\overline{3}} \cdot \overline{5}^1 = (-2) \cdot (3) \cdot (5) = (-10) \cdot 3 \\ & = (-10) \cdot \overline{3} = \overline{1} \cdot \overline{3} = \overline{1 \cdot 3} = \overline{3} \end{aligned}$$

Therefore, $\overline{27}^7 = \overline{3}$

Simpler at Every Step

Use the simpler representative principle at every step in a long calculation to avoid big numbers just like in the last example.

9.1.4 Classifying \mathbb{Z} -modules

Suppose that $a = 0$. Then if $A = \langle (a, 0), (0, b) \rangle$, the quotient \mathbb{Z}^2/A can be thought of as

$$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} = \mathbb{Z}/0\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} = \mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

This is because every element in \mathbb{Z} is already a unique shift (coset) of the \mathbb{Z} -module $\{0\}$. Ideas like this and the row and column operations of the last section can lead us to be able to describe isomorphically what all *finitely generated* \mathbb{Z} -modules look like.

Theorem 9.1.11 Classification of Finitely Generated \mathbb{Z} -modules

All finitely generated \mathbb{Z} -modules isomorphically look like

$$\mathbb{Z}^m \times \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_r\mathbb{Z}$$

for $m, r, a_1, \dots, a_r \in \mathbb{N}$.

Proof. Suppose that a \mathbb{Z} -module M is spanned by n elements x_1, \dots, x_n . Then we can think of n -tuples (a_1, \dots, a_n) of integer coefficients contained in \mathbb{Z}^n . This produces a nice \mathbb{Z} -module map (homomorphism) $\mathbb{Z}^n \rightarrow M$ given by $(a_1, \dots, a_n) \mapsto a_1x_1 + \cdots + a_nx_n$. Saying the module M is the span of x_1, \dots, x_n is

the same thing as saying that this map is surjective. The range is M . Each element of M describes a fiber box in a fiber box diagram. Each fiber box is a shift of the fiber over the additive identity of M . This is because our map is additive. That is, M is isomorphically described as a quotient of \mathbb{Z}^n with the submodule K that represents the fiber over the additive identity of M —zero. That is, K is the kernel.

Now, we can think of M isomorphically as \mathbb{Z}^n/K . Consider the case $n = 1$. The only possible submodules of \mathbb{Z}^1 that could possibly be K are of the form $m\mathbb{Z}$. This is because of the idea that the integer span of any integers r and t is the integer span of $\gcd(r, t)$. Not only that, but we can continue this idea even if we had an infinite list of integers u_1, u_2, \dots all in K . We would note that that the sequence

$$\{\gcd(u_1), \gcd(u_1, u_2), \gcd(u_1, u_2, u_3), \dots, \gcd(u_1, \dots, u_k), \dots\}$$

has a minimum value m since all subsets of integers have a minimum. This would yield that $K = m\mathbb{Z}$ so that M could be thought of as $\mathbb{Z}/m\mathbb{Z}$.

Now consider the case $n = 2$. Suppose first that we have a sequence of elements $(u_1, w_1), (u_2, w_2), \dots$ that span K . Let K' be the \mathbb{Z} -module consisting of all elements of K of the form $(u, 0)$. Since this is a submodule of $\mathbb{Z} \times \{0\}$ (which is the same as \mathbb{Z}), we can think of K' as being $m\mathbb{Z} \times \{0\}$ for some m so that it is the span of the single element $(m, 0)$.

The cosets of K' fill out all of K and partition it. We can take a \mathbb{Z} -module quotient K/K' . Notice that the only way for (a, b) and (c, d) to be in the same coset K' is if they are shift of K' apart. That is, $(a, b) = (c, d) + (u, 0)$ which implies that $b = d$. Conversely if $b = d$, then $(a, b) = (c, d) + \underbrace{(a - c, 0)}_{\in K'}$. Each second component w that occurs in the elements $(u, w) \in K$ uniquely determines a coset of K' in K . So let's look at the \mathbb{Z} -module W which consists of these second components. Let $W = \langle w_1, w_2, \dots \rangle \subset \mathbb{Z}$. We know that $W = r\mathbb{Z}$ for some r . This means that there exists an element of the form $(u_r, r) \in K$ whose span includes an element of every coset of K' .

To get all the elements of K , we simply need to add an element of K' , which we saw is the span of $(m, 0)$, to an element in the span of (u_r, r) . This shows that K is finitely generated—in fact, generated by two elements.

For $n > 2$, we can use an induction mechanism whose inductive step mirrors the case $n = 2$ to show that indeed K will be finitely generated—i.e. the span of finitely many elements of \mathbb{Z}^n . So, all finitely generated \mathbb{Z} -modules isomorphically are like a quotient of \mathbb{Z}^n with a submodule spanned by finitely many elements of \mathbb{Z}^n . We can take these elements and write them as columns in a matrix, do some row and column operations until we have a diagonal matrix (in the first n columns). The effect? Our \mathbb{Z} -module looks like $\mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_n\mathbb{Z}$ where some of the a_i 's could be 0. Where they are 0, we simply get $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$. \square

Corollary 9.1.12

Suppose that A is a *finite* \mathbb{Z} -module of size n . Then: ***scalar multiplication by n on A is the same as scalar multiplication by 0.***

Proof. Isomorphically think about the finite \mathbb{Z} -module as $\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_r\mathbb{Z}$ where $m = 0$ in the theorem since the group is finite. Then the size of A is $n = a_1 \cdot a_2 \cdots a_r$. If $x + a_k\mathbb{Z}$ is the coset chunk in the k th component, the scalar multiplication $n \cdot (x + a_k\mathbb{Z})$ is defined to be the coset chunk $nx + a_k\mathbb{Z}$. Since $n \in a_k\mathbb{Z}$, this is simply the zero coset chunk in the quotient. \square

9.1.5 Multiplicative Groups and Exponents

Our nice \mathbb{Z} -module structure does not just work for additive groups. All groups with a commutative group operation are \mathbb{Z} -modules. So if we turn to multiplication, we have just secured a way to know how exponents behave. We explain!

Multiplicative Groups R^\times

Suppose that R is a \mathbb{Z} -module which is also a ring. Let R^\times be all elements of R which admit a multiplicative inverse. Then R^\times is a commutative multiplicative group. *It is a \mathbb{Z} -module where we have replaced addition with multiplication!*

Theorem 9.1.13

Let n be the size of R^\times for the finite \mathbb{Z} -module ring R . Then if $a \in R$,

$$a^n = a^0 = \text{"1"} \text{ (multiplicative identity)}$$

Proof. This follows directly from the last corollary above since exponents are like scalar multiplication if the \mathbb{Z} -module is with respect to multiplication. \square

So now we just need a way to think about the sizes of multiplicative groups.

Theorem 9.1.14

Think of $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ as a ring with component-wise multiplication. Then inverses also work component-wise. In particular,

$$(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})^\times = (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times.$$

Theorem 9.1.15

Given two groups A and B , where $n = |A|$, the size of A , and $m = |B|$, the size of B , then nm is the size of $A \times B$.

Size of a Set Notation

Recall that the size of a set A is denoted $|A|$.

These theorems and the Chinese Remainder Theorem combined give us:

Corollary 9.1.16

Suppose that the prime factorization of m is

$$m = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$$

Then, $(\mathbb{Z}/m\mathbb{Z})^\times$ is isomorphic as a \mathbb{Z} -module to $(\mathbb{Z}/p_1^{r_1})^\times \times \cdots \times (\mathbb{Z}/p_k^{r_k})^\times$. In particular,

$$|(\mathbb{Z}/m\mathbb{Z})^\times| = |(\mathbb{Z}/p_1^{r_1})^\times| \cdots |(\mathbb{Z}/p_k^{r_k})^\times|$$

All we need now is a good way to determine $|(\mathbb{Z}/p^r\mathbb{Z})^\times|$ for a prime power p^r .

Let's go back to the bar notation in our discussion. Remember that $\bar{3}$ in $\mathbb{Z}/5\mathbb{Z}$ means $3 + 5\mathbb{Z}$.

Theorem 9.1.17

An element $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$.

Proof. The fact that $\gcd(a, m) = 1$ is equivalent by the Euclidean algorithm to saying that $ak + mt = 1$ for some integers k and t . This means that $ak = 1 + mt \in 1 + m\mathbb{Z} = \bar{1}$. This means that $\bar{a} \cdot \bar{k} = \bar{1}$ so that \bar{k} is an inverse. \square

So determining $|(\mathbb{Z}/m\mathbb{Z})^\times|$ is the same as determining how many integers $1, \dots, m$ have a greatest common factor of 1 with m .

Theorem 9.1.18

$$|(\mathbb{Z}/p^r\mathbb{Z})^\times| = (p-1)p^{r-1} = p^r - p^{r-1}$$

Proof. We are just computing how many of the first p^r counting numbers are not multiples of p . Just subtract p^{r-1} which is $\frac{1}{p}$ of all these numbers. \square

Euler-phi Function

We define:

$$\phi(m) = |\mathbb{Z}/m\mathbb{Z}^\times|$$

In particular, then:

$$\phi(p^r) = p^r - p^{r-1}$$

Theorem 9.1.19

Suppose that $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$. Then, $\overline{a}^k = \overline{a}^k \pmod{\phi(m)}$. That is, the exponents live in mod $\phi(m)$ while the bases live mod m .

Example 20. Let's compute $\overline{7}^{12}$ working in $\mathbb{Z}/11\mathbb{Z}$. First of all $\phi(11) = 11 - 1 = 10$. Hence the exponents live mod 10. So this exponent of 12 can be replaced by anything in $12 + 10\mathbb{Z}$. So what about 2? Really, we are computing $\overline{7}^2 = \overline{49} = \overline{5}$ since 49 is 5 more than a multiple of 11.

Theorem 9.1.20

The above discussions show that $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ if m and n do not share any common factors (i.e. the Chinese Remainder Theorem is at work.)

Example 21. Consider $\underline{2}^{49}$ in $\mathbb{Z}/144\mathbb{Z}$. We compute

$$\phi(144) = \phi(3^2 \cdot 2^4) = \phi(3^2) \cdot \phi(2^4) = (3^2 - 3) \cdot (2^4 - 2^3) = 6 \cdot 8 = 48$$

So our exponents live mod 48. This tells us that our exponent of 49 can be replaced by 1 so that:

$$\underline{2}^{49} = \underline{2}^1 = \underline{2}.$$

Multiplicative Inverses Notation

We let \underline{a}^{-1} signify a multiplicative inverse. This is the element such that $\underline{a} \cdot \underline{a}^{-1} = \underline{1}$.

Computing Multiplicative Inverses

Suppose that we would like to compute \underline{a}^{-1} in $\mathbb{Z}/m\mathbb{Z}$.

- Method 1: Use the Euclidean Algorithm. We find $ak + tm = 1$. Then $\underline{a}^{-1} = \underline{k}$.
- Method 2: Use Powers. We Compute $\phi(m)$. Then we know that the exponent -1 is the same as the exponent $m - 1$. Therefore, we compute \underline{a}^{m-1} .

Example 22. When we worked the Euclidean algorithm above for 91 and 11, we found that

$$4 \cdot 91 - 33 \cdot 11 = 364 - 363 = 1$$

Therefore, in $\mathbb{Z}/91\mathbb{Z}$, $\underline{11}^{-1} = \underline{-33}$.

Example 23. Let's compute $\underline{11}^{-1}$ in $\mathbb{Z}/91\mathbb{Z}$ using the power method. We know that $91 = 7 \cdot 13$. Therefore,

$$\phi(7 \cdot 13) = \phi(7) \cdot \phi(13) = (7 - 1) \cdot (13 - 1) = 6 \cdot 12 = 72$$

So, exponents live mod 72. Hence, an exponent of -1 is like 71. We raise $\underline{11}^{71}$. We write 71 as a sum of powers of 2.

$$71 = \underbrace{2^6}_{64} + \underbrace{2^2}_{4} + \underbrace{2^1}_{2} + \underbrace{2^0}_{1}$$

So we just keep squaring and reducing the representative. Remember that the bases (under the $\overline{}$) live mod 91.

$$\begin{aligned}\overline{11}^2 &= \overline{121} = \overline{30} \\ \overline{11}^4 &= \overline{30}^2 = \overline{900} = \overline{910 - 10} = \underbrace{\overline{910}}_0 + \overline{-10} = \overline{-10} \\ \overline{11}^8 &= \overline{-10}^2 = \overline{100} = \overline{9} \\ \overline{11}^{16} &= \overline{9}^2 = \overline{81} = \overline{-10} \\ \overline{11}^{32} &= \overline{-10}^2 = \overline{100} = \overline{9} \\ \overline{11}^{64} &= \overline{9}^2 = \overline{81} = \overline{-10}\end{aligned}$$

So,

$$\overline{11}^{71} = \overline{11}^{64} \cdot \overline{11}^4 \cdot \overline{11}^2 \cdot \overline{11}^1 = \underbrace{\overline{-10} \cdot \overline{-10}}_{= 100 = 9} \cdot \underbrace{\overline{30} \cdot \overline{11}}_{= 330} = \overline{-306} = \overline{-33}$$

Example 24. Extra example. We give an example of a \mathbb{Z} -module where the natural component-wise multiplication does not make it into a ring. Let R be all finite linear combinations of elements from an infinite set of standard basis vectors: $\{e_1, e_2, \dots\}$. Elements of R then are infinite tuples with only finitely components being nonzero. Think about the multiplicative identity. *Do you see the problem?* The multiplicative identity should be an infinite tuple with a 1 in each component—that is infinitely many nonzero components. So R then has no multiplicative identity.

Yet we can still get around this problem. We just have to define our multiplication differently. We let our multiplication shift further into the sequence of components which are indexed by \mathbb{N} . Multiplication does not stay in one component necessarily—but it can change “grades” to make what we call a “graded ring.”

We have just described a polynomial ring in disguise. We label e_{j-1} as x^j and establish the rule that multiplication by x^j shifts us j entries deeper into the sequence. This is like saying that $x^j \cdot x^m = x^{m+j}$. The identity element is simply $e_1 = x^{1-1} = x^0 = 1$ itself.

Key Concepts from this Section

- **\mathbb{Z} -module:** (page 1033) A \mathbb{Z} -module is the same thing as a vector space *except* the scalars come from \mathbb{Z} . Some common examples are
 - \mathbb{Z} the integers themselves.
 - $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ which consists of pairs of integers (x, y) like $(2, 7)$ or $(-1543, 78)$.
 - $\mathbb{Z}^3 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ which consists of triples of integers (x, y, z) like $(5, 3, 2)$ or $(99, -375, -100)$.
- **free \mathbb{Z} -module (finitely generated):** (page 1033) We will call a (finitely generated) \mathbb{Z} -module that can

be described (at least isomorphically) as \mathbb{Z}^m for some m a free (finitely generated) \mathbb{Z} -module. We say “finitely generated” to mean that the module is the \mathbb{Z} -span of finitely many elements. We will not call the elements of a \mathbb{Z} -module vectors—just elements.

- **submodule:** (page 1033) A submodule is to a module what a subspace is to a vector space.
- **\mathbb{Z} -rank of a \mathbb{Z} -module:** (page 1033) The \mathbb{Z} -rank of a module is the size of the smallest set of elements whose \mathbb{Z} -span is the whole module. It is like dimension—but we give it a different name because *rank alone cannot determine if a submodule is equal to the module—but dimension in a vector space would be enough!*
- **generators:** (page 1034) We say that that $(3, 1)$ and $(1, 2)$ generate A over \mathbb{Z} if A is the \mathbb{Z} -span of $(3, 1)$ and $(1, 2)$.
- **fundamental parallelogram:** (page 1034) We have represented a fundamental parallelogram that describes the submodule A in the illustration above.
- **\mathbb{Z} -module homomorphism (map):** (page 1035) An additive function that is scalable with respect to scalars in \mathbb{Z} is not called a linear transformation—that is reserved when we are dealing with vector spaces and scalars from a field. Here in this case, we say that we are dealing with a \mathbb{Z} -module map—yet most commonly a \mathbb{Z} -module homomorphism.

\mathbb{Z} -module homomorphisms $\mathbb{Z}^m \rightarrow \mathbb{Z}^n$ are represented by matrices just like linear transformations $\mathbb{R}^m \rightarrow \mathbb{R}^n$ are. The main difference is that the matrix entries of the \mathbb{Z} -module homomorphism *must* be integers.

- **\mathbb{Z} -module isomorphism:** (page 1036) A \mathbb{Z} -module isomorphism is a \mathbb{Z} -module homomorphism which has an inverse function which is also a \mathbb{Z} -module homomorphism.
- **invertible integers:** (page 1036) Multiplication by an integer is a \mathbb{Z} -module homomorphism. But it is not an isomorphism unless the inverse which is multiplication by the multiplicative inverse of the integer is also multiplication by an integer. The only integers whose multiplicative inverses are again integers are:

$$\begin{array}{cc} -1 & 1 \end{array}$$

- **\mathbb{Z} -basis:** (page 1036) A \mathbb{Z} -basis for a \mathbb{Z} -module K is a minimal collection of elements whose \mathbb{Z} -span is all of K . There is no collection that spans the whole space with a fewer number of elements in it.
- **\mathbb{Z} row and column operations:** (page 1036) Let a matrix M represent a \mathbb{Z} -module homomorphism. A row or column operation turned into a column interpretation matrix represents a \mathbb{Z} -module isomorphism *as long as rescaling only happens by invertible integers*.
- **theorem 9.1.1 :** (page 1037) A \mathbb{Z} -module isomorphism $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ bijectively sends the shifts of a submodule A to the shifts of the submodule $f(A)$.

- **theorem 9.1.2 :** (page 1037) Let A be the \mathbb{Z} -span of $u, v \in \mathbb{Z}^2$. Make a matrix with u and v as columns: $M = \begin{pmatrix} u & v \end{pmatrix}$. Then, let B be the \mathbb{Z} -span of the the columns of $R \cdot M \cdot C$ where R represents a row operations matrix and C represents a column operations matrix where the only rescalings if any are by invertible integers. Then the shifts of A are in bijective correspondence with the shifts of B .
- **cosets:** (page 1038) These shifts are called cosets of the submodule A in \mathbb{Z}^2
- **corollary 9.1.3 :** (page 1039) The absolute value of the determinant of M counts the number of cosets of A in \mathbb{Z}^2 if A is a \mathbb{Z} -rank 2 submodule of \mathbb{Z}^2 .
- **quotient module:** (page 1039) We define a \mathbb{Z} -module \mathbb{Z}^2/A . Call it the *quotient module* of \mathbb{Z}^2 with A . The elements in this \mathbb{Z} -module are the cosets of A in \mathbb{Z}^2 . Each element is a shift of a submodule. This is exactly how we thought about quotient vector spaces. The cosets of \mathbb{Z}^2/A can be labeled or determined from a set of representatives from each shift in a fundamental parallelogram describing A .
- **cosets, addition, and scalar multiplication:** (page 1040) Each coset of A in \mathbb{Z}^2 can be represented as:

$$(\text{point}) + A$$

where (point) is any point in the coset! It is like we have moved the origin to then (point) and then graphed the points of A from this *new origin*. Any point in the coset gives the same picture. Then, to add two cosets:

$$\left((\text{point } 1) + A \right) + \left((\text{point } 2) + A \right) = ((\text{point } 1) + (\text{point } 2)) + A$$

To rescale:

$$m \cdot \left((\text{point } 1) + A \right) = m \cdot (\text{point}) + A$$

- **bar notation for quotients:** (page 1041) In our example of $\mathbb{Z}/5\mathbb{Z}$, let $a \in \mathbb{Z}$. Then, \bar{a} is the coset of $5\mathbb{Z}$ that a is an element of. In particular, $a \in a + 5\mathbb{Z}$.
- **theorem 9.1.4 :** (page 1044) Quotients of \mathbb{Z} -modules are \mathbb{Z} -modules with a well-defined addition among the cosets.
- **theorem 9.1.5 :** (page 1044) \mathbb{Z} -modules are simply groups where the group operation is commutative. We have been focusing on the group operation of addition so far.
- **lemma 9.1.6 :** (page 1044) If $\gcd(a, b) = 1$, then there exist integers k and t such that $ka + tb = 1$. In other words, 1 is in the \mathbb{Z} -span of a and b . We could even say:

$$\langle a, b \rangle_{\mathbb{Z}} = \langle \gcd(a, b) \rangle_{\mathbb{Z}} \quad a, b \in \mathbb{Z}$$

- **theorem 9.1.7 chinese remainder theorem (\mathbb{Z} -module version):** (page 1045) Given two integers a and b whose greatest common factor (divisor) is 1, there exists a \mathbb{Z} -module isomorphism:

$$\mathbb{Z}/ab\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

- **multiplication for a ring:** (page 1048) In many \mathbb{Z} -modules there is a natural multiplication structure that arises very naturally. In fact in $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ it is perfectly natural just to make this multiplication component-wise so $\left(\frac{1}{2}, \frac{1}{3}\right) \cdot \left(\frac{1}{4}, \frac{1}{5}\right) = \left(\frac{1}{2 \cdot 4}, \frac{1}{3 \cdot 5}\right)$. This multiplication structure, as long as there is a multiplicative identity element can make a \mathbb{Z} -module into a ring. A ring is an additive group that also has a well-defined (commutative and associative) multiplication structure with an multiplicative identity. Multiplicative inverses *are not required*.
- **ring homomorphism:** (page 1048) Given two rings R_1 and R_2 that are \mathbb{Z} -modules, a ring homomorphism $\tilde{f} : R_1 \rightarrow R_2$ between them is a \mathbb{Z} -module homomorphism which is multiplicative.
- **theorem 9.1.8 chinese remainder theorem (ring version):** (page 1048) Given two integers a and b whose greatest common factor (divisor) is 1, there exists a ring isomorphism:

$$\tilde{f} : \mathbb{Z}/ab\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

Let k and t be integers such that $ka + tb = 1$.

- **corollary 9.1.9 :** (page 1050) Given two integers a and b whose greatest common factor (divisor) is 1, then the ring homomorphisms \tilde{f} and \tilde{f}^{-1} described in the above theorem are induced by the following matrix functions (in a column interpretation) $\mathbb{Z}^2 \rightarrow \mathbb{Z}^2$:

$$f : \begin{pmatrix} ka & 1 \\ -tb & 1 \end{pmatrix} \quad f^{-1} : \begin{pmatrix} 1 & -1 \\ tb & ka \end{pmatrix}$$

Let k and t be integers such that $ka + tb = 1$.

- **coset equations, systems of congruences:** (page 1050) Coset equations or systems of congruences for cosets of the kind $r + m\mathbb{Z}$ are systems like we have just discussed in the reading:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

This means that we are trying to find x so that $x \in (2 + 3\mathbb{Z}) \cap (3 + 5\mathbb{Z})$

- **corollary 9.1.10 :** (page 1051) Suppose that $\gcd(a, b) = 1$. The map $\tilde{f}^{-1} : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \rightarrow \mathbb{Z}/ab\mathbb{Z}$ is

given as the column interpretation map of the matrix

$$\tilde{f}^{-1} : \begin{pmatrix} tb & ka \end{pmatrix}$$

where $ka + tb = 1$. This map solves a system of equations.

- **solving a system of congruences:** (page 1052) Suppose that we would like to solve a system of coset equations:

$$\begin{aligned} x &\equiv p_1 \pmod{a} \\ x &\equiv p_2 \pmod{b} \end{aligned}$$

We find t and k so that $ka + tb = 1$. Then, all solutions are given by:

$$\begin{pmatrix} tb & ka \end{pmatrix} \cdot \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} + ab\mathbb{Z}$$

- **scalars to make 1:** (page 1054) Suppose that $\gcd(a, b) = 1$ and that $a > b$. Let q_0, q_1, \dots, q_r be the quotients in the Euclidean algorithm through to the last nonzero remainder. Suppose that $\begin{pmatrix} k & t \end{pmatrix}$ is the second row of the matrix product:

$$\begin{pmatrix} w & z \\ k & t \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & q_r \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & q_0 \end{pmatrix}$$

Then $ak + bt = 1$.

- **variations to finding scalars:** (page 1056) In our process for finding scalars k and t such that $ak + tb = 1$, there are a couple of variations. If $\gcd(a, b) \neq 1$, then the same process finds k and t such that

$$ak + tb = \gcd(a, b)$$

If instead one wishes to use a negative remainder in a step, the matrix at that step is the same except with the second column having the opposite sign:

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

In the end,

$$ak + tb = (\text{last nonzero remainder which could be } (\pm))$$

- **in and out principles:** (page 1057) When working with the bar notation in $\mathbb{Z}/m\mathbb{Z}$, we have the following:

$$\begin{aligned} - \quad \overline{a+b} &= \overline{a} + \overline{b} \\ - \quad \overline{a \cdot b} &= \overline{a} \cdot \overline{b} \\ - \quad \overline{a^m} &= \overline{a^m} \end{aligned}$$

- **simpler representative principle:** (page 1057) We can always write $\overline{a} = \overline{b}$ if a and b are in the same coset. It is nice if we can choose a small, nice representative.
- **simpler at every step:** (page 1058) Use the simpler representative principle at every step in a long calculation to avoid big numbers just like in the last example.
- **theorem 9.1.11 classification of finitely generated \mathbb{Z} -modules:** (page 1058) All finitely generated \mathbb{Z} -modules isomorphically look like

$$\mathbb{Z}^m \times \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_r\mathbb{Z}$$

for $m, r, a_1, \dots, a_r \in \mathbb{N}$.

- **corollary 9.1.12 :** (page 1059) Suppose that A is a *finite* \mathbb{Z} -module of size n . Then: **scalar multiplication by n on A is the same as scalar multiplication by 0.**
- **multiplicative groups R^\times :** (page 1060) Suppose that R is a \mathbb{Z} -module which is also a ring. Let R^\times be all elements of R which admit a multiplicative inverse. Then R^\times is a commutative multiplicative group. *It is a \mathbb{Z} -module where we have replaced addition with multiplication!*
- **theorem 9.1.13 :** (page 1060) Let n be the size of R^\times for the finite \mathbb{Z} -module ring R . Then if $a \in R$,

$$a^n = a^0 = \text{"1"} \text{ (multiplicative identity)}$$

- **theorem 9.1.14 :** (page 1060) Think of $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ as a ring with component-wise multiplication. Then inverses also work component-wise. In particular,

$$(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})^\times = (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times.$$

- **theorem 9.1.15 :** (page 1061) Given two groups A and B , where $n = |A|$, the size of A , and $m = |B|$, the size of B , then nm is the size of $A \times B$.
- **size of a set notation:** (page 1061) Recall that the size of a set A is denoted $|A|$.
- **corollary 9.1.16 :** (page 1061) Suppose that the prime factorization of m is

$$m = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$$

Then, $(\mathbb{Z}/m\mathbb{Z})^\times$ is isomorphic as a \mathbb{Z} -module to $(\mathbb{Z}/p_1^{r_1})^\times \times \cdots \times (\mathbb{Z}/p_k^{r_k})^\times$. In particular,

$$|(\mathbb{Z}/m\mathbb{Z})^\times| = |(\mathbb{Z}/p_1^{r_1})^\times| \cdots |(\mathbb{Z}/p_k^{r_k})^\times|$$

- **theorem 9.1.17 :** (page 1061) An element $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$.
- **theorem 9.1.18 :** (page 1062)

$$|(\mathbb{Z}/p^r\mathbb{Z})^\times| = (p - 1)p^{r-1} = p^r - p^{r-1}$$

- **euler-phi function:** (page 1062) We define:

$$\phi(m) = |\mathbb{Z}/m\mathbb{Z}^\times|$$

In particular, then:

$$\phi(p^r) = p^r - p^{r-1}$$

- **theorem 9.1.19 :** (page 1062) Suppose that $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$. Then, $\overline{a}^k = \overline{a}^k \pmod{\phi(m)}$. That is, the exponents live in mod $\phi(m)$ while the bases live mod m .
- **theorem 9.1.20 :** (page 1062) The above discussions show that $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ if m and n do not share any common factors (i.e. the Chinese Remainder Theorem is at work.)
- **multiplicative inverses notation:** (page 1063) We let \overline{a}^{-1} signify a multiplicative inverse. This is the element such that $\overline{a} \cdot \overline{a}^{-1} = \overline{1}$.
- **computing multiplicative inverses:** (page 1063) Suppose that we would like to compute \overline{a}^{-1} in $\mathbb{Z}/m\mathbb{Z}$.
 - Method 1: Use the Euclidean Algorithm. We find $ak + tm = 1$. Then $\overline{a}^{-1} = \overline{k}$.
 - Method 2: Use Powers. We Compute $\phi(m)$. Then we know that the exponent -1 is the same as the exponent $m - 1$. Therefore, we compute \overline{a}^{m-1} .

9.1.6 Exercises

Solving Systems of Congruences

Solve the following systems of congruences using the techniques of this section.

$$\begin{aligned} \text{1. } x &\equiv 1 \pmod{5} \\ &x \equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} \text{2. } x &\equiv 8 \pmod{11} \\ &x \equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} \text{3. } x &\equiv 2 \pmod{11} \\ &x \equiv 5 \pmod{7} \end{aligned}$$

$$\begin{aligned} \text{4. } x &\equiv 3 \pmod{11} \\ &x \equiv 5 \pmod{13} \end{aligned}$$

$$\begin{aligned} \text{5. } x &\equiv 10 \pmod{11} \\ &x \equiv 4 \pmod{5} \end{aligned}$$

$$\begin{aligned} \text{6. } x &\equiv 12 \pmod{13} \\ &x \equiv 3 \pmod{5} \end{aligned}$$

$$\begin{aligned} \text{7. } x &\equiv 11 \pmod{13} \\ &x \equiv 2 \pmod{5} \end{aligned}$$

$$\begin{aligned} \text{8. } x &\equiv 2 \pmod{5} \\ &x \equiv 2 \pmod{7} \end{aligned}$$

$$\begin{aligned} \text{9. } x &\equiv 9 \pmod{11} \\ &x \equiv 2 \pmod{7} \end{aligned}$$

$$\begin{aligned} \text{10. } x &\equiv 9 \pmod{11} \\ &x \equiv 11 \pmod{13} \end{aligned}$$

$$\begin{aligned} \text{11. } x &\equiv 5 \pmod{11} \\ &x \equiv 3 \pmod{5} \end{aligned}$$

$$\begin{aligned} \text{12. } x &\equiv 9 \pmod{11} \\ &x \equiv 4 \pmod{7} \end{aligned}$$

$$\begin{aligned} \text{13. } x &\equiv 7 \pmod{11} \\ &x \equiv 2 \pmod{5} \\ &x \equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} &x \equiv 9 \pmod{11} \\ \text{14. } x &\equiv 2 \pmod{5} \\ &x \equiv 5 \pmod{7} \end{aligned}$$

$$\begin{aligned} \text{15. } x &\equiv 2 \pmod{11} \\ &x \equiv 4 \pmod{5} \\ &x \equiv 4 \pmod{7} \end{aligned}$$

$$\begin{aligned} &x \equiv 10 \pmod{11} \\ \text{16. } x &\equiv 2 \pmod{5} \\ &x \equiv 3 \pmod{7} \end{aligned}$$

$$x \equiv 5 \pmod{13}$$

17. $x \equiv 1 \pmod{5}$

$$x \equiv 5 \pmod{7}$$

$$x \equiv 8 \pmod{11}$$

18. $x \equiv 9 \pmod{13}$

$$x \equiv 1 \pmod{7}$$

$$x \equiv 2 \pmod{13}$$

19. $x \equiv 5 \pmod{11}$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 8 \pmod{11}$$

20. $x \equiv 2 \pmod{5}$

$$x \equiv 1 \pmod{7}$$

$$x \equiv 9 \pmod{11}$$

21. $x \equiv 2 \pmod{5}$

$$x \equiv 1 \pmod{7}$$

$$x \equiv 9 \pmod{11}$$

22. $x \equiv 3 \pmod{5}$

$$x \equiv 4 \pmod{7}$$

$$x \equiv 3 \pmod{13}$$

23. $x \equiv 2 \pmod{5}$

$$x \equiv 1 \pmod{7}$$

$$x \equiv 5 \pmod{11}$$

24. $x \equiv 1 \pmod{5}$

$$x \equiv 6 \pmod{7}$$

Raising a coset to a power in $\mathbb{Z}/N\mathbb{Z}$

Suppose that $\underline{\quad}$ refers to $\mathbb{Z}/N\mathbb{Z}$. Find $\phi(N)$ and use it to compute the given power as a simple representative mod N .

25. $N = 45, \underline{2^{25}}$

26. $N = 75, \underline{7^{81}}$

27. $N = 135, \underline{2^{145}}$

28. $N = 675, \underline{7^{361}}$

29. $N = 100, \underline{3^{82}}$

30. $N = 15, \underline{4^{18}}$

31. $N = 225, \underline{2^{242}}$

32. $N = 20, \underline{3^{16}}$

33. $N = 40, \underline{3^{33}}$

34. $N = 200, \underline{3^{161}}$

35. $N = 10, \underline{3^6}$

36. $N = 50, \underline{3^{41}}$

9.1.7 Solutions

1. $31 \pmod{35}$

2. $52 \pmod{77}$

3. $68 \pmod{77}$

4. $135 \pmod{143}$

5. $54 \pmod{55}$

6. $38 \pmod{65}$

7. $37 \pmod{65}$

8. $2 \pmod{35}$

9. $9 \pmod{77}$

10. $141 \pmod{143}$

11. $38 \pmod{55}$

12. $53 \pmod{77}$

13. $227 \pmod{385}$

14. $152 \pmod{385}$

15. $354 \pmod{385}$

16. $87 \pmod{385}$

17. $96 \pmod{455}$

18. $932 \pmod{1001}$

19. $522 \pmod{715}$

20. $162 \pmod{385}$

21. $372 \pmod{385}$

22. $53 \pmod{385}$

23. $302 \pmod{455}$

24. $181 \pmod{385}$

25. $\phi(N) = 24, \quad \boxed{2}$

26. $\phi(N) = 40, \quad \boxed{7}$

$$\text{27. } \phi(N) = 72, \quad \boxed{2}$$

$$\text{28. } \phi(N) = 360, \quad \boxed{7}$$

$$\text{29. } \phi(N) = 40, \quad \boxed{9}$$

$$\text{30. } \phi(N) = 8, \quad \boxed{1}$$

$$\text{31. } \phi(N) = 120, \quad \boxed{4}$$

$$\text{32. } \phi(N) = 8, \quad \boxed{1}$$

$$\text{33. } \phi(N) = 16, \quad \boxed{3}$$

$$\text{34. } \phi(N) = 80, \quad \boxed{3}$$

$$\text{35. } \phi(N) = 4, \quad \boxed{9}$$

$$\text{36. } \phi(N) = 20, \quad \boxed{3}$$

Field Extensions and Galois

9.2

Groups

9.2.1 Algebraic Field Extensions	1077
9.2.2 Proving the Fundamental Theorem of Algebra	1092
9.2.3 Examples: Matrix Diagonalization to Compute Galois Groups	1094
9.2.4 Cyclotomic Polynomials	1105
9.2.5 A Linear Transformation that Counts what is Primitive	1108
9.2.6 Exercises	1116
9.2.7 Solutions	1117

Questions to Guide Your Study:

- *What are fields, rings, and field extensions?*
- *How can we isomorphically think of an algebraic field extension as a polynomial quotient ring?*
- *What are algebraic numbers? What are algebraic integers and how do they form a subring of a field extension?*
- *What is a primitive element of a field extension and how can it help us determine all ring homomorphisms from the field, that keep the original field (before the extension) fixed?*
- *What is a normal field extension and how do we obtain a group of symmetries in such an extension?*
- *What is the Fundamental Theorem of Galois Theory?*
- *How can we use these ideas (along with some group theory) to help prove the Fundamental Theorem of Algebra?*
- *How can we use matrix diagonalization to actually compute the group of symmetries of a normal field extension?*
- *What are cyclotomic polynomials and what kinds of extensions do they describe?*
- *How can we use a matrix to count primitive roots?*

We have talked about fields and we have talked about vector spaces. Yet there is something very peculiar in all of this. If a field F_1 is a subfield of another field F_2 , then F_2 is actually a vector space with scalars in F_1 .

Wait! Fields are vector spaces over each other?

This allows linear algebra to play a key role in the study fields themselves.

One can lift factoring numbers from a ring like \mathbb{Z} to a field like \mathbb{Q} and then to a new field and subring. The effect is that linear algebra techniques can be used in the study of integers and knowing how to factor them quickly!

Fields can also have nice symmetries that keep subfields fixed. There are many applications of such symmetries in the study of polynomial equations, number theory, and elsewhere.

A main goal of this section is to develop enough ideas to give code examples of how our matrix techniques of diagonalization can be used to determine exactly which permutations of roots define the algebraic symmetries we are discussing.

9.2.1 Algebraic Field Extensions

The notions of field and ring were defined earlier in the book. They are given here again briefly as a reminder.

Field

A field is an additive commutative group with respect to $+$. There is a multiplication operation defined such that with 0 omitted, we have a multiplicative group. The multiplication is commutative and distributes over addition.

Multiplicative Inverse

The multiplicative inverse of an element a is the element b such that $a \cdot b = b \cdot a$ is the multiplicative identity 1.

Ring

A ring is like a field except elements are not required to have multiplicative inverses in the ring.

Example 1. The set \mathbb{Q} is a field—it has a nice addition and multiplication and every nonzero element has a multiplicative inverse. But \mathbb{Z} is not a field. It is a ring.

Subfield

Given two fields F_1 and F_2 , if $F_1 \subset F_2$, then we say that F_1 is a *subfield* of F_2 .

Field Extension

Given two fields F_1 and F_2 , if $F_1 \subset F_2$, then we say that F_2 is a *field extension* of F_1 .

Example 2. The field \mathbb{C} is a field extension of \mathbb{R} and of \mathbb{Q} . The field \mathbb{R} is an extension of \mathbb{Q} .

Finiteness Convention

Unless otherwise indicated, we assume that all field extensions (except \mathbb{C}) in what follows are finite dimensional \mathbb{Q} -vector spaces.

Let $\mathbb{Q}[x]$ denote the ring of all polynomials in x with coefficients in \mathbb{Q} . The Euclidean algorithm works well in the ring $\mathbb{Q}[x]$ so that we can find greatest common factors. We will see it in action. First, let $\mathcal{C} = \{p_1(x), p_2(x), \dots, p_r(x)\}$ be a collection of polynomials in $\mathbb{Q}[x]$. The polynomial span of \mathcal{C} is all linear combinations:

$$a_1(x)p_1(x) + a_2(x)p_2(x) + \cdots + a_r(x)p_r(x)$$

for polynomial scalars $a_1(x), a_2(x), \dots, a_r(x)$. This polynomial span is a $\mathbb{Q}[x]$ -submodule of $\mathbb{Q}[x]$ itself!

This $\mathbb{Q}[x]$ -submodule of $\mathbb{Q}[x]$ has a simple form. It is the polynomial span of just one element:

$$\gcd(p_1(x), p_2(x), \dots, p_r(x))$$

Let's use this idea as we describe field extensions of \mathbb{Q} .

$\mathbb{Q}(\alpha)$

The field $\mathbb{Q}(\alpha)$ is the smallest field containing both \mathbb{Q} and α .

Intuitively, we can think of $\mathbb{Q}(\alpha)$ as just being all the ways of adding, multiplying and dividing with α and elements of \mathbb{Q} . But there is a very nice description if α is a root of a polynomial.

Simple Algebraic Field Extension

We call a field extension $\mathbb{Q}(\alpha)$ of \mathbb{Q} where α is the root of a polynomial in $\mathbb{Q}[x]$ a *simple algebraic field extension of \mathbb{Q}* . We can replace \mathbb{Q} with any field F letting α denote a root of a polynomial in $F[x]$. Then $F(\alpha)$ is a *simple algebraic field extension of F* .

Let α be a root of a polynomial $p(x)$. In fact, it is the root of a polynomial that is irreducible—so that it does not factor nontrivially. If we let x act as α , then $\mathbb{Q}(\alpha)$ can be thought of as a $\mathbb{Q}[x]$ module. In particular, we can make a $\mathbb{Q}[x]$ -module homomorphism:

$$\mathbb{Q}[x] \rightarrow \mathbb{Q}(\alpha)$$

where a polynomial $h(x)$ in $\mathbb{Q}[x]$ is simply sent to $h(\alpha)$ in $\mathbb{Q}(\alpha)$. Think about the kernel of this map: all polynomials $h(x)$ where $h(\alpha) = 0$. This kernel is a $\mathbb{Q}[x]$ -module, contains $p(x)$ and is not all of $\mathbb{Q}[x]$. In particular, it does not contain 1 since “1” never evaluates as 0. This kernel module is the span of the

greatest common factor of all elements in it. Since $p(x)$ is irreducible, the greatest common factor of any other polynomial with it is either $p(x)$ or 1. But we know it is not 1. Therefore, $p(x)$ is a factor of every polynomial in the kernel. The kernel is equal to the polynomial span of $p(x)$. We can label this polynomial span simply as $p(x)\mathbb{Q}[x]$

This tells us that the quotient $\mathbb{Q}[x]/p(x)\mathbb{Q}[x]$ indexes the range of the map $\mathbb{Q}[x] \rightarrow \mathbb{Q}(\alpha)$ since the nonzero fibers are shifts of the kernel. But, because $p(x)$ is irreducible, any polynomial not in the kernel does not share any common factors with it. Via the Euclidean algorithm, that polynomial should have a multiplicative inverse in $\mathbb{Q}[x]/p(x)\mathbb{Q}[x]$ just like we thought of multiplicative inverses in $\mathbb{Z}/m\mathbb{Z}$. Hence, $\mathbb{Q}[x]/p(x)\mathbb{Q}[x]$ is not just a ring, but a field. Since $\mathbb{Q}(\alpha)$ is the smallest field containing \mathbb{Q} and α our map must be an isomorphism. The variable x is like α and for sure \mathbb{Q} is represented in this quotient.

Wow! We can represent a simple algebraic field extension $\mathbb{Q}(\alpha)$ isomorphically as a quotient of $\mathbb{Q}[x]$.

Theorem 9.2.1

Take an irreducible polynomial $p(x)$ in $\mathbb{Q}[x]$ that has α as a root. Then $\mathbb{Q}(\alpha)$ is isomorphic to the quotient $\mathbb{Q}[x]/p(x)\mathbb{Q}[x]$.

Monic Polynomial

Any polynomial whose leading coefficient is 1 is called a *monic polynomial*.

Minimal Polynomial

Rescale the irreducible polynomial $p(x)$ that has α as its root to be a monic polynomial. Then, this polynomial is called the minimal polynomial of α .

Theorem 9.2.2

The field $\mathbb{Q}(\alpha)$ is a \mathbb{Q} -vector space with dimension n where $n = \deg(p(x))$.

Proof. We will think of $\mathbb{Q}(\alpha)$ as $\mathbb{Q}[x]/p(x)\mathbb{Q}[x]$ since they are isomorphic. Remember when we let x represent a matrix action? It had a minimal polynomial. Using that minimal polynomial, we could represent any power x^m as a polynomial of degree less than its minimal polynomial via polynomial division. The same is true here since we think of $p(x)$ as being zero. Therefore, we can represent all cosets in the quotient $\mathbb{Q}[x]/p(x)\mathbb{Q}[x]$ by polynomials of degree up to but not including n . Notice that any nonzero polynomial $a(x) \in \mathbb{Q}[x]$ of degree

less than n cannot be equal to zero in this quotient by the minimality of $p(x)$. This implies that $1, x, x^2, \dots, x^{n-1}$ are linearly independent over \mathbb{Q} . Therefore, $\mathbb{Q}(\alpha)$, with the \mathbb{Q} -scalar action which it borrows from $\mathbb{Q}[x]$ is a \mathbb{Q} -vector space with dimension n . \square

Theorem 9.2.3

Using our notation, the set of elements $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ makes up a basis for the \mathbb{Q} -vector space $\mathbb{Q}(\alpha)$.

All elements in the field $\mathbb{Q}(\alpha)$ act on $\mathbb{Q}(\alpha)$ via multiplication since this is *both* a field and a vector space! They are \mathbb{Q} -linear transformations describable as matrices and as such have minimal polynomials associated with them which are the minimal polynomials of their associated matrix.

This shows that all elements of $\mathbb{Q}(\alpha)$ are algebraic numbers: they are roots of their own minimal polynomials (when multiplication by them is thought of as \mathbb{Q} -linear transformations $\mathbb{Q}(\alpha) \rightarrow \mathbb{Q}(\alpha)$).

Algebraic Number

An algebraic number over \mathbb{Q} is any root of any polynomial in $\mathbb{Q}[x]$. Generally, an algebraic number over a field F is any root of any polynomial in $F[x]$.

Theorem 9.2.4

All elements in $\mathbb{Q}(\alpha)$ where α is an algebraic number are algebraic numbers. The field \mathbb{Q} may be replaced with any field F so that we can say that all elements in $F(\alpha)$ where α is an algebraic number over F will also be algebraic numbers!

Minimal Polynomial of Element and Matrix

The minimal polynomial of an element in an algebraic number field and the minimal polynomial of the matrix which describes multiplication by that element as a vector space isomorphism are the same.

Some of these minimal polynomials are in $\mathbb{Z}[x]$. When they are in $\mathbb{Z}[x]$ they have a special name.

Algebraic Integers \mathcal{O}_K

Any element of an algebraic number field that admits a minimal polynomial in $\mathbb{Z}[x]$ is called an *algebraic integer*. We often use \mathcal{O}_K to denote the algebraic integers in $K = \mathbb{Q}(\alpha)$.

Algebraic integers in $K = \mathbb{Q}(\alpha)$ behave a lot like how \mathbb{Z} behaves in \mathbb{Q} . The use? Number theorists study how primes in \mathbb{Z} look in various \mathcal{O}_K to get a better feel for how they interact with each other in \mathbb{Z} . In particular, the \mathbb{Z} -submodule $p\mathbb{Z}$ for a prime number in \mathbb{Z} factors into products of “prime” \mathcal{O}_K -submodules of \mathcal{O}_K . That is, we lift prime factorizations of \mathbb{Z} into prime factorizations in \mathcal{O}_K . This heightened perspective teaches us a lot about the integers \mathbb{Z} and what we can do with them. Though we do not go into details in this text, the interested reader is invited to explore further.

The currently fastest known algorithm for factoring large numbers uses these ideas!

The General Number Field Sieve.

If we can find *any* polynomial in $\mathbb{Z}[x]$ that an algebraic number is a root of, it automatically forces that algebraic number to be an algebraic integer.

Lemma 9.2.5

If an element is a root of a polynomial in $\mathbb{Z}[x]$, then its minimal polynomial is also in $\mathbb{Z}[x]$.

Proof. Suppose that the an algebraic number w over \mathbb{Q} is a root of the *monic* polynomial $q(x) \in \mathbb{Z}[x]$ so that its leading coefficient is 1. This means that the minimal polynomial of w in $\mathbb{Q}[x]$ must be a factor of $q(x)$. Suppose that its minimal is $a(x)$. Then, $q(x) = a(x)b(x)$ is in $\mathbb{Z}[x]$ while $a(x)$ and $b(x)$ are in $\mathbb{Q}[x]$. Since $a(x)$ is monic and $q(x)$ is monic, we are forced to have $b(x)$ monic as well since the leading coefficients of $a(x)$ and $b(x)$ multiply to give the leading coefficient 1 of $q(x)$. We would like to show that $a(x)$ and $b(x)$ are both in $\mathbb{Z}[x]$. Choose $r_a \in \mathbb{Z}$ minimally so that $r_a a(x) \in \mathbb{Z}[x]$ and $r_b \in \mathbb{Z}$ minimally so that $r_b b(x) \in \mathbb{Z}[x]$. That is, r_a and r_b are chosen so that the gcd of the coefficients of $r_a a(x) \in \mathbb{Z}[x]$ is 1 and the gcd of the coefficients of $r_b b(x) \in \mathbb{Z}[x]$ is 1. Then, we have:

$$r_a r_b q(x) = (r_a a(x))(r_b b(x))$$

Let p be a prime factor of $r_a r_b$. Then reducing coefficients mod p we find that the equation becomes:

$$\overline{0} = \overline{(r_a a(x))} \cdot \overline{(r_b b(x))}$$

Reducing coefficients mod p means that we are working in the field $\mathbb{Z}/p\mathbb{Z}$ written as \mathbb{F}_p . The only way for two polynomials in $\mathbb{F}_p[x]$ to multiply to 0 (since the degrees of nonzero polynomials add in a product and this clearly is not happening) is for one of those polynomials to be zero. That is, $\overline{(r_a a(x))}$ or $\overline{(r_b b(x))}$ is $\overline{0}$. This means that p is a factor of every coefficient in one of these. But this contradicts the fact that the gcd of the coefficients of each is 1. Therefore, there can be no prime factors of $r_a r_b$ so that $r_a = \pm 1$ and $r_b = \pm 1$. Yet this means that $a(x) \in \mathbb{Z}[x]$ and $b(x) \in \mathbb{Z}[x]$. \square

Corollary 9.2.6

The only monic factors in $\mathbb{Q}[x]$ of a monic polynomial in $\mathbb{Z}[x]$ are again in $\mathbb{Z}[x]$.

Theorem 9.2.7

The set \mathcal{O}_K is a ring.

Proof. Let α and β be algebraic integers in a field extension K of \mathbb{Q} with minimal polynomials $p(x)$ of degree n and $q(y)$ of degree m respectively.

Take the 2-variable polynomial ring $\mathbb{Z}[x, y]$. Define $g : \mathbb{Z}[x, y] \rightarrow K$ by $x \mapsto \alpha$ and $y \mapsto \beta$. Such relabeling (just replacing symbols) is clearly additive and \mathbb{Z} -scalable. So g is a \mathbb{Z} -module homomorphism. In fact, replacing symbols preserves multiplication too so that g is a *ring homomorphism*.

Let W be the $\mathbb{Z}[x, y]$ span of $g(x)$ and $g(y)$. Since $g(p(x)) = p(\alpha) = g(q(x)) = q(\beta) = 0$, $W \subset \ker(g)$. This means that the cosets of W are contained completely in the cosets of the $\ker(g)$ in $\mathbb{Z}[x, y]$. A coset of W is sent to the same image as a coset of $\ker(g)$ which is a fiber of g . This means, g makes a \mathbb{Z} -module map from the set of cosets of W to K :

$$h : \mathbb{Z}[x, y]/W \rightarrow K$$

Because we quotient or “mod out” by $p(x)$, we can replace any power x^j by its remainder when we divide by $p(x)$. That being said, all powers x^j in $\mathbb{Z}[x, y]/W$ are in the span of $\{1, x, x^2, \dots, x^{n-1}\}$. Similarly, all powers of y^j are in the span of $\{1, y, y^2, \dots, y^{m-1}\}$. Since $\mathbb{Z}[x, y]$ is generated by $x^i y^j$ over \mathbb{Z} , then $\mathbb{Z}[x, y]/W$ is finitely generated over \mathbb{Z} . Also, multiplication by an integer cannot take something that is not in W into W —no integer behaves like scalar multiplication by 0 in the quotient $\mathbb{Z}[x, y]/W$. Hence, the \mathbb{Z} -module type of $\mathbb{Z}[x, y]/W$ is \mathbb{Z}^r for some r .

Notice that multiplication by $(x + y)$ sends W to W . Therefore, it sends a coset $a + W$ to $(x + y)a + W$. So it induces a \mathbb{Z} -module map $\mathbb{Z}[x, y]/W \rightarrow \mathbb{Z}[x, y]/W$ which can be thought of as a \mathbb{Z} -module map $\mathbb{Z}^r \rightarrow \mathbb{Z}^r$. This can be represented by a matrix which has a minimal (monic) polynomial $r(x) \in \mathbb{Z}[x]$.

In particular this means that multiplication by $r(x + y)$ acts like 0 on $\mathbb{Z}[x, y]/W$ so that $r(x + y) \cdot 1 \in W$. Note that since g is a ring homomorphism splitting across multiplication and addition:

$$g(r(x + y)) = r(g(x) + g(y)) = r(\alpha + \beta)$$

Also since $r(x + y) \in W$,

$$g(r(x + y)) = h(r(x + y) + W) = h(W) = 0$$

Hence,

$$r(\alpha + \beta) = 0.$$

Therefore, $\alpha + \beta$ is an algebraic integer. The argument is identical for showing that $\alpha \cdot \beta$ is an algebraic integer. Since -1 is a root of $x + 1$, -1 is an algebraic integer so that if $\beta = -1$, then $\alpha \cdot (-1) = -\alpha$ is also an algebraic integer. Also note that 1 (root of $x - 1$) is in \mathcal{O}_K .

Therefore, the set \mathcal{O}_K which is a subset of the field K is closed under addition, multiplication and taking additive inverses. *It is a ring!*

□

Algebraic Field Extension

A field K is called an algebraic field extension of a field F if it is the smallest field containing both F and a collection of algebraic numbers over F .

$\mathbb{Q}(\alpha, \beta)$

The field $\mathbb{Q}(\alpha, \beta)$ is the algebraic field extension of \mathbb{Q} formed by adjoining α and β .

We will show that $\mathbb{Q}(\alpha, \beta)$ is actually a simple algebraic field extension $\mathbb{Q}(\gamma)$ for some γ . Such a γ is called a primitive element of the extension.

Primitive Element

Given an algebraic field extension K of F , an element $\gamma \in K$ is called a primitive element of the extension if $K = F(\gamma)$.

But first, we will use the following fact which we do not prove here:

Fundamental Theorem of Algebra

Every degree n polynomial in $\mathbb{C}[x]$ has exactly n roots in \mathbb{C} counting multiplicity.

Actually using the Fundamental Theorem of Algebra for what we are about to do is too much!

Instead, we can actually derive it using the results that we are about to obtain. Every time we look at the field $F[x]/p(x)F[x]$ where $p(x)$ is irreducible in $F[x]$, we have created a field which is a field extension of F that contains a root of $p(x)$. In fact the coset $x + p(x)F[x]$ abstractly describes this root. But still we can make a field extension that has the root. Let's call this root β . Our new field we will isomorphically label and think of as $F(\beta)$. This means that in this new field extension $F(\beta)$, $p(x) = (x - \beta) \cdot q(x) \in F(\beta)[x]$ since β is now a good coefficient. Now repeat this idea to have a field extension of $F(\beta)$ that contains a root of $q(x)$, etc. until we have a field that contains all of the roots of $p(x)$. Let's call this field K . Therefore, $p(x)$ is completely factorable in $K[x]$ into linear factors $(x - \omega)$. Some of these could be repeated. Each factorization of $p(x)$ can only have n roots counting multiplicity due to adding exponents in polynomial factorization.

But what if there were two different factorizations? Could we not have more than n roots?

This is not the case and is guaranteed because of the Euclidean algorithm in $K[x]$. If there is one factor that appears in one factorization and not the other, simply “mod” out by that factor in both factorizations. In one factorization we would get zero and in the other, we would get something that has an inverse in that mod. *But zero is not invertible in any mod by any polynomial!* Therefore, the factorization is unique and there are exactly n roots counting multiplicity in the field extension K .

So even if we never knew \mathbb{C} existed, we would still be in good shape!

Theorem 9.2.8 Primitive Element Theorem

The field $\mathbb{Q}(\alpha, \beta)$ is equal to $\mathbb{Q}(\gamma)$ for an algebraic number γ . In particular, any algebraic field extension formed from a subfield F of \mathbb{C} by adjoining a finite number of algebraic numbers is a simple algebraic field extension formable by adjoining a single element.

Proof. Let F be a subfield of \mathbb{C} that is an algebraic field extension of \mathbb{Q} . Let c be an element of F and let $p(x)$ be the minimal polynomial of c .

We have some key ideas that help us analyze algebraic field extensions:

The only places that c can be sent in a ring homomorphism $\phi : F \rightarrow \mathbb{C}$ are to roots of $p(x)$ since

$$0 = p(c) = \phi(0) = \phi(p(c)) = p(\phi(c))$$

That is, $\phi(c)$ is a root of $p(x)$.

Suppose that $\phi : F(\alpha) \rightarrow \mathbb{C}$ is a ring homomorphism between the fields $F(\alpha)$ and \mathbb{C} such that $\phi(t) = t$ for all $t \in F$. Then, any element of $F(\alpha)$ can be written as a polynomial in $F[x]$ where x is replaced by α . The image of such a polynomial under the function ϕ is completely determined by the image of α . So if the minimal polynomial over F (i.e. in $F[x]$) has degree n , then *there are at most n distinct ring homomorphisms $F(\alpha) \rightarrow \mathbb{C}$ and no more that fix all the elements of F .*

Find $\gamma \in \mathbb{Q}(\alpha, \beta)$ so that there is one and only one ring homomorphism $\mathbb{Q}(\alpha, \beta) \rightarrow \mathbb{C}$ that fix all the elements of $\mathbb{Q}(\gamma)$. This would show that all elements of $\mathbb{Q}(\alpha, \beta)$ have minimal polynomials over $\mathbb{Q}(\gamma)$ (i.e. in $\mathbb{Q}(\gamma)[x]$) of degree 1. That is, those elements would be in $\mathbb{Q}(\gamma)$. This would be enough.

So how do we find such a $\gamma \in \mathbb{Q}(\alpha, \beta)$? First of all, $\mathbb{Q}(\alpha, \beta)$ is a field extension of $\mathbb{Q}(\alpha)$ where everything can be expressed as a polynomial in $\mathbb{Q}(\alpha)[x]$ with x replaced by β . And everything in $\mathbb{Q}(\alpha)$ can be written as a polynomial in $\mathbb{Q}[x]$ with x replaced by α . So, everything in $\mathbb{Q}(\alpha, \beta)$ can be written as a 2-variable polynomial with the variables really being the constants α and β . Therefore, every ring homomorphism $\mathbb{Q}(\alpha, \beta) \rightarrow \mathbb{C}$ that fixes the elements of \mathbb{Q} is completely determined by where it sends α and β . Since there are only finitely many options for both α and β , there are only finitely many ring homomorphisms that work for ϕ .

What we do is to find an element $k \cdot \alpha + \beta \in \mathbb{Q}(\alpha, \beta)$ for some $k \in \mathbb{Q}$ such that the only time $\phi(k \cdot \alpha + \beta) = k \cdot \alpha + \beta$ among all the ring homomorphisms $\phi : \mathbb{Q}(\alpha, \beta) \rightarrow \mathbb{C}$ that fix the elements of \mathbb{Q} is when ϕ is the identity map.

Let's look at this equation:

$$\phi(k \cdot \alpha + \beta) = k \cdot \alpha + \beta$$

Since ϕ is additive and scalable:

$$k \cdot \phi(\alpha) + \phi(\beta) = k \cdot \alpha + \beta$$

$$k \cdot \phi(\alpha) - k \cdot \alpha = \beta - \phi(\beta)$$

$$k = \frac{\beta - \phi(\beta)}{\phi(\alpha) - \alpha} \text{ or } k = 0$$

In other words, k must satisfy such equalities in order for ϕ to fix $k \cdot \alpha + \beta$. Since there are only finitely many ϕ we are looking at, there are only finitely many values of k to avoid. Since \mathbb{Q} is infinite, we are in good shape. Most $k \cdot \alpha + \beta$ will work as an acceptable γ . \square

Theorem 9.2.9

Given $\gamma \in \mathbb{C}$ that is the root of a monic polynomial $p(x)$ in $\mathbb{Q}[x]$, then there are exactly n distinct ring homomorphisms $\mathbb{Q}(\gamma) \rightarrow \mathbb{C}$ that fix all the elements of \mathbb{Q} .

Proof. Looking at the ideas of the last proof, these functions ϕ are uniquely determined by which root of the

minimal polynomial $p(x)$ of γ that γ should be sent to. If $p(x)$ has degree n , then there are precisely n roots that γ could be sent to. Yet some of these roots might be the same because the fundamental theorem of algebra says that there are precisely n roots counting multiplicity. We do not know if all these roots are distinct. If two of them were the same, they would yield the same homomorphism. Yet, we will use the fact that $p(x)$ is irreducible in $\mathbb{Q}[x]$. We know that the derivative $p'(x)$ has degree $n - 1$ and cannot share a (monic polynomial) common factor with $p(x)$ other than 1 since $p(x)$ is irreducible. Therefore, using the Euclidean algorithm, we can find $a(x)$ and $b(x)$ so that

$$a(x)p(x) + b(x)p'(x) = 1$$

If $p(x)$ has a repeated factor $(x - \omega)$, then it can be written as $p(x) = (x - \omega)^2 \cdot q(x)$. Using the product rule,

$$p'(x) = 2(x - \omega) \cdot q(x) + (x - \omega)^2 \cdot q'(x)$$

So it looks like if there were a repeated factor that $(x - \omega)$ would have to be a common factor to both $p(x)$ and $p'(x)$. Notice how this yields a problem with $a(x)p(x) + b(x)p'(x) = 1$. Because $q(x)$ would then be a factor of $a(x)p(x) + b(x)p'(x)$ —which means it should be a factor of 1—a contradiction! Hence, all the roots of $p(x)$ are distinct elements of \mathbb{C} so that there are precisely n distinct ring homomorphisms of the kind we are looking for. \square

Theorem 9.2.10

A ring homomorphism $\phi : \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ that fixes all of the elements of \mathbb{Q} is injective.

Proof. Let $p(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over \mathbb{Q} of degree n . But since $\phi(\alpha)$ is also a root of $p(x)$, it has the same minimal polynomial as α .

Consider the map that sends α to $x + p(x) \cdot \mathbb{Q}[x]$ in $\mathbb{Q}[x]/p(x) \cdot \mathbb{Q}[x]$. We have seen that this is an isomorphism from $\mathbb{Q}(\alpha)$. Now, send $x + p(x)$ to $\phi(\alpha)$ (another root of $p(x)$) which is again an isomorphism this time to $\mathbb{Q}(\phi(\alpha))$ which is the range of ϕ . The compositions of two isomorphisms is again an isomorphism. Then ϕ is an isomorphism onto its range and hence injective. \square

Normal Field Extension

A normal field extension K of F such that $F \subset K \subset \mathbb{C}$ is one such that all of the ring homomorphisms $K \rightarrow \mathbb{C}$ have range in K . That is, they can be thought of as functions $K \rightarrow K$.

Start with a field $\mathbb{Q}(\alpha)$ where α has minimal polynomial $p(x) \in \mathbb{Q}[x]$. Then, adjoin all of the roots of $p(x)$ to $\mathbb{Q}(\alpha)$ to get a field K . Think about a ring homomorphism $\psi : K \rightarrow \mathbb{C}$. It depends on the destinations of all of the roots of $p(x)$ that we have adjoined. These roots are of the form $\phi(\alpha)$ where $\phi : \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ is a ring homomorphism. Now think of $\psi(\phi(\alpha))$. Notice that $\psi \circ \phi$ is a ring homomorphism $\mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ so that $\psi(\phi(\alpha))$ is a root of $p(x)$ which is in K . Notice that ψ sends $\phi(\alpha)$ to something in K . Therefore, the range is

in K so that ψ can be thought of as $K \rightarrow K$. Thus, adjoining all of the roots of the minimal polynomial of α to $\mathbb{Q}(\alpha)$ creates a new field which is a normal field extension of \mathbb{Q} .

Theorem 9.2.11

Suppose that $F(\alpha) \subset \mathbb{C}$ is an algebraic field extension of F . Then, adjoining all of the roots of the minimal polynomial of α in $F[x]$ produces a normal field extension of F .

Normal Closure

Given an algebraic field extension $F(\alpha)$ of F , if we adjoin all of the roots of the minimal polynomial of α we get a new field K which we have just seen is normal. We call K the normal closure of the field $F(\alpha)$.

The normal closure K of $\mathbb{Q}(\alpha)$ itself is a *simple* algebraic field extension obtainable by adjoining an element γ . So $K = \mathbb{Q}(\gamma)$. The minimal polynomial of γ has degree equal to the dimension of K as a \mathbb{Q} -vector space. But even more is true. Every ring homomorphism $K \rightarrow \mathbb{C}$ that fixes elements of \mathbb{Q} can be thought of as an injective map $K \rightarrow K$ as we have seen. This map is also *surjective*.

Theorem 9.2.12

Suppose that $F \subset K \subset \mathbb{C}$ are fields and that K is the normal closure of F . Let ϕ be a ring homomorphism $K \rightarrow K$ that fixes all of the elements of F . Then ϕ is an isomorphism.

Proof. Let γ be such that $K = F(\gamma)$. Then γ and $\phi(\gamma)$ are two roots of the minimal polynomial $p(x) \in F[x]$ of γ over F of degree n . We know that the dimension of $F(\phi(\gamma))$ and the dimension of $K = F(\gamma)$ as F -vector spaces is in both cases n since $p(x)$ is the minimal polynomial of both $\phi(\gamma)$ and γ . Since K is normal and $F(\phi(\gamma))$ is the range of ϕ , we know that $F(\phi(\gamma)) \subset K$ is an n -dimensional subspace of an n -dimensional vector space and must therefore be the whole space. This tells us that the range is equal to the codomain so that ϕ is surjective. We have already shown above that ϕ is injective. \square

Notice that there are exactly n distinct ring homomorphisms of $K \rightarrow \mathbb{C}$ and all of these reduce to isomorphisms $K \rightarrow K$ which are completely determined by the destination of γ among the n distinct roots of $p(x)$. These isomorphisms when restricted to the set of roots of $p(x)$ become self-bijections on the set of n roots. That is, they are *permutations* of the roots.

Another word for a self-isomorphism is *automorphism*. We describe the group with respect to the composition operation \circ of automorphisms $K \rightarrow K$ that fix F the *automorphism group* of K over F otherwise known as the *Galois group* of K over F .

Automorphism

An isomorphism $K \rightarrow K$ where the domain is the same as the codomain is called an automorphism.

Galois Group

Given a normal field extension K of F , such that both are subfields of \mathbb{C} , the group of automorphisms $K \rightarrow K$ that fix F with the operation of composition is called the *Galois Group* of K over F .

The Galois group for K over F is completely describable as a subgroup of permutations among the roots of the minimal polynomial $p(x) \in F[x]$ of γ if $K = F(\gamma)$.

Suppose that $F \subset K \subset \mathbb{C}$ are fields and that K is normal. Suppose that G is the Galois group of K over F . We would like to establish a bijective correspondence between the subfields of K containing F and the subgroups of G . This illustrates some utility of Galois groups. They are useful for studying subfields. In fact, they are very useful for seeing how primes in \mathbb{Z} decompose in rings of integers of field extensions above it. Just to give some flavor though we prove the following which is part of the Fundamental Theorem of Galois theory.

Theorem 9.2.13 Fundamental Theorem of Galois Theory

We only give part of the actual theorem—there is a bijective correspondence between the fields L such that $F \subset L \subset K \subset \mathbb{C}$ and the subgroups of the Galois group G of the normal extension K of F .

Proof. Let L be such that $F \subset L \subset K$. There exists β so that $K = L(\beta)$. Let H_L be the subgroup of G comprised of the automorphisms that fix all the elements of L .

H_L

We use H_L to denote the subgroup of G comprised of the automorphisms that fix all the elements of L .

Let $g(x) \in L[x]$ be the minimal polynomial of β over L of degree m . We see that there are precisely m automorphisms of K that accomplish the task of being in H_L .

Notice that if T were also a subfield of K such that these same m automorphisms in H_L were the unique m automorphisms that fixed its elements, then H_L would be the Galois group of both K over L and of K over T . Then the dimension of K over L and of K over T would be the same.

We will use this fact in a minute. First, let's consider our task:

We are forming a correspondence *from* fields to subgroups: $L \mapsto H_L$. We need to establish that this correspondence is both injective and surjective.

Is the correspondence surjective? That is, given any subgroup of G , does it arise as H_L , i.e. all of the automorphisms of G that fix L for some L ? Consider the set K^H which we will use to denote all of the elements of K that H fixes.

$$K^H$$

The notation K^H denotes the fixed subfield of K by the elements of the automorphism subgroup H . That is, it consists of all elements of K that H fixes.

Because automorphisms split across addition, multiplication and multiplicative inverses, this set is closed under these operations as well—let's see why: if $a, b \in K^H$ and $\phi \in H$, then $\phi(a + b) = \phi(a) + \phi(b) = a + b$ so that $a + b \in K^H$. That is, K^H is a field. Let's call it the fixed field of H . So the question is whether K^H is sent to H via our correspondence.

Let's consider where K^H is sent. It is sent to the subgroup of *all* elements of G that fix K^H . We know H is in this subgroup—but is it the whole thing?

Let $L = K^H$. Then, $K = L(\beta)$ for some β . Now let

$$g(x) = \prod_{h \in H} (x - h(\beta))$$

Notice what happens if we apply any element $h_0 \in H$ to the coefficients of $g(x)$: we would get

$$\prod_{h \in H} (x - h_0 \circ h(\beta))$$

Note that $h_0 \circ H = H$: we can see this since h_0 has an inverse in H and by closure of the group operation \circ in H we know that $h_0^{-1} \circ H \subset H$. This tells us that $H = h_0 \circ h_0^{-1} \circ H \subset h_0 \circ H$. Therefore:

$$g(x) = \prod_{h \in H} (x - h_0 \circ h(\beta)) = \prod_{h \in H} (x - h(\beta))$$

The coefficients of $g(x)$ are fixed by the elements of H so that they are in K^H which we are calling L . Therefore, $g(x) \in L[x]$. Then since β is a root of $g(x)$, the minimal polynomial of β in $L[x]$ is a factor of $g(x)$. Yet $g(x)$ is also a factor of the minimal polynomial since all images of β under images of the automorphisms of G are roots of the minimal polynomial. So $g(x)$ itself is the minimal polynomial of β over L .

This tells us that the dimension of K as a L -vector space is precisely the degree of $g(x)$ which is the size of H . Since K is normal, we can talk about the Galois group of K over L . This Galois group *must be* H itself since the roots of $g(x)$ uniquely determine the automorphisms that fix L and send β somewhere—these are precisely the automorphisms that make up the Galois group of K over L . Remember that this Galois group of K over L is *all automorphisms* in the Galois group of G over F that fix L . So we have established that the correspondence is surjective.

Now, let's think about injectivity. Suppose that T and L both map to H under the correspondence $L \mapsto H_L$. That is, suppose that $H = H_L = H_T$. If $L \neq T$, then the correspondence would not be injective. So we need to show that $L = T$. We already know the correspondence is surjective. In fact, we know that $K^H \mapsto H$. Think about what K^H is. It is all elements of K which are fixed by H . Wait! The subfields T and L are both fixed by H so that they are subfields of K^H . Remember that $H = H_L$ is the Galois group of K over L . It is also the Galois group of K over T and K over K^H . This means that the dimension of K over all three fields L , T , and K^H is the same. These ideas taken together force $L = T = K^H$. The correspondence is therefore injective. \square

In the process of this last proof, we have the following (using the above notation):

Corollary 9.2.14

The dimension of K as a vector space with coefficients in K^H is the same as the size of the subgroup H of G .

Verify the following to yourself:

Corollary 9.2.15

In the correspondence, if $H_1 \subset H_2 \subset G$, then $K^{H_1} \supset K^{H_2} \supset L$ where $L = K^G$. The correspondence is inclusion reversing.

This next result will allow us to say even more about our correspondence:

Theorem 9.2.16

Consider fields $F \subset L \subset K$. We can think of L as $F(\alpha)$ for some α and K as $L(\beta)$ for some β . Suppose that the minimal polynomial of α in $F[x]$ has degree m and the minimal polynomial of β in $F(\alpha)[x]$ has degree r . the dimension of K as a F -vector space is mr .

Proof. First of all, it should be clear that the elements $\alpha^i\beta^j$ for $i = 1, \dots, m$ and $j = 1, \dots, r$ span K . If a

linear combination of them were equal to zero, just factor out the α^i 's so that we have a sum of them with their coefficients being linear combinations of β^j 's. Since the α^i 's are linearly independent, the linear combinations of the β^j 's must be zero. Since the β^j 's are linearly independent, their coefficients which are all coefficients in our original linear combination are all zeros. Hence, the set of products $\alpha^i\beta^j$'s are linearly independent and there are mr of them. Because they also span K , the dimension of K must be mr as a F vector space. \square

Suppose that K is a normal extension of F and that L , α , and β are as in the statement of this last theorem. Any automorphism ϕ in the Galois group of K over F is uniquely determined by the image of α and the image of β since these determine the images of the basis elements of K as a vector space over F . Since there are exactly mr automorphisms, and α has m choices of destinations and β has r , these choices can be made independently to arrive at an automorphism. This tells us that a ring homomorphism $L \rightarrow K$ that fixes F can be extended in r different ways to an automorphism $K \rightarrow K$. Let ϕ send α to c and β to itself. Then, ϕ with domain restricted to L is the ring homomorphism we are considering. Letting H be the Galois group of K over L (since K is normal), we have $\phi \circ H$ represents *all* of the possible extensions our ring homomorphism can have to an automorphism of K . Note that the size of H and hence $\phi \circ H$ is r .

Now when is L itself a normal extension so that it has a Galois group and we do not have to keep thinking about ring homomorphisms $L \rightarrow K$ and instead think of automorphisms $L \rightarrow L$?

It would make sense if quotienting out by H to consider G/H , the set of left cosets of H like $\phi \circ H$ (the extensions of a single ring homomorphism $L \rightarrow K$) actually formed a nice group. Realize that each left coset refers to a ring homomorphism of L . Do these ring homomorphisms (cosets) form a group (i.e. a Galois group of L over F)?

It turns out that the extension L is normal as we desire precisely when G/H is a group!

Normal Subgroup

A subgroup of a group G is normal when the set of left cosets denoted as the quotient G/H (or the set of just right cosets denoted as $H\backslash G$) is itself a group. The group operation \star is given by:

$$(g_1H) \star (g_2H) = g_1Hg_2H = (g_1g_2) \cdot H$$

Theorem 9.2.17

In our Galois subgroup to field correspondence, the subfield is normal precisely when the subgroup is normal.

Proof. Let G be the Galois group of K over F . Suppose that H is a normal subgroup of G . Then, $g_1Hg_2H = g_1g_2H$ for any $g_1, g_2 \in G$. Multiplying by g^{-1} on the left, we have $Hg_2H = g_2H$. Now choose $\text{id} \in H$ so: $Hg_2\text{id} \subset g_2H$. That is, $Hg \subset gH$. For finite groups any left coset and right coset are the same size with a

bijective correspondence to the subgroup H . Hence, $Hg = gH$.

Now take any element k in K^H , any $h \in H$, and any $g \in G$. Notice that $h(g(k)) = gh_1(k)$ for some h_1 since $Hg = gH$. Since h_1 fixes all the elements in K^H , $h_1(k) = k$ so that $h(g(k)) = g(k)$. That is, any $h \in H$ will fix $g(k)$. This forces $g(k) \in K^H$ so g produces a function $K^H \rightarrow K^H$ when the domain of g is restricted to K^H . Since this is true for all $g \in G$ and every ring homomorphism $K^H \rightarrow K$ that fixes F is extended by an element of G , K^H is normal.

When K^H is normal, each automorphism $K^H \rightarrow K^H$ extends to a whole collection of automorphisms of G —this collection is a whole coset of H . The group operation between the automorphisms of K^H over F extends to a group operation between the cosets which forces H to be normal. In particular, we can choose representatives g of our cosets in the description above that send β to itself so that the representative is only interested in the destination of α . Such g commute with the elements of H so $gh = hg$ and each left coset gH is the same as the right coset Hg . Notice that if $g_1 \in gH$ is another representative of the coset gH that $g_1 = gh$ for some h and $g_1H = ghH = gH$ since $hH = H$. This type of reasoning shows that $g_1H = Hg_1$. Therefore, every left coset gH is equal to the right coset Hg for any $g \in G$. This gives the nice desired group operation: $g_1Hg_2H = g_1g_2H$. \square

9.2.2 Proving the Fundamental Theorem of Algebra

There are a lot of fascinating ideas which come about because of the correspondences we have just proven. One of them is the Fundamental Theorem of Algebra itself. Even though we made mention of it already, we also discussed how we could get by without it—we know that for a given polynomial $p(x) \in \mathbb{C}[x]$, there exists some field out there M so that a $p(x)$ will completely factor into linear factors $(x - \omega)$ when thought of in $M[x]$ for $\omega \in M$. We discussed why we could assume this fact. But the trick is that we can always let $M = \mathbb{C}$ every time and that is enough! We just need this Galois correspondence, some other group theory ideas and the fact that we have a quadratic formula and that odd degree polynomials have either a down up or up down end behavior when graphed in real coordinates. In particular, since the odd degree polynomial is continuous *it must cross the x-axis*. So any odd degree polynomial has a factor $(x - r)$ for a root where $r \in \mathbb{R}$.

The only irreducible odd degree polynomials in $\mathbb{C}[x]$ have degree 1.

Ok. suppose that α is a root of an irreducible polynomial $f(x) \in \mathbb{C}[x]$. Let K be the normal closure of $\mathbb{C}(\alpha)$ and suppose that G is the Galois group of K over \mathbb{R} . This is a finite group. Suppose that it has n elements. We can think of M as being $M = \mathbb{R}(\beta)$ for some β where the minimal polynomial $g(x)$ of β has degree n . Since $g(x)$ is irreducible, it either has degree 1 which would mean that $\beta \in \mathbb{R}$ and we would be done or it is has even degree. So let's suppose that n is even.

We will come back to the proof of the Fundamental Theorem of Algebra after we have developed a couple of ideas from group theory.

Let's just consider an arbitrary finite group G for now with an even number of elements n . Consider all pairs (g, w) for $g, w \in G$ such that $gw = \text{id}$ except exclude the case (id, id) . Since every element $g \in G$ has a

unique inverse, there are $n - 1$ such pairs with the exclusion. Some of these pairs are repeated via reordering if $g \neq w$ so that (g, w) and (w, g) both occur distinctly counted in these $n - 1$ pairs. If this was true for all (g, w) , then $n - 1$ would be even which is a contradiction. Hence, there is at least one g so that $g = w$ which implies that $g^2 = \text{id}$. This is a special case of Cauchy's theorem.

Cauchy's Theorem Special Case

Every group with an even number of elements has at least one of them where $g^2 = \text{id}$.

Now let's go back to an arbitrary group G with n elements and partition it into what we call "conjugacy classes"—group elements that are related to each other $a \sim b$ by $a = gbg^{-1}$ for some b . There is a subgroup B of all group elements g of G such that $gbg^{-1} = b$. Each coset of B gives a different element a to which b is "conjugate" to. The number of cosets is a factor of n since each coset has the same size and the disjoint union of them is all of G (so disjoint sets of the same size combine to give G). Hence, the size of each class is a factor of n .

The size of Conjugacy Classes

The size of a conjugacy class as described above is a factor of the number of elements of the group.

By induction we wish to use these ideas to show that if the size of G is $2^m t$ where t is odd, then there is a subgroup of G of size 2^m . We induct on the size of n . Trivially, when $n = 1$, $m = 0$ and the whole group is a subgroup of size $2^0 = 1$. Now, assume that it is true for group sizes up through $n - 1$. We will show that it must be true for n too.

First, suppose that there is a subgroup H smaller than G that has an odd number of cosets. The size of G is the number of cosets multiplied to the size of H . Since 2^m shares no common factor with the number of cosets so must be a factor of the size of H . Then, by the induction hypothesis, H has a subgroup of the size 2^m which is the desired subgroup of G .

So, now assume that no subgroups of G have an odd number of cosets. This implies that the sizes of the conjugacy classes of G , which are equal to the size of a coset collection, are all even in length. This means that the number of conjugacy classes of size 1 (which includes the identity element) is even as well since the size of G is even and the conjugacy classes partition G . Now if an element has conjugacy class size 1 like $ggb^{-1} = \text{id} b \text{id}^{-1} = b$, then $gb = bg$ for all g , meaning it commutes with all the other group elements. The subset of all such elements in G is a subgroup of G called the center of G . Let's denote it by C .

By Cauchy's theorem, there exists $c \in C$ such that $c^2 = \text{id}$ and $Y = \{1, c\}$ is a subgroup of G . Since c commutes with every element of G , then $gY = Yg$ for all g so that Y is a normal subgroup of G . The size of the quotient G/Y is $\frac{n}{2}$ so that by the induction hypothesis, it has a subgroup T of size 2^{m-1} .

Let $u : G/Y \rightarrow T$ be the group map defined by sending an element to the coset of Y it is in. Then u^{-1} sends the partition made from the cosets of T bijectively (preimages of disjoint things are disjoint and u is surjective) to the cosets of $u^{-1}(T)$ which is itself a group—for example, if $a, b \in u^{-1}(T)$, then $u(a), u(b) \in T$

so that $u(ab) = u(a) \cdot u(b) \in T$ which shows that $ab \in u^{-1}(T)$. The bijective correspondence tells us that there are precisely as many cosets of T in G/Y as there are of $u^{-1}(T)$ in G . This number is t in both cases so that $u^{-1}(T)$ is the subgroup of size 2^m that we are after.

First 2-Sylow Theorem

Every finite group of size $2^m t$ where t is odd has a subgroup of size 2^m .

The last part of our induction argument that we just considered actually works when we change the induction hypothesis to: “a group of size 2^m has a subgroup of size 2^{m-1} .”

Corollary 9.2.18

Groups of size 2^m have subgroups of size 2^{m-1} .

Now back to our proof.

We are considering G as the Galois group of K over \mathbb{R} and suppose that it has size $n = 2^m t$ where t is odd. Then, it has a subgroup J of size 2^m . Then consider the fixed field K^J of J . The dimension of K over K^J is 2^m as a K^J -vector space by the Galois correspondence. The dimension of K^J over \mathbb{R} as a \mathbb{R} -vector space is t and is given by $\mathbb{R}(\gamma)$ for some γ with minimal polynomial of degree t which is odd. Yet we already saw that such an irreducible polynomial of odd degree must be degree 1 over \mathbb{R} . Therefore, $K^J = \mathbb{R}$ so that $G = J$. So the dimension of K over \mathbb{R} is 2^m . Now think that $\mathbb{C} = \mathbb{R}(i)$ and the minimal polynomial of i is $x^2 + 1$ so that \mathbb{C} has dimension 2 over \mathbb{R} .

Now, let G' be the Galois group of K over \mathbb{C} . It has size 2^{m-1} since the dimension of K over \mathbb{C} is 2^{m-1} . The group G' has a subgroup J' of size 2^{m-2} by our corollary. Then the dimension of K over $K^{J'}$ is 2^{m-2} and so the dimension over $K^{J'}$ over \mathbb{C} is 2. But by the quadratic formula and the fact that every complex number has a square root in \mathbb{C} , there cannot exist any degree 2 extensions of \mathbb{C} . This is our contradiction if we assume that $m > 1$. Hence, $m = 1$ so the dimension of K over \mathbb{C} is 1. That is, $K = \mathbb{C}$. Therefore, \mathbb{C} contains α . Remember that α was an arbitrary root of a polynomial in $\mathbb{C}[x]$. Therefore, \mathbb{C} contains all roots of any polynomial in $\mathbb{C}[x]$.

9.2.3 Examples: Matrix Diagonalization to Compute Galois Groups

We will now use eigenvectors to determine Galois groups of field extensions of \mathbb{Q} in terms of permutations of roots!

Example 3. *Finding a Primitive Element.* Suppose that we have a field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over \mathbb{Q} . Note $x^2 - 2$ is irreducible over \mathbb{Q} . Therefore, $\{1, \sqrt{2}\}$ forms a basis for $\mathbb{Q}(\sqrt{2})$ as a vector space over \mathbb{Q} (i.e. with scalars in \mathbb{Q}). Similarly, $\{1, \sqrt{3}\}$ forms a basis for $\mathbb{Q}(\sqrt{3})$ over \mathbb{Q} . Suppose that $k \in \mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3})$. Then, $k = a + b\sqrt{2} = c + d\sqrt{3}$ for $a, b, c, d \in \mathbb{Q}$. Let $e = c - a$. Then, we can write:

$$b\sqrt{2} = e + d\sqrt{3}$$

Squaring:

$$2b^2 = e^2 + 2ed\sqrt{3} + 3d^2$$

This forces $\sqrt{3}$ to be in \mathbb{Q} . This cannot be true since $\sqrt{3}$ is a root of an irreducible polynomial of degree 2 over \mathbb{Q} . Therefore, $\sqrt{3}$ is not in $\mathbb{Q}(\sqrt{2})$. Hence, $x^2 - 3$ does not factor in $\mathbb{Q}(\sqrt{2})[x]$. Therefore, it must be irreducible over $\mathbb{Q}(\sqrt{2})$ with a basis of $\{1, \sqrt{3}\}$ as a $\mathbb{Q}(\sqrt{2})$ -vector space (i.e. scalars in $\mathbb{Q}(\sqrt{2})$).

The proof of theorem 9.2.16 shows that in such a situation, a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ arises as products of basis elements from $\{1, \sqrt{2}\}$ and $\{1, \sqrt{3}\}$. Therefore, we have:

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$$

as a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a \mathbb{Q} -vector space of dimension 4. Let's see if we can find a primitive element for this field extension. In a previous proof, we saw that such an element can be of the form $\sqrt{2} + a\sqrt{3}$ where $a \in \mathbb{Q}$. Let's try $\sqrt{2} + \sqrt{3}$. To check to see if this element is really a primitive one, we turn to matrices.

First, let's think of $\sqrt{2}$ and $\sqrt{3}$ as matrix functions that act as linear transformations $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$ via their multiplication action. We will think of the basis element "1" as e_1 , " $\sqrt{2}$ " as e_2 , " $\sqrt{3}$ " as e_3 and " $\sqrt{6}$ " as e_4 . Then the vector $(1, 0, 0, 0)$ represents "1," the vector $(0, 1, 0, 0)$ represents $\sqrt{2}$, the vector $(0, 0, 1, 0)$ represents " $\sqrt{3}$ " and $(0, 0, 0, 1)$ represents " $\sqrt{6}$." Multiplication by $\sqrt{2}$ then sends $(1, 0, 0, 0)$ (really 1) to $(0, 1, 0, 0)$ (really $\sqrt{2}$). It also sends $(0, 0, 0, 1)$ (really $\sqrt{6}$) to $(0, 0, 2, 0)$ (really $2\sqrt{3} = \sqrt{12}$). Using these ideas, we have:

$$\begin{aligned} \sqrt{2} \cdot & : \begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix} & \sqrt{3} \cdot & : \begin{pmatrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \\ (\sqrt{2} + \sqrt{3}) \cdot & : \begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix} \end{aligned}$$

The characteristic polynomial of this last matrix is:

$$x^4 - 10x^2 + 1$$

which is irreducible and hence is the minimal polynomial of $\sqrt{2} + \sqrt{3}$. This means that $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ has dimension 4 as a \mathbb{Q} -vector space. Since $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

Since both $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ have \mathbb{Q} -dimension 4, they must therefore be equal:

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

Hence, $\sqrt{2} + \sqrt{3}$ is a primitive element that generates $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over \mathbb{Q} .

Theorem 9.2.19

Suppose that $K = F(\gamma)$ where F is either \mathbb{Q} or an extension of it and γ is an algebraic number over F . Let A be the matrix which gives the multiplication action of γ on K as a F -vector space with respect to some basis. Then, A is diagonalizable and it has n distinct eigenvalues representing the n distinct roots of its minimal polynomial where n is the dimension of K as a F -vector space. The same matrix U that diagonalizes the matrix A as $D = U^{-1}AU$ also diagonalizes the matrices for the multiplication action of every other element of K .

Proof. Since γ is a primitive element of the field extension, then its minimal polynomial has degree equal to the dimension of K as a F -vector space. Minimal polynomials are always irreducible. An earlier proof showed that irreducible polynomials in $F[x]$ where F is an extension of \mathbb{Q} have no repeated roots. The condition for diagonalizability is that the minimal polynomial has no repeated roots.

Every element of K can be written as a F -linear combination of powers of γ . So, the multiplication action matrix of any element of K is a F -linear combination of powers of the matrix A . Notice that

$$U^{-1}A^2U = U^{-1}AAU = \underbrace{U^{-1}AU}_{D} \underbrace{UU^{-1}AU}_{D}$$

Since multiplying two diagonal matrices together is still a diagonal matrix, U diagonalizes A^2 which represents γ^2 . The same is true for every power γ^j .

Suppose that $U^{-1}BU$ is a diagonal matrix. Then if $r \in F$,

$$U^{-1}rBU = rU^{-1}BU$$

is still a diagonal matrix. Therefore, rB is diagonalized by U .

If B and C are both diagonalized by U , then

$$U^{-1}(B + C)U = U^{-1}BU + U^{-1}CU$$

which is the sum of two diagonal matrices is also diagonal. Hence the sum $B + C$ can be diagonalized by U . \square

Remember that we build U by finding eigenvectors.

Corollary 9.2.20

The matrices representing the multiplication action of any element in an algebraic field extension K over F where F is either \mathbb{Q} or an extension of it *all share the same eigenvectors*. The eigenvalues associated to those eigenvectors may change, but the idea of being an eigenvector carries over perfectly from one of these matrices to another.

Corollary 9.2.21

If $K = F(\gamma)$ is an algebraic field extension of dimension n (where F is an extension of \mathbb{Q}), the n ring homomorphisms ϕ_1, \dots, ϕ_n given as $K \rightarrow \mathbb{C}$ can be described by the following:

- Let U diagonalize the matrix A representing the multiplication action of K as a F -vector space of γ with respect to some basis.
- Represent an element $\beta \in K$ as the matrix M_β of its multiplication action on K as a F -vector space with respect to the same basis.
- Compute $U^{-1}BU$.
- Then, $\phi_i(\beta)$ is the i th diagonal entry of $U^{-1}M_\beta U$.

That is,

$$\phi_i(\beta) = e_i^T U^{-1} M_\beta U e_i$$

If K is a normal field extension, these give the automorphisms $K \rightarrow K$ in the Galois group of K over F .

Proof. First, diagonalizing by U splits across matrix multiplication and addition. Next, projecting to the i th diagonal coordinate splits across diagonal matrix multiplication and addition. Therefore, their composition gives a ring homomorphism which sends M_γ to one of its possible n different eigenvalues (roots) of the minimal polynomial of γ . \square

Since change of basis does not change the characteristic polynomial of a matrix and consequently does not change its trace nor its determinant, we can make the following definitions.

Trace in an Algebraic Field Extension

We define the trace of an element $k \in K$ of an algebraic field extension K over F (of finite dimension over F where K and F are subfields of \mathbb{C}) as being the trace of any matrix B representing its multiplication action over K as a vector space over F . From what we have above, this is equivalent to the sum of diagonal entries $U^{-1}BU$ which is the sum

$$\sum_i \phi_i(k)$$

for the n ring homomorphisms $K \rightarrow \mathbb{C}$.

Norm in an Algebraic Field Extension

We define the norm of an element $k \in K$ of an algebraic field extension K over F (of finite dimension over F where K and F are subfields of \mathbb{C}) as being the trace of any matrix B representing its multiplication action over K as a vector space over F . From what we have above, this is equivalent to the product of diagonal entries $U^{-1}BU$ which is the product

$$\prod_i \phi_i(k)$$

for the n ring homomorphisms $K \rightarrow \mathbb{C}$.

Example 4. Computing the Galois Group. Let's go back to our example of $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. The minimal polynomial of $\sqrt{2} + \sqrt{3}$ is $x^4 - 10x^2 + 1$. Its four distinct roots are:

$$\sqrt{2} + \sqrt{3} \quad -\sqrt{2} + \sqrt{3} \quad \sqrt{2} - \sqrt{3} \quad -\sqrt{2} - \sqrt{3}$$

The following code uses the ideas above to compute the Galois group of the extension $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ over \mathbb{Q} and presents the result in permutation cycle notation where the roots are labeled as 1 through 4. The automorphisms are build using diagonalization of the matrices corresponding to the roots and then projecting them to a specified diagonal coordinate which again will be a root. So we are looking at permutations of roots.



Link to run the code.

```
#Matrix for sqrt(2)
a=matrix(4,4,[0,2,0,0,1,0,0,0,0,0,0,2,0,0,1,0])
#Matrix for sqrt(3)
b=matrix(4,4,[0,0,3,0,0,0,0,3,1,0,0,0,0,1,0,0])
#Matrix for sqrt(2)+sqrt(3)
A=a+b

#We can compute the minimal polynomial of sqrt(2)+sqrt(3):
x = polygen(QQ, 'x')
f=(a+b).minpoly()
print(f)

#These are lists corresponding to the same roots of this minimal polynomial
#MM gives the matrix form and R gives the number form
MM=[a+b,a-b,-a+b,-a-b]
R=[sqrt(2)+sqrt(3),sqrt(2)-sqrt(3),-sqrt(2)+sqrt(3),-sqrt(2)-sqrt(3)]

#Returns Matrix (A-Eigenvalue*Identity)
def mm(j):
    return A-R[j]*matrix.identity(4)

#Compute Eigenvectors by Ranges corresponding to factors of the minimal polynomial
A0=mm(1)*mm(2)*mm(3)
A1=mm(0)*mm(2)*mm(3)
A2=mm(0)*mm(1)*mm(3)
A3=mm(0)*mm(1)*mm(2)
L=[A0,A1,A2,A3]

#This is the matrix that diagonalizes all the matrices corresponding to
#elements in the field
U=matrix([C.columns()[0] for C in L]).transpose().n()
print(U)
```

```

#Build a table where each row will represent the outputs of an automorphism
#where the inputs are in the first row.
#This first table is of numerical approximations
TC=[]
#Ranges through the roots in matrix form
for M in MM:
    cc=[]
    for w in L:
        #one of the four eigenvectors
        t=matrix(4,1,w.columns()[0])
        AL=list(M*t.n())
        tL=list(t.n())
        #Computes eigenvalue for the matrix M for eigenvector t
        cc+=[AL[0]/tL[0]]
    TC+=[cc]
T=matrix(TC).transpose()

#This next table relabels the numerical approximations with exact values
dcc={round(TC[0][0],ndigits=3):R[0], round(TC[0][1],ndigits=3):R[1]}
dcc[round(TC[0][2],ndigits=3)]=R[2]
dcc[round(TC[0][3],ndigits=3)]=R[3]
TC2=[]
for M in MM:
    cc=[]
    for w in L:
        t=matrix(4,1,w.columns()[0])
        AL=list(M*t.n())
        tL=list(t.n())
        cc+=[dcc[round(AL[0]/tL[0],ndigits=3)]]
    TC2+=[cc]
T2=matrix(TC2).transpose()
#print(T2)

#Now relabel the roots as 1,2,3,4
dc={round(TC[0][0],ndigits=3):1, round(TC[0][1],ndigits=3):2}
dc[round(TC[0][2],ndigits=3)]=3
dc[round(TC[0][3],ndigits=3)]=4

Functions=[]
for g in T:
    Functions+=[[dc[round(r,ndigits=3)] for r in g]]
print(matrix(Functions))

#Turn each row as a permutation function into cycle notation.
G = SymmetricGroup(4)
FunctionCycles=[]
for g in Functions:
    FunctionCycles+=[G(Permutation(g))]
print(FunctionCycles)

```

Output:

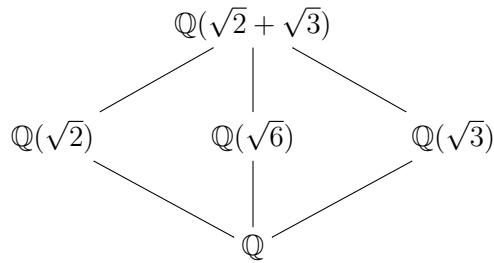
```
x^4 - 10*x^2 + 1
[ 15.4134846045141  1.55707814396306 -1.55707814396306 -15.4134846045141]
[ 10.8989794855664  1.10102051443364  1.10102051443364  10.8989794855664]
[ 8.89897948556636 -0.898979485566356 -0.898979485566357  8.89897948556636]
[ 6.29252873988395 -0.635674490391564  0.635674490391564 -6.29252873988395]
[ sqrt(3) + sqrt(2) -sqrt(3) + sqrt(2)  sqrt(3) - sqrt(2) -sqrt(3) - sqrt(2) ]
[-sqrt(3) + sqrt(2)  sqrt(3) + sqrt(2) -sqrt(3) - sqrt(2)  sqrt(3) - sqrt(2) ]
[ sqrt(3) - sqrt(2) -sqrt(3) - sqrt(2)  sqrt(3) + sqrt(2) -sqrt(3) + sqrt(2) ]
[-sqrt(3) - sqrt(2)  sqrt(3) - sqrt(2) -sqrt(3) + sqrt(2)  sqrt(3) + sqrt(2) ]
[1 2 3 4]
[2 1 4 3]
[3 4 1 2]
[4 3 2 1]
[(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)]
```

The four automorphisms as functions on the roots making the Galois group G are given as:

$$\begin{array}{c|ccccc}
r & \sqrt{3} + \sqrt{2} & -\sqrt{3} + \sqrt{2} & \sqrt{3} - \sqrt{2} & -\sqrt{3} - \sqrt{2} \\
\hline
\phi_1(r) & \sqrt{3} + \sqrt{2} & -\sqrt{3} + \sqrt{2} & \sqrt{3} - \sqrt{2} & -\sqrt{3} - \sqrt{2} \\
\phi_2(r) & -\sqrt{3} + \sqrt{2} & \sqrt{3} + \sqrt{2} & -\sqrt{3} - \sqrt{2} & \sqrt{3} - \sqrt{2} \\
\phi_3(r) & \sqrt{3} - \sqrt{2} & -\sqrt{3} - \sqrt{2} & \sqrt{3} + \sqrt{2} & -\sqrt{3} + \sqrt{2} \\
\phi_4(r) & -\sqrt{3} - \sqrt{2} & \sqrt{3} - \sqrt{2} & -\sqrt{3} + \sqrt{2} & \sqrt{3} + \sqrt{2}
\end{array}$$

Notice that ϕ_1 is the same as id. The five subgroups of G with the fields that they fix are:

$\underbrace{\{\phi_1\}}$	$\underbrace{\{\phi_1, \phi_2\}}$	$\underbrace{\{\phi_1, \phi_3\}}$	$\underbrace{\{\phi_1, \phi_4\}}$	$\underbrace{\{\phi_1, \phi_2, \phi_3, \phi_4\}}$
Fixes $\mathbb{Q}(\sqrt{2} + \sqrt{3})$	Fixes $\mathbb{Q}(\sqrt{2})$	Fixes $\mathbb{Q}(\sqrt{3})$	Fixes $\mathbb{Q}(\sqrt{6})$	Fixes \mathbb{Q}



The subgroups are in perfect correspondence with the intermediate fields between \mathbb{Q} and $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Example 5. Consider the roots of $x^4 + 2$ which is irreducible in $\mathbb{Q}[x]$. The four roots are $\pm i\sqrt[4]{2}$ and $\pm \sqrt[4]{2}$. Let L be the extension of \mathbb{Q} that comes from adjoining these roots. Then, L is a normal extension of \mathbb{Q} so that we can talk about the Galois group of this field extension.

Note that $\sqrt[2]{4} \in L$. We know that the dimension of $\mathbb{Q}(\sqrt[4]{2})$ as a \mathbb{Q} -vector space is 4 since the minimal polynomial of $\sqrt[4]{2}$ is $x^4 + 2$ which has degree 4.

Further realize that $i \in L$ just by dividing two of these roots. Since the minimal polynomial of i is $x^2 + 1$, the dimension of $\mathbb{Q}(i)$ as a vector space over \mathbb{Q} is 2. Notice that $\mathbb{Q}(i) \cap \mathbb{R} = \mathbb{Q}$ so that $\mathbb{Q}(i) \cap \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}$. In particular:

$$i \notin \mathbb{Q}(\sqrt[4]{2})$$

Hence, i is linearly independent to all the elements in $\mathbb{Q}(\sqrt[4]{2})$. This tells us that $x^2 + 1 = (x - i)(x + i)$ is irreducible in $\mathbb{Q}(\sqrt[4]{2})$.

Thus, a basis for $\mathbb{Q}(i, \sqrt[4]{2})$ comes from the set product of the two bases $\{1, i\}$ and $\{1, \sqrt[4]{2}, \sqrt[4]{2}^2, \sqrt[4]{2}^3\}$ to yield:

$$\{1, \sqrt[4]{2}, \sqrt[4]{2}^2, \sqrt[4]{2}^3, i, i\sqrt[4]{2}, i\sqrt[4]{2}^2, i\sqrt[4]{2}^3\}$$

It should be clear that $L = \mathbb{Q}(i, \sqrt[4]{2})$. Thus, L has dimension 8 over \mathbb{Q} . Adding one root gives dimension 4—but adding *all* roots gives dimension 8.

With respect to this basis, multiplication by i is given by the matrix:

$$i \cdot : \begin{pmatrix} 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

This matrix has a minimal polynomial of $x^2 + 1$ just like i itself. We also consider multiplication by $\sqrt[4]{2}$ as a matrix:

$$\sqrt[4]{2} \cdot : \begin{pmatrix} 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

This matrix has a minimal polynomial as $x^4 - 2$ which is the same as the minimal polynomial of $\sqrt[4]{2}$. Now if

we add these two matrices together we get:

$$i + \sqrt[4]{2} : \begin{pmatrix} 0 & 0 & 0 & 2 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

This matrix has a minimal polynomial of:

$$p(x) = x^8 + 4x^6 + 2x^4 + 28x^2 + 1$$

which is irreducible. Hence, $i + \sqrt[4]{2}$ is a primitive element of our extension. The Galois group of L over \mathbb{Q} then gives 8 permutations of the roots of $p(x)$ which are uniquely determined by the destination of the root $i + \sqrt[4]{2}$. The roots are:

$$\{\sqrt[4]{2} + i, i \cdot \sqrt[4]{2} + i, -\sqrt[4]{2} + i, -i \cdot \sqrt[4]{2} + i, \sqrt[4]{2} - i, i \cdot \sqrt[4]{2} - i, -\sqrt[4]{2} - i, -i \cdot \sqrt[4]{2} - i\}$$

The following code computes the automorphisms.



[Link to run the code.](#)

```
#Matrix for i
imL=[[0,0,0,0,1,0,0,0]+[0,0,0,0,0,1,0,0]+[0,0,0,0,0,0,1,0]+[0,0,0,0,0,0,0,1]
imL+=[-1,0,0,0,0,0,0,0]+[0,-1,0,0,0,0,0,0]+[0,0,-1,0,0,0,0,0]+[0,0,0,-1,0,0,0,0]
im=matrix(8,8,imL).transpose()
#matrix for fourth root of 2
reL=[[0,1,0,0,0,0,0,0]+[0,0,1,0,0,0,0,0]+[0,0,0,1,0,0,0,0]+[2,0,0,0,0,0,0,0]
reL+=[[0,0,0,0,1,0,0,0]+[0,0,0,0,0,1,0,0]+[0,0,0,0,0,0,1,0]+[0,0,0,2,0,0,0,0]
re=matrix(8,8,reL).transpose()
#matrix for primitive element
A=re+im
f(x)=A.minpoly()
print(A.minpoly())
aa=2^(1/4)
#The list of roots of f(x)
R=[aa*I,I*aa+I,-aa+I,-I*aa+I,aa-I,I*aa-I,-aa-I,-I*aa-I]

#Computes A-x*I
def mm(j):
    return A-R[j]*matrix.identity(8)
#Computes an eigenvector for a given eigenvalue
def Eigenvec(k):
    L=list(range(8))
    L.remove(k)
    W=matrix.identity(8)
    for j in L:
        W=W.n()*(mm(j).n())
    t=matrix(W.columns()[0]).transpose()
    return t
#List of matrices corresponding to the roots
MM=[re+im,im*re+im,-re+im,-im*re+im,re-im,im*re-im,-re-im,-im*re-im]
TC=[]
#Builds the Table
for k in range(8):
    cc=[]
    M=MM[k]
    for j in range(8):
        t=Eigenvec(j)
        AL=list(M*t.n())
        tL=list(t.n())
        cc+=[AL[0]/tL[0]]
    TC+=[cc]
T=matrix(TC).transpose()
print(T)
```

The output yields the following table of automorphisms:

r	$\sqrt[4]{2} + i$	$i \cdot \sqrt[4]{2} + i$	$-\sqrt[4]{2} + i$	$-i \cdot \sqrt[4]{2} + i$	$\sqrt[4]{2} - i$	$i \cdot \sqrt[4]{2} - i$	$-\sqrt[4]{2} - i$	$-i \cdot \sqrt[4]{2} - i$
$\phi_1(r)$	$\sqrt[4]{2} + i$	$i \cdot \sqrt[4]{2} + i$	$-\sqrt[4]{2} + i$	$-i \cdot \sqrt[4]{2} + i$	$\sqrt[4]{2} - i$	$i \cdot \sqrt[4]{2} - i$	$-\sqrt[4]{2} - i$	$-i \cdot \sqrt[4]{2} - i$
$\phi_2(r)$	$i \cdot \sqrt[4]{2} + i$	$-\sqrt[4]{2} + i$	$-i \cdot \sqrt[4]{2} + i$	$\sqrt[4]{2} + i$	$i \cdot \sqrt[4]{2} - i$	$-\sqrt[4]{2} - i$	$-i \cdot \sqrt[4]{2} - i$	$\sqrt[4]{2} - i$
$\phi_3(r)$	$-\sqrt[4]{2} + i$	$-i \cdot \sqrt[4]{2} + i$	$\sqrt[4]{2} + i$	$i \cdot \sqrt[4]{2} + i$	$-\sqrt[4]{2} - i$	$-i \cdot \sqrt[4]{2} - i$	$\sqrt[4]{2} - i$	$i \cdot \sqrt[4]{2} - i$
$\phi_4(r)$	$-i \cdot \sqrt[4]{2} + i$	$\sqrt[4]{2} + i$	$i \cdot \sqrt[4]{2} + i$	$-\sqrt[4]{2} + i$	$-i \cdot \sqrt[4]{2} - i$	$\sqrt[4]{2} - i$	$i \cdot \sqrt[4]{2} - i$	$-\sqrt[4]{2} - i$
$\phi_5(r)$	$\sqrt[4]{2} - i$	$-i \cdot \sqrt[4]{2} - i$	$-\sqrt[4]{2} - i$	$i \cdot \sqrt[4]{2} - i$	$\sqrt[4]{2} + i$	$-i \cdot \sqrt[4]{2} + i$	$-\sqrt[4]{2} + i$	$i \cdot \sqrt[4]{2} + i$
$\phi_6(r)$	$i \cdot \sqrt[4]{2} - i$	$\sqrt[4]{2} - i$	$-i \cdot \sqrt[4]{2} - i$	$-\sqrt[4]{2} - i$	$i \cdot \sqrt[4]{2} + i$	$\sqrt[4]{2} + i$	$-i \cdot \sqrt[4]{2} + i$	$-\sqrt[4]{2} + i$
$\phi_7(r)$	$-\sqrt[4]{2} - i$	$i \cdot \sqrt[4]{2} - i$	$\sqrt[4]{2} - i$	$-i \cdot \sqrt[4]{2} - i$	$-\sqrt[4]{2} + i$	$i \cdot \sqrt[4]{2} + i$	$\sqrt[4]{2} + i$	$-i \cdot \sqrt[4]{2} + i$
$\phi_8(r)$	$-i \cdot \sqrt[4]{2} - i$	$-\sqrt[4]{2} - i$	$i \cdot \sqrt[4]{2} - i$	$\sqrt[4]{2} - i$	$-i \cdot \sqrt[4]{2} + i$	$-\sqrt[4]{2} + i$	$i \cdot \sqrt[4]{2} + i$	$\sqrt[4]{2} + i$

Further code may be run to turn these automorphisms into a cycle notation of a permutation of their roots:

$[((), (1, 2, 3, 4)(5, 6, 7, 8), (1, 3)(2, 4)(5, 7)(6, 8), (1, 4, 3, 2)(5, 8, 7, 6), (1, 5)(2, 8)(3, 7)(4, 6),$

$(1, 6)(2, 5)(3, 8)(4, 7), (1, 7)(2, 6)(3, 5)(4, 8), (1, 8)(2, 7)(3, 6)(4, 5)]$

One can check that if we relabel $(1, 2, 3, 4)(5, 6, 7, 8)$ and $(1, 5)(2, 8)(3, 7)(4, 6)$ as s , the group elements can be written as:

$$\{\text{id}, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

where the multiplication between elements *means composition*. One can also see that $rs = sr^3$. This group has the same structure as the symmetry group on the vertices of a square where r is rotation and s is reflection. This group is called the Dihedral group of order 8.

9.2.4 Cyclotomic Polynomials

Example 6. *Cyclotomic Polynomial.* Consider the extension $\mathbb{Q}(\zeta)$ for $\zeta \in \mathbb{C}$ where $n = 10$ is the smallest positive integer exponent such that $\zeta^n = 1$. In this example, we will find the minimal polynomial of ζ —it will be called a *cyclotomic polynomial*.

Primitive Root of Unity

Such a ζ is called a primitive 10th root of unity (i.e. 1).

The powers therefore repeat themselves every 10. Thinking about this repetition, the first time that $(\zeta^3)^m = 1$ will be $m = 10$ since 3 shares no common factor with 10. The first time $3m$ will be a multiple of 10 is when $m = 10$ itself. This requires that ζ^3 is also a *primitive* 10th root of unity. Using this same logic, the following are all primitive 10th roots of unity:

$$\zeta, \zeta^3, \zeta^7, \zeta^9$$

Recall that the Euler- ϕ function applied to 10 introduced in the last section counts how many integers from 1 to 10 share no common factors with 10 so $\phi(10) = 4$.

Any ring homomorphism fixing \mathbb{Q} (these are injective) will send a primitive 10th root of unity to another primitive 10th root of unity since otherwise it would send something nonzero to zero. Since all possible ring homomorphism images are accounted for, these are all the roots of the minimal polynomial of ζ over \mathbb{Q} which itself has no repeated roots.

Hence,

$$p(x) = (x - \zeta) \cdot (x - \zeta^3) \cdot (x - \zeta^7) \cdot (x - \zeta^9) \in \mathbb{Q}[x]$$

We also have that $p(x)$ is a factor of $x^{10} - 1$ since ζ is a root of both $p(x)$ and $x^{10} - 1$ and $p(x)$ is minimal. The polynomial $p(x)$ has a special name:

Cyclotomic Polynomial

A cyclotomic polynomial is a monic (i.e. leading coefficient is 1) *irreducible* polynomial factor in $\mathbb{Q}[x]$ of $x^n - 1$ for a positive integer n . The roots of a cyclotomic polynomial are all the primitive m th roots of unity for one integer m .

Use the following SageMath code to multiply out $p(x)$ to see what it is:



[Link to run the code.](#)

```
zeta=E(5) #E(5) means primitive 5th root of 1 in SageMath
expand((x-zeta)*(x-zeta^3)*(x-zeta^7)*(x-zeta^9))
```

The result is:

$$p(x) = x^4 - x^3 + x^2 - x + 1$$

Example 7. Another Cyclotomic Polynomial. Using ζ from the previous example, notice that ζ^2 is a primitive 5th root of unity. In fact, any time that we have ζ^{2k} where k shares no common factor with 10, we have a primitive 5th root of unity. Since powers of ζ repeat every 10, and 2 is a factor of 10, ζ^{2k} only ranges through 5 powers $k = 1, \dots, 5$. Only four of these where k shares no common factor with $\frac{10}{2} = 5$ yield primitive roots. That is, there are four values of $2k$ between 1 and 10 where the greatest common factor of $2k$ and 10 is 2 itself: k does not bring anything extra with it. These represent the four primitive 5th roots of unity. Note that $\phi(\frac{10}{2}) = 4$ can be used to count these.

Let d be a factor of n . Then, $\phi\left(\frac{n}{d}\right)$ computes how many primitive $\frac{n}{d}$ roots of unity there are. In particular, if ζ is a primitive n th root of unity, then this computes how many integers from 1 to n have a greatest common factor of d with n .

So, using ζ as a primitive 10th root of unity, we have that the four distinct roots of the minimal polynomial

of ζ^2 (all primitive 5th roots of unity) are:

$$\zeta^2, \zeta^4, \zeta^6, \zeta^8$$

This tells us:

$$q(x) = (x - \zeta^2) \cdot (x - \zeta^4) \cdot (x - \zeta^6) \cdot (x - \zeta^8) \in \mathbb{Q}[x]$$

In fact:

$$q(x) = x^4 + x^3 + x^2 + x + 1$$

Example 8. *Finishing off the cyclotomic polynomial factors of $x^{10} - 1$.* Using this same logic, there is $\phi(\frac{10}{5}) = \phi(2) = 1$ primitive second root of unity and it is given by ζ^5 where 5 is the unique integer from 1 to 10 whose greatest common factor with 10 is 5. The cyclotomic polynomial that has all of the primitive second roots is $x + 1$ which has a root of $-1 = \zeta^5$. *This is the one and only primitive second root of unity.*

Likewise, the cyclotomic polynomial that has the one and only one primitive first roots of unity is $x - 1$. The root is $1 = \zeta^{10}$ itself.

Cyclotomic Polynomial Factors of $x^{10} - 1$

$$x^{10} - 1 = (x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)(x + 1)(x - 1)$$

Wait! How do we know that there even exists a primitive root of unity for a given integer n ?

Theorem 9.2.22

There exists a primitive n th root of unity in \mathbb{C} .

Proof. We first show that the roots of $f(x) = x^n - 1$ are all distinct. Notice that the greatest common factor of $f(x) = x^n - 1$ with $f'(x) = nx^{n-1}$ is 1. This means that $a(x)f(x) + b(x)f'(x) = 1$ for some $a(x)$ and $b(x)$ so that both $f(x)$ and $f'(x)$ cannot share the same nontrivial factor. Otherwise, 1 would have a nontrivial factor. By the product rule, if there were a repeated factor in $f(x)$ so $f(x) = (x - \alpha)^2 q(x)$, then $f'(x) = 2(x - \alpha)q(x) + (x - \alpha)^2 q'(x)$ —that is, $f(x)$ and $f'(x)$ would be required to share a factor.

All roots of $x^n - 1$ are n th roots of unity. These make up a finite commutative multiplicative group of size n . This group considered as a \mathbb{Z} -module is of the form $\mathbb{Z}/a_1\mathbb{Z} \times \cdots \mathbb{Z}/a_r\mathbb{Z}$ where multiplication is replaced by addition and 1 is replaced with 0.

What if this product were $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$? Then from $\mathbb{Z}/6\mathbb{Z}$, we would have $(\underline{\textcolor{red}{0}}, \underline{\textcolor{green}{0}}), (\underline{\textcolor{red}{2}}, \underline{\textcolor{green}{0}})$ and

($\frac{1}{4}$, $\frac{1}{2}$) when multiplied by 3 will all be zero. When transformed to the elements these describe with addition replaced by multiplication, this is the same as saying that raising all three of these distinct elements to the third power results in the identity—these are 3 third roots of unity. But by the same token, ($\frac{1}{2}$, $\frac{1}{3}$), ($\frac{1}{2}$, $\frac{1}{6}$) are two more that are not accounted for. So there will be five third roots of unity. But wait! The polynomial $x^3 - 1$ cannot have more than three roots! So such a situation cannot occur.

Such a situation occurs if $\gcd(a_i, a_j) = k \neq 1$. Then there are k k th roots of unity coming from $\mathbb{Z}/a_i\mathbb{Z}$ and *different* ones coming from $\frac{a_j}{k} \cdot \mathbb{Z}/a_j\mathbb{Z}$. Yet, the polynomial $x^k - 1$ cannot have more than k roots. This is a contradiction. Hence the a_i share no nontrivial factors.

By the Chinese remainder theorem, this means that our \mathbb{Z} -module form becomes $\mathbb{Z}/(a_1 \cdots a_r)\mathbb{Z}$ which is generated additively by a single element $\frac{1}{1}$. Since the size of this group is n , $n = a_1 \cdots a_r$. Translating back to multiplication, $\frac{1}{1}$ itself traces back to our primitive n th root of unity. \square

If we have one primitive j th root, we automatically have $\phi(j)$ coming with it. From our discussion above, $\phi(\frac{n}{d})$ where d is a factor of n counts how many numbers 1 to n have greatest common factor d with n . Every integer 1 to n has exactly one unique greatest common factor with n . Hence,

$$n = \sum_{d=\text{factor of } n} \phi\left(\frac{n}{d}\right) = \sum_{j=\text{factor of } n} \phi(j)$$

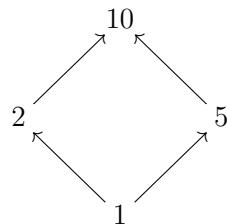
noting that $j = \frac{n}{d}$ runs through all of the factors of n . Since each factor j of n gives at least one primitive j th root, it gives $\phi(j)$ primitive j th roots for sure. It can give no more since the sum of the $\phi(j)$'s already is n and there are no more than n n th roots.

Theorem 9.2.23

There are precisely $\phi(n)$ primitive n th roots of unity in \mathbb{C} .

9.2.5 A Linear Transformation that Counts what is Primitive

The idea of “counting what is primitive” when talking about roots of unity can be done via a linear transformation. Consider the example of the last subsection of finding the roots of unity that are powers of ζ where ζ is a primitive 10th root. Produce a diagram of factors of 10 where “ \rightarrow ” is used to denote the relationship “is a factor of.”



We can think of these numbers as not simply denoting factors of 10 but the different types of roots of unity (of 1) we can have. There are precisely 10 distinct 10th roots of unity but not all of them all primitive. Some are

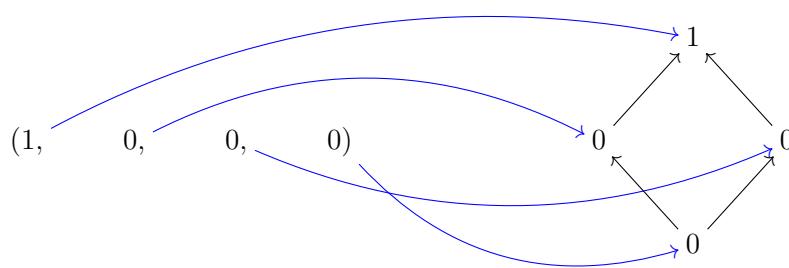
5th roots and some are second roots and one is a first root. There are 5 distinct 5th roots and 2 distinct second roots and 1 distinct first roots—not all of these are primitive. So, the question is:

How do we go from what is not necessarily primitive, to what is primitive?

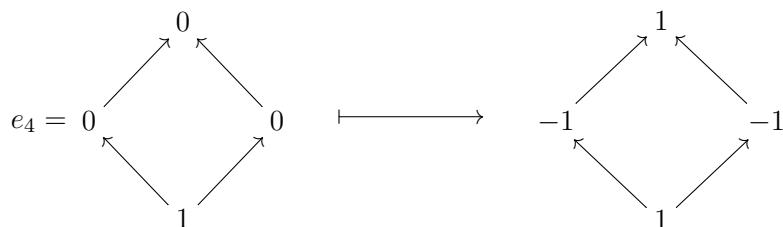
We can do so with a linear transformation—knowing where certain “standard basis vectors” go.

We can think of what is not necessarily primitive as the sum of everything primitive below and up to that point.

If we replace the entries in the “is a factor of” diagram with 0’s and just one 1, and find what is primitive for that diagram, we have found the destination of a standard basis vector. Collect these destinations into a matrix and we can compute what is primitive given *any beginning numbers* on our diagram. The matrix is what we call a *Möbius matrix*. Concretely, think of a standard basis vector as:



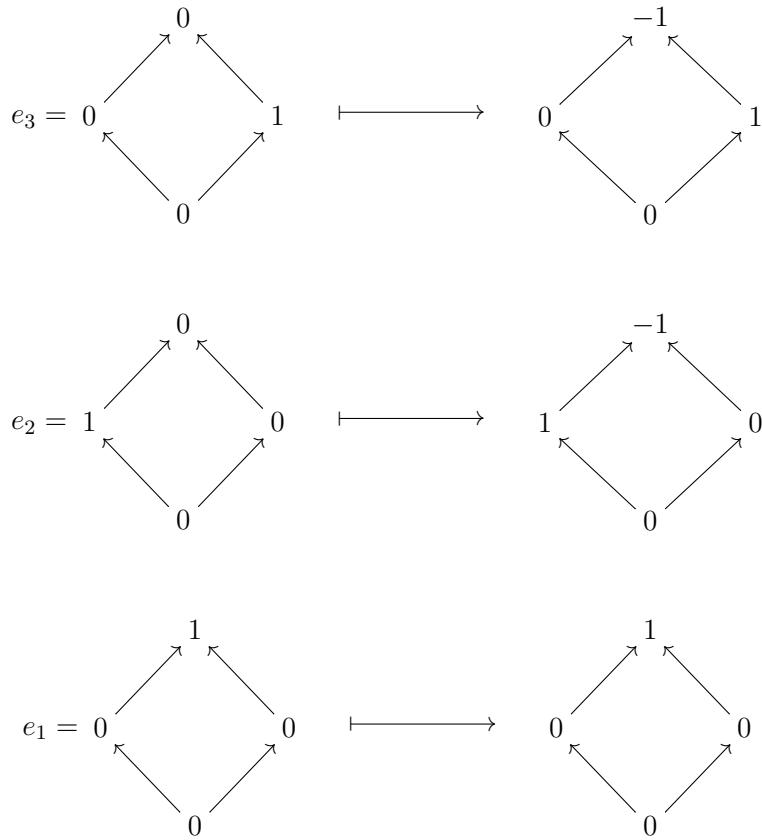
In the following, we are pretending that the standard basis construction of 0’s and a 1 gives us things that are *not necessarily primitive* with respect to our diagram. Then, we send each standard basis construction to the corresponding primitive construction where the sum of what is primitive up to and including a point should equal the entry of the standard basis vector. *Verify that these are the unique corresponding primitive constructions!*



Explanation of the Primitive Construction Destination

Consider this destination of e_4 . Notice that the sum of all of its entries $1 + (-1) + (-1) + 1$ is 0. This 0 corresponds to the top entry on in the standard basis construction.

Notice also that in the destination the sum of the bottom 1 and the -1 on the left is 0. This corresponds to the left-most 0 entry in e_4 .



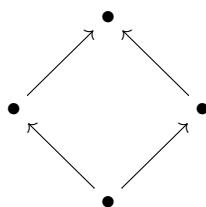
Let $f : \mathbb{R}^4 \rightarrow \mathbb{R}^4$ be the function that finds primitive constructions in relation to our structure. Then, we can write

$$\begin{aligned} f(e_1) &= (1, 0, 0, 0) \\ f(e_2) &= (-1, 1, 0, 0) \\ f(e_3) &= (-1, 0, 1, 0) \\ f(e_4) &= (1, -1, -1, 1) \end{aligned}$$

We can therefore express f as the matrix:

$$\begin{pmatrix} f(e_1) & f(e_2) & f(e_3) & f(e_4) \end{pmatrix} = \begin{pmatrix} 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

This is the Möbius matrix associated with our structure



Therefore, we can count the number of primitive roots of unity via:

$$f(10, 2, 5, 1) = \begin{pmatrix} 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 10 \\ 2 \\ 5 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \\ 4 \\ 1 \end{pmatrix}$$

Notice that this perfectly matches up with the numbers of primitive 10th roots, second roots, 5th roots and first roots!

This is just an alternative approach to using $\phi(10) = 4$, $\phi(2) = 1$, $\phi(5) = 4$, $\phi(1) = 1$. Both ways count something that is primitive.

There is a number theoretic function μ used to get the top row of the Möbius matrix. The top row of the matrix can be expressed as

$$\left(\mu\left(\frac{10}{10}\right) \quad \mu\left(\frac{10}{2}\right) \quad \mu\left(\frac{10}{5}\right) \quad \mu\left(\frac{10}{1}\right) \right)$$

where

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ has a square factor} \\ (-1)^k & \text{otherwise where } k \text{ is the number of distinct prime divisors of } n \end{cases}.$$

To learn more about this and other applications of Möbius matrices see [1].

Key Concepts from this Section

- **field:** (page 1077) A field is an additive commutative group with respect to $+$. There is a multiplication operation defined such that with 0 omitted, we have a multiplicative group. The multiplication is commutative and distributes over addition.
- **multiplicative inverse:** (page 1077) The multiplicative inverse of an element a is the element b such that $a \cdot b = b \cdot a$ is the multiplicative identity 1.
- **ring:** (page 1077) A ring is like a field except elements are not required to have multiplicative inverses in the ring.
- **subfield:** (page 1077) Given two fields F_1 and F_2 , if $F_1 \subset F_2$, then we say that F_1 is a *subfield* of F_2 .
- **field extension:** (page 1077) Given two fields F_1 and F_2 , if $F_1 \subset F_2$, then we say that F_2 is a *field extension* of F_1 .
- **finiteness convention:** (page 1077) Unless otherwise indicated, we assume that all field extensions (except \mathbb{C}) in what follows are finite dimensional \mathbb{Q} -vector spaces.

- **$\mathbb{Q}(\alpha)$:** (page 1078) The field $\mathbb{Q}(\alpha)$ is the smallest field containing both \mathbb{Q} and α .
- **simple algebraic field extension:** (page 1078) We call a field extension $\mathbb{Q}(\alpha)$ of \mathbb{Q} where α is the root of a polynomial in $\mathbb{Q}[x]$ a *simple algebraic field extension of \mathbb{Q}* . We can replace \mathbb{Q} with any field F letting α denote a root of a polynomial in $F[x]$. Then $F(\alpha)$ is a *simple algebraic field extension of F* .
- **theorem 9.2.1 :** (page 1079) Take an irreducible polynomial $p(x)$ in $\mathbb{Q}[x]$ that has α as a root. Then $\mathbb{Q}(\alpha)$ is isomorphic to the quotient $\mathbb{Q}[x]/p(x)\mathbb{Q}[x]$.
- **monic polynomial:** (page 1079) Any polynomial whose leading coefficient is 1 is called a *monic polynomial*.
- **minimal polynomial:** (page 1079) Rescale the irreducible polynomial $p(x)$ that has α as its root to be a monic polynomial. Then, this polynomial is called the minimal polynomial of α .
- **theorem 9.2.2 :** (page 1079) The field $\mathbb{Q}(\alpha)$ is a \mathbb{Q} -vector space with dimension n where $n = \deg(p(x))$.
- **theorem 9.2.3 :** (page 1080) Using our notation, the set of elements $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ makes up a basis for the \mathbb{Q} -vector space $\mathbb{Q}(\alpha)$.
- **algebraic number:** (page 1080) An algebraic number over \mathbb{Q} is any root of any polynomial in $\mathbb{Q}[x]$. Generally, an algebraic number over a field F is any root of any polynomial in $F[x]$.
- **theorem 9.2.4 :** (page 1080) All elements in $\mathbb{Q}(\alpha)$ where α is an algebraic number are algebraic numbers. The field \mathbb{Q} may be replaced with any field F so that we can say that all elements in $F(\alpha)$ where α is an algebraic number over F will also be algebraic numbers!
- **minimal polynomial of element and matrix:** (page 1080) The minimal polynomial of an element in an algebraic number field and the minimal polynomial of the matrix which describes multiplication by that element as a vector space isomorphism are the same.
- **algebraic integers \mathcal{O}_K :** (page 1080) Any element of an algebraic number field that admits a minimal polynomial in $\mathbb{Z}[x]$ is called an *algebraic integer*. We often use \mathcal{O}_K to denote the algebraic integers in $K = \mathbb{Q}(\alpha)$.
- **lemma 9.2.5 :** (page 1081) If an element is a root of a polynomial in $\mathbb{Z}[x]$, then its minimal polynomial is also in $\mathbb{Z}[x]$.
- **corollary 9.2.6 :** (page 1082) The only monic factors in $\mathbb{Q}[x]$ of a monic polynomial in $\mathbb{Z}[x]$ are again in $\mathbb{Z}[x]$.
- **theorem 9.2.7 :** (page 1082) The set \mathcal{O}_K is a ring.
- **algebraic field extension:** (page 1083) A field K is called an algebraic field extension of a field F if it is the smallest field containing both F and a collection of algebraic numbers over F .

- **$\mathbb{Q}(\alpha, \beta)$:** (page 1083) The field $\mathbb{Q}(\alpha, \beta)$ is the algebraic field extension of \mathbb{Q} formed by adjoining α and β .
- **primitive element:** (page 1083) Given an algebraic field extension K of F , an element $\gamma \in K$ is called a primitive element of the extension if $K = F(\gamma)$.
- **fundamental theorem of algebra:** (page 1083) Every degree n polynomial in $\mathbb{C}[x]$ has exactly n roots in \mathbb{C} counting multiplicity.
- **theorem 9.2.8 primitive element theorem:** (page 1084) The field $\mathbb{Q}(\alpha, \beta)$ is equal to $\mathbb{Q}(\gamma)$ for an algebraic number γ . In particular, any algebraic field extension formed from a subfield F of \mathbb{C} by adjoining a finite number of algebraic numbers is a *simple algebraic field extension* formable by adjoining a *single* element.
- **theorem 9.2.9 :** (page 1085) Given $\gamma \in \mathbb{C}$ that is the root of a monic polynomial $p(x)$ in $\mathbb{Q}[x]$, then there are exactly n distinct ring homomorphisms $\mathbb{Q}(\gamma) \rightarrow \mathbb{C}$ that fix all the elements of \mathbb{Q} .
- **theorem 9.2.10 :** (page 1086) A ring homomorphism $\phi : \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ that fixes all of the elements of \mathbb{Q} is injective.
- **normal field extension:** (page 1086) A normal field extension K of F such that $F \subset K \subset \mathbb{C}$ is one such that all of the ring homomorphisms $K \rightarrow \mathbb{C}$ have range in K . That is, they can be thought of as functions $K \rightarrow K$.
- **theorem 9.2.11 :** (page 1087) Suppose that $F(\alpha) \subset \mathbb{C}$ is an algebraic field extension of F . Then, adjoining all of the roots of the minimal polynomial of α in $F[x]$ produces a normal field extension of F .
- **normal closure:** (page 1087) Given an algebraic field extension $F(\alpha)$ of F , if we adjoin all of the roots of the minimal polynomial of α we get a new field K which we have just seen is normal. We call K the normal closure of the field $F(\alpha)$.
- **theorem 9.2.12 :** (page 1087) Suppose that $F \subset K \subset \mathbb{C}$ are fields and that K is the normal closure of F . Let ϕ be a ring homomorphism $K \rightarrow K$ that fixes all of the elements of F . Then ϕ is an isomorphism.
- **automorphism:** (page 1087) An isomorphism $K \rightarrow K$ where the domain is the same as the codomain is called an automorphism.
- **galois group:** (page 1088) Given a normal field extension K of F , such that both are subfields of \mathbb{C} , the group of automorphisms $K \rightarrow K$ that fix F with the operation of composition is called the *Galois Group* of K over F .
- **theorem 9.2.13 fundamental theorem of galois theory:** (page 1088) We only give part of the actual theorem—there is a bijective correspondence between the fields L such that $F \subset L \subset K \subset \mathbb{C}$ and the subgroups of the Galois group G of the normal extension K of F .

- **corollary 9.2.14 :** (page 1088) The dimension of K as a vector space with coefficients in K^H is the same as the size of the subgroup H of G .
- **corollary 9.2.15 :** (page 1089) In the correspondence, if $H_1 \subset H_2 \subset G$, then $K^{H_1} \supset K^{H_2} \supset L$ where $L = K^G$. The correspondence is inclusion reversing.
- **theorem 9.2.16 :** (page 1090) Consider fields $F \subset L \subset K$. We can think of L as $F(\alpha)$ for some α and K as $L(\beta)$ for some β . Suppose that the minimal polynomial of α in $F[x]$ has degree m and the minimal polynomial of β in $F(\alpha)[x]$ has degree r . the dimension of K as a F -vector space is mr .
- **normal subgroup:** (page 1090) A subgroup of a group G is normal when the set of left cosets denoted as the quotient G/H (or the set of just right cosets denoted as $H\backslash G$) is itself a group. The group operation \star is given by:

$$(g_1H) \star (g_2H) = g_1Hg_2H = (g_1g_2) \cdot H$$

- **theorem 9.2.17 :** (page 1090) In our Galois subgroup to field correspondence, the subfield is normal precisely when the subgroup is normal.
- **cauchy's theorem special case:** (page 1091) Every group with an even number of elements has at least one of them where $g^2 = \text{id}$.
- **the size of conjugacy classes:** (page 1091) The size of a conjugacy class as described above is a factor of the number of elements of the group.
- **first 2-sylow theorem:** (page 1093) Every finite group of size $2^m t$ where t is odd has a subgroup of size 2^m .
- **corollary 9.2.18 :** (page 1093) Groups of size 2^m have subgroups of size 2^{m-1} .
- **theorem 9.2.19 :** (page 1094) Suppose that $K = F(\gamma)$ where F is either \mathbb{Q} or an extension of it and γ is an algebraic number over F . Let A be the matrix which gives the multiplication action of γ on K as a F -vector space with respect to some basis. Then, A is diagonalizable and it has n distinct eigenvalues representing the n distinct roots of its minimal polynomial where n is the dimension of K as a F -vector space. The same matrix U that diagonalizes the matrix A as $D = U^{-1}AU$ also diagonalizes the matrices for the multiplication action of every other element of K .
- **corollary 9.2.20 :** (page 1094) The matrices representing the multiplication action of any element in an algebraic field extension K over F where F is either \mathbb{Q} or an extension of it all share the same eigenvectors. The eigenvalues associated to those eigenvectors may change, but the idea of being an eigenvector carries over perfectly from one of these matrices to another.
- **corollary 9.2.21 :** (page 1096) If $K = F(\gamma)$ is an algebraic field extension of dimension n (where F is an extension of \mathbb{Q}), the n ring homomorphisms ϕ_1, \dots, ϕ_n given as $K \rightarrow \mathbb{C}$ can be described by the following:

- Let U diagonalize the matrix A representing the multiplication action of K as a F -vector space of γ with respect to some basis.
- Represent an element $\beta \in K$ as the matrix M_β of its multiplication action on K as a F -vector space with respect to the same basis.
- Compute $U^{-1}BU$.
- Then, $\phi_i(\beta)$ is the i th diagonal entry of $U^{-1}M_\beta U$.

That is,

$$\phi_i(\beta) = e_i^T U^{-1} M_\beta U e_i$$

If K is a normal field extension, these give the automorphisms $K \rightarrow K$ in the Galois group of K over F .

- **trace in an algebraic field extension:** (page 1097) We define the trace of an element $k \in K$ of an algebraic field extension K over F (of finite dimension over F where K and F are subfields of \mathbb{C}) as being the trace of any matrix B representing its multiplication action over K as a vector space over F . From what we have above, this is equivalent to the sum of diagonal entries $U^{-1}BU$ which is the sum

$$\sum_i \phi_i(k)$$

for the n ring homomorphisms $K \rightarrow \mathbb{C}$.

- **norm in an algebraic field extension:** (page 1097) We define the norm of an element $k \in K$ of an algebraic field extension K over F (of finite dimension over F where K and F are subfields of \mathbb{C}) as being the trace of any matrix B representing its multiplication action over K as a vector space over F . From what we have above, this is equivalent to the product of diagonal entries $U^{-1}BU$ which is the product

$$\prod_i \phi_i(k)$$

for the n ring homomorphisms $K \rightarrow \mathbb{C}$.

- **primitive root of unity:** (page 1098) Such a ζ is called a primitive 10th root of unity (i.e. 1).
- **cyclotomic polynomial:** (page 1098) A cyclotomic polynomial is a monic (i.e. leading coefficient is 1) irreducible polynomial factor in $\mathbb{Q}[x]$ of $x^n - 1$ for a positive integer n . The roots of a cyclotomic polynomial are all the primitive m th roots of unity for one integer m .
- **theorem 9.2.22 :** (page 1105) There exists a primitive n th root of unity in \mathbb{C} .
- **theorem 9.2.23 :** (page 1106) There are precisely $\phi(n)$ primitive n th roots of unity in \mathbb{C} .

9.2.6 Exercises

Using Code to Compute Galois Groups

Modify the code of this section to compute the Galois groups of the following normal field extensions of \mathbb{Q} . List the effect of each automorphism on ζ .

1. $\mathbb{Q}(\zeta)$ where ζ is a primitive 5th root of unity.
2. $\mathbb{Q}(\zeta)$ where ζ is a primitive 12th root of unity.
3. $\mathbb{Q}(\zeta)$ where ζ is a primitive 15th root of unity.

9.2.7 Solutions

1. The four automorphisms are given by $\zeta \mapsto \zeta$, $\zeta \mapsto \zeta^2$, $\zeta \mapsto \zeta^3$, and $\zeta \mapsto \zeta^4$.
2. The four automorphisms are determined by sending ζ to each one of ζ , ζ^5 , ζ^7 , ζ^{11} .
3. The eight automorphisms are determined by sending ζ to each one of ζ , ζ^2 , ζ^4 , ζ^7 , ζ^8 , ζ^{11} , ζ^{13} , ζ^{14} .

Factorization of Integers

9.3

Using Field Extensions

9.3.1 A Bilinear Map and Rings of Integers.	1119
9.3.2 How to Find Factors in \mathcal{O}_K	1129
9.3.3 Factorization into Ideals	1134
9.3.4 More on Repetitions in Ideal Factorization.	1146
9.3.5 Quadratic Reciprocity	1148
9.3.6 Sums of Squares	1152
9.3.7 Using Squares in Modular Arithmetic to Factor Large Numbers	1156
9.3.8 General Number Field Sieve	1161

Questions to Guide Your Study:

- *How can we use traces to build a bilinear map from our field extension to \mathbb{Q}^n ?*
- *What information does this trace map give us about the ring of integers?*
- *What are ideals? How can they be used with factorization?*
- *What information does our trace map give us about how ideals factor into prime ideals?*
- *How does ideal factorization help think about when a prime is a sum of two squares?*
- *How does ideal factorization help think about how p being a square mod q is related to q being a square mod p ?*
- *What are some algorithms and code that use field extensions to factor numbers?*

9.3.1 A Bilinear Map and Rings of Integers.

We are going to find a bilinear map on field extensions which allows us to study rings of integers and even say something about how things factor in them.

Consider the field extension $\mathbb{Q}(i)$ of \mathbb{Q} . The minimal polynomial of i is $x^2 + 1$. The vector space $\mathbb{Q}(i)$ is two-dimensional over \mathbb{Q} with a basis of $\{1, i\}$. We can compute the trace of an element in $\mathbb{Q}(i)$ by taking the trace of the matrix which represents its multiplication action. The multiplication action of i is given by the matrix

$$i : \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

since $i \cdot 1 = i$ means that 1 (thought of as e_1) is sent to i (thought of as e_2) and $i \cdot i = -1$ means that i (thought of as e_2) is sent to -1 (thought of as $-e_1$). The trace of this matrix is 0. The trace of the matrix for 1 which is

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

is 2.

Now, from this trace information we can build a bilinear map

$$T : \mathbb{Q}(i) \times \mathbb{Q}(i) \rightarrow \mathbb{Q} \quad (a, b) \mapsto \text{tr}(a \cdot b)$$

Multiplication itself is bilinear. Taking a trace of the sum of two matrices is the same as taking the trace of each and then adding them—that is, taking a trace is *additive*. Fixing a then causes $b \mapsto \text{tr}(a \cdot b)$ to still be a linear map and similarly when we fix b , $a \mapsto \text{tr}(a \cdot b)$ is a linear map.

Hence, T , as a *bilinear map*, can be represented by a 2×2 matrix as follows:

$$T : \begin{pmatrix} \text{tr}(1 \cdot 1) & \text{tr}(1 \cdot i) \\ \text{tr}(i \cdot 1) & \text{tr}(i \cdot i) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

Trace Bilinear Form

Let K be a field extension of \mathbb{Q} of finite dimension. We define the trace form $T : K \times K \rightarrow \mathbb{Q}$ to be the map $(a, b) \mapsto \text{tr}(a \cdot b)$ where we take the trace of any matrix representing the multiplication action of (ab) thought of as a map $K \rightarrow K$.

Any basis for K over \mathbb{Q} will yield the same *trace* function tr since the characteristic polynomial of the matrix for ab remains the same under a change of basis. *Changing the basis could however change the characteristic polynomial of the bilinear matrix for T . Yet the actual function T itself will remain unaltered because it represents a result of tr which remains unaltered!*

Changing the Basis of a Bilinear form

Suppose that the matrix A represents a bilinear transformation T having a column input and a row input. Then suppose that U is the “unpretending matrix” for a new basis. Then

$$U^T A U$$

represents the bilinear transformation with respect to this new basis.

Proof. Suppose that $v \in \mathbb{Q}^2$ and $w \in \mathbb{Q}^2$ represent $a \in K$ and $b \in K$ with respect to the new basis of K over \mathbb{Q} . Then Uv and Uw represent a and b with respect to the old basis. So, using the matrix A , which is written with respect to the old basis:

$$\begin{aligned} T(a, b) &= \underbrace{(Uv)^T}_{\text{row input}} \cdot A \cdot \underbrace{(Uw)}_{\text{column input}} \\ &= v^T \cdot \underbrace{U^T A U}_{\text{new matrix}} \cdot w \end{aligned}$$

□

In particular, the determinant of the matrix for T could change upon a change of basis!

We call the determinant of the matrix for T with respect to a basis \mathcal{B} the *discriminant* of the basis \mathcal{B} .

Discriminant of a Basis

Let K be a field extension of \mathbb{Q} of finite dimension and suppose that $\mathcal{B} = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is a basis for K over \mathbb{Q} . Then, we define the discriminant of \mathcal{B} to be the determinant of the trace bilinear form $(a, b) \mapsto \text{tr}(ab)$ written as a $n \times n$ bilinear matrix with respect to the basis \mathcal{B} in both inputs.

Example 1. The discriminant of the basis $\{1, i\}$ for $\mathbb{Q}(i)$ over \mathbb{Q} is:

$$\det \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 4$$

The matrix for T can also be used as just an ordinary linear transformation considered in just a column interpretation.

Let

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

be the matrix for T . Then A under a column interpretation represents a map with domain K , written with respect to the \mathbb{Q} -basis $\{1, i\}$ and output \mathbb{Q}^2 . For instance, A acting on $\frac{1}{2} - i$ is given by:

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} \frac{1}{2} \\ -1 \end{pmatrix}}_{\frac{1}{2} - i} = \underbrace{\begin{pmatrix} 1 \\ -2 \end{pmatrix}}_{\in \mathbb{Q}^2}$$

If we are going to think about how things factor in $\mathbb{Q}(i)$, we need to be thinking of things analogous to integers. We use the ring of integers $\mathcal{O}_{\mathbb{Q}(i)}$.

Let's recall that the ring of integers $\mathcal{O}_{\mathbb{Q}(i)}$ is the set of all elements of $\mathbb{Q}(i)$ whose minimal polynomials are in $\mathbb{Z}[x]$.

Theorem 9.3.1

If $a \in \mathcal{O}_K$, the ring of integers of K , then $\text{tr}(a) \in \mathbb{Z}$.

Proof. The characteristic polynomial of a has the same set of irreducible factors as the minimal polynomial of a which itself is in $\mathbb{Z}[x]$ by virtue of a being an algebraic integer. A monic polynomial in $\mathbb{Z}[x]$ cannot factor into irreducibles that themselves are not in $\mathbb{Z}[x]$ by a result in the previous section. So, these factors are in $\mathbb{Z}[x]$ thus forcing the characteristic polynomial to be in $\mathbb{Z}[x]$. Hence, the trace of an algebraic integer (*remember that the trace is a coefficient of the characteristic polynomial*) is always in \mathbb{Z} . \square

This shows that the column interpretation map g of T defines a \mathbb{Z} -module homomorphism:

$$g : \mathcal{O}_{\mathbb{Q}(i)} \rightarrow \mathbb{Z}^2$$

That is, the output of any algebraic integer will be in \mathbb{Z}^2 . Notice that since $\mathcal{O}_{\mathbb{Q}(i)}$ is a ring, $\mathbb{Z} + \mathbb{Z} \cdot i \subset \mathcal{O}_{\mathbb{Q}(i)}$ and 1 and i are linearly independent over \mathbb{Z} . So $\mathcal{O}_{\mathbb{Q}(i)}$ contains a \mathbb{Z} -submodule of free \mathbb{Z} -rank 2. Also, notice in our case that g represents an injection since its matrix has nonzero determinant (the discriminant of the basis $\{1, i\}$). Hence, the image $g(\mathcal{O}_{\mathbb{Q}(i)})$ contains a submodule of \mathbb{Z}^2 of free \mathbb{Z} -rank 2.

It turns out that

$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z} + \mathbb{Z} \cdot i$$

so that $g(\mathcal{O}_{\mathbb{Q}(i)})$ is this free \mathbb{Z} -rank 2 submodule of \mathbb{Z}^2 . To see this, we take an arbitrary element of $\mathbb{Q}(i)$ such as $a + bi$ and consider its multiplication action matrix in column interpretation with respect to the basis $\{1, i\}$:

$$a + bi : \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

The first column represents the image of 1 and the second the image of i when we multiply by $a + bi$.

To require the characteristic polynomial to be in $\mathbb{Z}[x]$, we require its coefficients to be in \mathbb{Z} . Since this is a 2×2 matrix, we need the trace which is $2a$ and the determinant $a^2 + b^2$ to both be in \mathbb{Z} . Thus, $a = \frac{\tilde{a}}{2}$ for some $\tilde{a} \in \mathbb{Z}$. Also:

$$a^2 + b^2 = \left(\frac{\tilde{a}}{2}\right)^2 + b^2 = \frac{\tilde{a}^2}{4} + b^2 = \frac{\tilde{a}^2 + 4b^2}{4} \in \mathbb{Z}$$

This means that $\tilde{a}^2 + 4b^2$ is divisible by 4 so that \tilde{a}^2 is divisible by 4. This implies that \tilde{a} is divisible by 2 so that $a = \frac{\tilde{a}}{2} \in \mathbb{Z}$. Yet this forces $b^2 \in \mathbb{Z}$ so that $b \in \mathbb{Z}$. This means that the only way for $a + bi$ to be in $\mathcal{O}_{\mathbb{Q}(i)}$ is for $a + bi \in \mathbb{Z} + \mathbb{Z} \cdot i$. That is, $\mathcal{O}_{\mathbb{Q}(i)} \subset \mathbb{Z} + \mathbb{Z} \cdot i$. We already saw that $\mathcal{O}_{\mathbb{Q}(i)} \supset \mathbb{Z} + \mathbb{Z} \cdot i$.

Theorem 9.3.2

We have a description of the ring of integers of $\mathbb{Q}(i)$:

$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z} + \mathbb{Z} \cdot i$$

Gaussian Integers

We call the ring of integers of $\mathbb{Q}(i)$ the *Gaussian Integers*. It is the set $\mathbb{Z} + \mathbb{Z} \cdot i$.

In particular, the column interpretation map g of the matrix for T with respect to the domain basis $\{1, i\}$ represents a map $\mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ where the \mathbb{Z}^2 of the domain perfectly represents $\mathcal{O}_{\mathbb{Q}(i)}$. That is, all the elements of $\mathcal{O}_{\mathbb{Q}(i)}$ can be described by an ordered pair in \mathbb{Z}^2 . For instance, $3 + 4i \in \mathcal{O}_{\mathbb{Q}(i)}$ can be represented as $(3, 4) \in \mathbb{Z}^2$.

The number of cosets of $g(\mathcal{O}_{\mathbb{Q}(i)})$ in \mathbb{Z}^2 can give us valuable information. Since the matrix for g has determinant 4 (i.e. this is the discriminant of the basis $\{1, i\}$), then there are 4 cosets of $g(\mathcal{O}_{\mathbb{Q}(i)})$ in \mathbb{Z}^2 . Since $(2, 0)$ and $(0, 2)$ are the columns of the matrix for g , then:

$$g(\mathcal{O}_{\mathbb{Q}(i)}) = \mathbb{Z} \cdot (2, 0) + \mathbb{Z} \cdot (0, 2)$$

$$\mathbb{Z}/((2\mathbb{Z}, 0) + (0, 2\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

We will soon see that an integer prime dividing our determinant of 4 is the only kind of prime that will have a “nontrivial” square factor in the ring of integers $\mathcal{O}_{\mathbb{Q}(i)}$.

Theorem 9.3.3

Let \mathcal{B} be a basis for K (a field which is finite dimensional) over \mathbb{Q} such that \mathcal{B} is also a generating set over \mathbb{Z} for \mathcal{O}_K . Then if p is a prime which is not a factor of the discriminant of B , then p cannot have α^2 as a factor for any *nonunit* (explained below) $\alpha \in \mathcal{O}_K$. On the other hand, if p is a factor of the discriminant, then such a factorization of α^2 is possible.

Example 2. For instance, 2 is a factor of 4 and

$$2 = (1 + i)^2 \cdot (-i)$$

Notice that $-i$ has a multiplicative inverse of i in $\mathcal{O}_{\mathbb{Q}(i)}$. We call $-i$ a *unit* in the ring of integers. We could call it a *Gaussian unit*.

Unit in a Ring

An element u of a ring R is called a unit of R if u has a multiplicative inverse $u^{-1} \in R$.

The number $1 + i$ does not have an inverse in $\mathcal{O}_{\mathbb{Q}(i)}$. In fact, its norm, which is defined as the determinant of its multiplication action is $1^2 + 1^2$ using our $a^2 + b^2$ description above. Determinants multiply as matrices multiply and the determinants of the matrices describing algebraic integers are integers. Since this determinant is 2, it is primitive—it could not have come from anything whose determinant is ± 1 (which only happens for units). In fact, we say that $1 + i$ is a *prime Gaussian integer*—it can not be factored more into other primes.

Prime Gaussian Integer

Let $a + bi \in \mathcal{O}_{\mathbb{Q}(i)}$. Then $a + bi$ is a prime Gaussian integer if and only if its only factorizations can be expressed as units multiplied to $a + bi$. In particular, though not necessary, this happens when $a^2 + b^2$, the norm of $a + bi$ in the field extension $\mathbb{Q}(i)$ over \mathbb{Q} , is a prime number.

So, 2 factors as a Gaussian unit $(-i)$ multiplied by the square of the Gaussian prime $1 + i$.

Questions to Explore

Why does the discriminant tell us whether a number can have a square factor in the ring of integers? What techniques can we use to see how prime numbers factor into rings of integers?

Let's look at another example of a field extension and build up some ideas that can help us see.

Example 3. Consider the field $\mathbb{Q}(\sqrt{5})$. Let's consider the map

$$\mathbb{Q}(\sqrt{5}) \times \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{Z}^2$$

which comes from the column interpretation of the bilinear transformation

$$T : \mathbb{Q}(\sqrt{5}) \times \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{Q}(\sqrt{5})$$

given by $(a, b) \mapsto \text{tr}(a \cdot b)$. We need to choose a basis with respect to which we will write our matrix. Let's choose algebraic integers.

Before we do so, let's illustrate how you can find an algebraic *integer* from an algebraic *number*. For instance, suppose that we have an algebraic number like

$$w = \frac{1 + \sqrt{5}}{4}$$

Let's find a monic polynomial which has w as its root. We set:

$$\begin{aligned} x = \frac{1 + \sqrt{5}}{4} &\implies 4x - 1 = \sqrt{5} \implies (4x - 1)^2 = 5 \implies 16x^2 - 8x + 1 = 5 \implies \\ 16x^2 - 8x - 4 &= 0 \implies x^2 - \frac{1}{2}x - \frac{1}{4} \end{aligned}$$

Take this polynomial and multiply it by 4 to have:

$$4x^2 - 2x - 1 = 0$$

Now, group this as $(2x)^2 - (2x) - 1 = 0$ to see that $2w = \frac{1+\sqrt{5}}{2}$ is an algebraic integer. This is just an example of the following:

Theorem 9.3.4

Every algebraic number is only a multiple of \mathbb{Z} away from an algebraic integer.

Let's see how things work when we use the basis $\{1, \frac{1+\sqrt{5}}{2}\}$ for $\mathbb{Q}(\sqrt{5})$ as a \mathbb{Q} vector space in order to

describe our matrix for T . We compute the images of the map T on pairs of basis elements:

$$T\left(1, \frac{1+\sqrt{5}}{2}\right) = \text{tr}\left(1 \cdot \frac{1+\sqrt{5}}{2}\right)$$

For this example, *to show an alternate technique to compute the trace* we appeal to the Galois group of $\mathbb{Q}(\sqrt{5})$ over \mathbb{Q} . We can do this since the field $\mathbb{Q}(\sqrt{5})$ contains all of the roots of $x^2 - 5$ so that it is a normal extension. There are only two automorphisms. Let ϕ_1 be the one which maps $\sqrt{5} \mapsto \sqrt{5}$ and ϕ_2 the one which maps $\sqrt{5} \mapsto -\sqrt{5}$.

To compute the trace of an element a in this extension is the same as computing $\phi_1(a) + \phi_2(a)$ as was given in a result in the last section if ϕ_1 and ϕ_2 are the two automorphisms of the Galois group.

So to continue our example, we have:

$$\text{tr}\left(1 \cdot \frac{1+\sqrt{5}}{2}\right) = \frac{1+\sqrt{5}}{2} + \frac{1-\sqrt{5}}{2} = 1$$

We also compute:

$$\begin{aligned} T(1, 1) &= \phi_1(1) + \phi_2(1) = 1 + 1 = 2 \\ T\left(\frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\right) &= \text{tr}\left(\frac{1+2\sqrt{5}+5}{4}\right) = \underbrace{\frac{6+2\sqrt{5}}{4}}_{\phi_1} + \underbrace{\frac{6-2\sqrt{5}}{4}}_{\phi_2} \end{aligned}$$

Putting these into the bilinear matrix for T , we have:

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

This has determinant 5.

Now let's suppose that we change the basis $\{1, \frac{1+\sqrt{5}}{2}\}$ to another one via a matrix U so that the *bilinear* matrix for T would read as

$$U^T A U$$

since $T(u, v)$ is now being written as

$$T(Uu, Uv) = (Uu)^T A (Uv) = u^T \underbrace{U^T A U}_{\substack{\text{bilinear form} \\ \text{with respect to} \\ \text{new basis}}} v$$

The columns of U represent the new basis in terms of the old basis $\{1, \frac{1+\sqrt{5}}{2}\}$.

Suppose that the new basis consists of algebraic integers. What if

$$\mathcal{O}_{\mathbb{Q}(\sqrt{5})} \stackrel{?}{=} \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{1 + \sqrt{5}}{2}$$

This would mean that the columns of U would live in \mathbb{Z}^2 .

So, the determinant of $U^T A U$ would be

$$\underbrace{\det(U^T) \cdot \det(A) \cdot \det(U)}_{=\det(U)} = \det(U)^2 \cdot \det(A)$$

Since the column entries of U are in \mathbb{Z} , then $c = \det(U) \in \mathbb{Z}$ and $\det(U)^2 = c^2$.

We can expect that the matrix for T with respect to the new basis has a *square integer factor*.

Wait! The determinant of our matrix A representing T is 5: *it has no square factors!* This automatically guarantees that the basis we chose has $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ as its \mathbb{Z} -span. We have just shown that:

$$\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{1 + \sqrt{5}}{2}$$

Theorem 9.3.5

Let \mathcal{B} be a basis for K (a field which is finite dimensional) over \mathbb{Q} such that it has a discriminant which is square-free. Then, we know that \mathcal{B} generates \mathcal{O}_K over \mathbb{Z} .

Suppose that g is the column interpretation map for a matrix A which describes T . Suppose that A is written respect to a basis consisting of algebraic integers $\{\alpha, \beta\}$. Then, g represents a map $\mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{Z}^2$. Since the traces of algebraic integers (elements of $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$) are integers, then:

$$g(\mathcal{O}_{\mathbb{Q}(\sqrt{5})}) \subset \mathbb{Z}^2$$

Taking preimages keeps things distinct: *different fibers do not intersect!* In a preimage, codomain elements are simply replaced by their fibers.

This means that taking preimages with respect to T respects set inclusion.

So:

$$\mathcal{O}_{\mathbb{Q}(\sqrt{5})} \subset g^{-1}(\mathbb{Z}^2)$$

The inverse of the matrix for T is its adjugate which has integer entries multiplied by the reciprocal of its determinant. Suppose that its determinant is d . Then:

Theorem 9.3.6

$$\mathcal{O}_{\mathbb{Q}(\sqrt{5})} \subset T^{-1}(\mathbb{Z}^2) \subset \frac{1}{d} \cdot (\mathbb{Z} \cdot \alpha + \mathbb{Z} \cdot \beta)$$

This can be generalized to any ring of integers \mathcal{O}_K where K is a field extension of dimension n over \mathbb{Q} , \mathbb{Z}^2 is replaced by \mathbb{Z}^n , and $\{\alpha, \beta\}$ is replaced by an appropriate basis. Notice that $\{\alpha, \beta\}$ do not have to generate \mathcal{O}_K over \mathbb{Z} .

So if we do not know what the ring of integers is exactly, we have a good place in which to search!

Now, back to our bilinear form T . Suppose that we write it with respect to a basis $\{1, \alpha\}$ and suppose that ϕ_1 and ϕ_2 are the two Galois automorphisms. Then, our matrix looks like the following remembering that we are taking the trace of products:

$$\begin{pmatrix} \phi_1(1 \cdot 1) + \phi_2(1 \cdot 1) & \phi_1(1 \cdot \alpha) + \phi_2(1 \cdot \alpha) \\ \phi_1(\alpha \cdot 1) + \phi_2(\alpha \cdot 1) & \phi_1(\alpha \cdot \alpha) + \phi_2(\alpha \cdot \alpha) \end{pmatrix}$$

Remembering that ϕ_1 and ϕ_2 are ring homomorphisms, they are multiplicative (split across multiplication) so that this is:

$$\begin{pmatrix} \phi_1(1) \cdot \phi_1(1) + \phi_2(1) \cdot \phi_2(1) & \phi_1(1) \cdot \phi_1(\alpha) + \phi_2(1) \cdot \phi_2(\alpha) \\ \phi_1(\alpha) \cdot \phi_1(1) + \phi_2(\alpha) \cdot \phi_2(1) & \phi_1(\alpha) \cdot \phi_1(\alpha) + \phi_2(\alpha) \cdot \phi_2(\alpha) \end{pmatrix}$$

Notice that this comes from a matrix multiplication:

$$\begin{pmatrix} \phi_1(1) & \phi_2(1) \\ \phi_1(\alpha) & \phi_2(\alpha) \end{pmatrix} \cdot \begin{pmatrix} \phi_1(1) & \phi_1(\alpha) \\ \phi_1(1) & \phi_2(\alpha) \end{pmatrix}$$

or simply:

$$\underbrace{\begin{pmatrix} 1 & 1 \\ \phi_1(\alpha) & \phi_2(\alpha) \end{pmatrix}}_{B^T} \cdot \underbrace{\begin{pmatrix} 1 & \phi_1(\alpha) \\ 1 & \phi_2(\alpha) \end{pmatrix}}_B$$

Notice that:

$$\begin{pmatrix} 1 & \phi_1(\alpha) \\ 1 & \cdot(-1) \cdot \phi_1(\alpha) \\ & \phi_2(\alpha) \end{pmatrix} \rightarrow \begin{pmatrix} 1 & \phi_1(\alpha) \\ 0 & \phi_2(\alpha) - \phi_1(\alpha) \end{pmatrix}$$

This tells us that the determinant of B is $(\phi_2(\alpha) - \phi_1(\alpha))$ so that determinant of our matrix for T is

$$(\phi_2(\alpha) - \phi_1(\alpha))^2$$

since $\det(B) = \det(B^T)$. Notice $\phi_1(\alpha)$ and $\phi_2(\alpha)$ are the two distinct roots of the minimal polynomial for α . A *continued process of row operations similar to that above* can be used to show generally that:

Theorem 9.3.7

The discriminant of a power basis $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ of a field K over \mathbb{Q} is *always* the square of the product of differences of distinct roots of the minimal polynomial of α . Note: the generalization of matrix B in our discussion above is called a *Vandermonde matrix*.

Remember:

- The roots of an irreducible monic polynomial with coefficients in \mathbb{Q} are all distinct.
- Changing the basis keeps a determinant nonzero.

Theorem 9.3.8

Any matrix describing T will have a nonzero determinant. In particular, the column interpretation map of the matrix will be injective.

In particular, notice that in our case with $\mathbb{Q}(\sqrt{5})$ using $\alpha = \frac{1 + \sqrt{5}}{2}$, we have:

$$\phi_2(\alpha) - \phi_1(\alpha) = \frac{1 - \sqrt{5}}{2} - \frac{1 + \sqrt{5}}{2} = -\sqrt{5}$$

The determinant of B is $(-\sqrt{5})^2 = 5$.

This allows us to factor 5 as a square in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$.

Does something similar happen in $\mathbb{Q}(i)$? The determinant we found for our matrix for T was 4. Using $\alpha = i$, we have

$$\phi_2(\alpha) - \phi_1(\alpha) = i - (-i) = -2i$$

Yet squaring this does not give a factorization of 2 like we saw before.

We need a few more ideas here.

9.3.2 How to Find Factors in \mathcal{O}_K

Let's think generally. Suppose we are working with an algebraic extension $K = \mathbb{Q}(\alpha)$ of vector space dimension n over \mathbb{Q} where $\alpha \in \mathcal{O}_K$.

- Let $T : K \times K \rightarrow \mathbb{Q}^n$ denote the bilinear trace map as it has in our examples above.
- Let d be the discriminant of the basis $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ for K as a vector space over \mathbb{Q} .
- Also let g be the column interpretation map of the matrix for T written with respect to this basis.

We will use the following notation:

$\mathbb{Z}[\alpha]$

The set $\mathbb{Z}[\alpha]$ simply means $\mathbb{Z}[x]$ with x replaced by α . So this includes expressions like $2\alpha^3 - 5\alpha + 7$.

Theorem 9.3.9

Let $\alpha \in \mathcal{O}_K$, then the ring $\mathbb{Z}[\alpha]$ is isomorphic to $\mathbb{Z}[x]/f(x)\mathbb{Z}[x]$ where $f(x)$ is the minimal polynomial for α .

Proof. Since $\alpha \in \mathcal{O}_K$, then $f(x) \in \mathbb{Z}[x]$. The map

$$a(x) + f(x)\mathbb{Z}[x] \mapsto a(\alpha) + \underbrace{f(\alpha)\mathbb{Z}[\alpha]}_{=0} = a(\alpha)$$

is a well-defined \mathbb{Z} -module surjective map

$$\mathbb{Z}[x]/f(x)\mathbb{Z}[x] \rightarrow \mathbb{Z}[\alpha]$$

Suppose that $a(x) + f(x)\mathbb{Z}[x] \mapsto 0$. Then, $a(\alpha) = 0$. By the minimality of f , $f(x)$ is a factor of $a(x)$ which forces $a(x) + f(x)\mathbb{Z}[x]$ to be the zero coset. Hence, our map is injective. \square

Now back to our questions. We are going to talk about how to find factors of an integer prime in a ring of integers. We will also discuss why and how the discriminant plays a role.

To help us, we will develop some notation that we can use for counting the number of cosets of a subgroup B of A . In particular, we will be applying this notation when we talk about ideals—because these are additive subgroups.

Index $[A : B]$

We let $[A : B]$ denote the number of cosets of B in A . We call the number $[A : B]$ the *index* of B in A .

Theorem 9.3.10

If $A \supset B \supset C$ are commutative additive groups, then:

$$[A : B] \cdot [B : C] = [A : C]$$

Proof. The coset partition caused by shifts of C in B is itself shifted into every coset of B in A . Thus, the number of cosets of C in A is the number of cosets of C in B multiplied by the number of cosets of B in A . \square

$\mathbb{Z}[\alpha]$ is the \mathbb{Z} -span of the basis $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ for K as a vector space over \mathbb{Q} .

Then $\mathbb{Z}[\alpha]$ need not be all of \mathcal{O}_K . In particular,

$$g(\mathbb{Z}[\alpha]) \subset g(\mathcal{O}_K) \subset \mathbb{Z}^2$$

From this we have:

$$[\mathbb{Z}^2 : g(\mathcal{O}_K)] \leq [\mathbb{Z}^2 : g(\mathbb{Z}[\alpha])]$$

with equality only if $\mathbb{Z}[\alpha] = \mathcal{O}_K$.

Let “ $a \mid b$ ” mean “ a is a factor of b ” which can also be said as “ a divides b .” Then it is clear from how cosets equally partition that:

$$[\mathbb{Z}^2 : g(\mathcal{O}_K)] \mid [\mathbb{Z}^2 : g(\mathbb{Z}[\alpha])]$$

What if a prime p were not a factor of our discriminant d ?

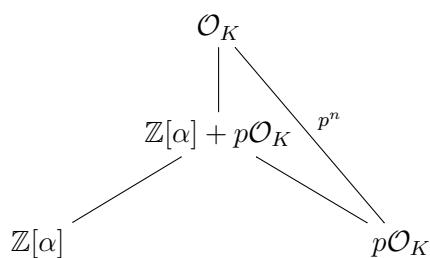
So we are saying that p is not a factor of $[\mathbb{Z}^2 : g(S)]$ which implies that it is also not a factor of $[\mathbb{Z}^2 : g(\mathcal{O}_K)]$.

Theorem 9.3.11

$$[\mathcal{O}_K : p\mathcal{O}_K] = p^n$$

Proof. We know that the map g injects \mathcal{O}_K into \mathbb{Z}^n as a free rank n \mathbb{Z} submodule. Yet any free rank n \mathbb{Z} module is isomorphic itself to \mathbb{Z}^n . This isomorphism is scalable by integers. In particular, it preserves multiplication by p from domain to codomain. In the codomain \mathbb{Z}^n of this isomorphism, multiplication by p can be thought of as multiplication by $p \cdot \text{id}_{n \times n}$ which has determinant p^n . Thus the number of cosets in \mathbb{Z}^n of the image of this matrix is p^n . By isomorphism back to the domain, we get that this is the same as the number of cosets of $p\mathcal{O}_K$ in \mathcal{O}_K . \square

Consider the following diagram where p^n refers to $[\mathcal{O}_K : p\mathcal{O}_K]$:



Notice that

$$[\mathcal{O}_K : \mathbb{Z}[\alpha] + p\mathcal{O}_K] \mid \underbrace{[\mathcal{O}_K : \mathbb{Z}[\alpha]]}_{=[g(\mathcal{O}_K) : g(\mathbb{Z}[\alpha])]} \mid d = [\mathbb{Z}^2 : g(\mathbb{Z}[\alpha])] \quad [\mathcal{O}_K : \mathbb{Z}[\alpha] + p\mathcal{O}_K] \mid [\mathcal{O}_K : p\mathcal{O}_K] = p^n$$

Since $p \nmid d$ (p is not a factor of d), then $[\mathcal{O}_K : \mathbb{Z}[\alpha] + p\mathcal{O}_K]$ is forced to be 1. Hence:

$$\mathbb{Z}[\alpha] + p\mathcal{O}_K = \mathcal{O}_K$$

So every element of \mathcal{O}_K is a multiple of p away from an element in $\mathbb{Z}[\alpha]$. This tells us that every chunk in the quotient $\mathcal{O}_K/p \cdot \mathcal{O}_K$ is uniquely accounted for in the quotient $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$. *These quotients are isomorphic.*

Proof. Every chunk in $\mathcal{O}_K/p \cdot \mathcal{O}_K$ has a representative given in $\mathbb{Z}[\alpha]$ and if the difference of two of these $\mathbb{Z}[\alpha]$ representatives were in $p \cdot \mathcal{O}_K$, then that difference would also be in $\mathbb{Z}[\alpha]$ since $\mathbb{Z}[\alpha]$ is an additive group. \square

What is so nice about the quotient $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$?

Let $f(x)$ be the minimal polynomial for α . Remember that $\mathbb{Z}[\alpha]$ isomorphically looks like $\mathbb{Z}[x]/f(x)\mathbb{Z}[x]$. The integer p passes through any \mathbb{Z} -module isomorphism unchanged because such a map is scalable by integers—integers can pass freely from the domain to the codomain of such an isomorphism. So, $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$ is like we are modding out by multiples of p in the quotient $\mathbb{Z}[x]/f(x)\mathbb{Z}[x]$.

Multiplication by p to a coset $a(x) + f(x)\mathbb{Z}[x]$ is defined as simply multiplying the representative $a(x)$ by p . *This is well defined!* If desired, in your mind you can think of this scalar multiplication not as multiplication but instead as repeated set addition

$$\underbrace{(a(x) + f(x)\mathbb{Z}[x]) + \cdots + (a(x) + f(x)\mathbb{Z}[x])}_{p \text{ times}}$$

(You can take $a(x)$ in all of the sets except for one from which you take $a(x) + f(x)$. Notice that $p \cdot a(x) + f(x)$ is an example of something obtained in this set addition.)

So we are saying that multiples of p in $\mathbb{Z}[x]/f(x)\mathbb{Z}[x]$ are of the form $p \cdot a(x) + f(x)\mathbb{Z}[x]$. These make up a \mathbb{Z} submodule which becomes 0 when we quotient out by it. So, $a(x) + f(x)\mathbb{Z}[x]$ and $b(x) + f(x)\mathbb{Z}[x]$ are thought of as being the same if $a(x) - b(x)$ is in the zero coset of this modding out by p . That is, $a(x) - b(x)$ is a multiple of p .

Wait! Polynomials add component wise—by like terms. So, the coefficients themselves need to be a multiple of p apart so that $a(x) + f(x)\mathbb{Z}[x]$ and $b(x) + f(x)\mathbb{Z}[x]$ appear in the same chunk when modding out by p . So the coefficients are considered in $\mathbb{Z}/p\mathbb{Z}$ which is also denoted as \mathbb{F}_p —the finite field with p elements.

This means that if we mod out by multiples of p in $\mathbb{Z}[x]/f(x)\mathbb{Z}[x]$, we are really looking isomorphically at:

$$\mathbb{F}_p[x]/\overline{f(x)} \mathbb{F}_p[x]$$

where $\overline{}$ corresponds to modding out coefficients by p .

We are going to look at subsets of $\mathbb{F}_p[x]/\overline{f(x)} \mathbb{F}_p[x]$. We would like these subsets to be closed under polynomial multiplication—not just multiplication from \mathbb{Z} .

Can we think of elements of $\mathbb{Z}[x]$ as scalars? Yes we can! For instance, we can take an element of $\mathbb{F}_p[x]/\overline{f(x)} \mathbb{F}_p[x]$ such as $\overline{a(x)} + \overline{f(x)} \mathbb{F}_p[x]$ and define multiplication by $b(x) \in \mathbb{Z}[x]$ as:

$$b(x) \cdot (\overline{a(x)} + \overline{f(x)} \mathbb{F}_p[x]) = \overline{b(x)a(x)} + \overline{f(x)} \mathbb{F}_p[x])$$

This multiplication follows all of the rules for scalar multiplication in modules and is well defined. In particular, any representative of this coset would have given the same result. That is, we could have chosen $\overline{a(x)} + \overline{r(x)f(x)}$ as a representative. Then realize that $\overline{b(x)a(x)} + \overline{b(x)r(x)f(x)}$ is also a representative of $\overline{b(x)a(x)} + \overline{f(x)} \mathbb{F}_p[x]$.

We want to look at subsets of $\mathbb{F}_p[x]/\overline{f(x)} \mathbb{F}_p[x]$ that are closed under multiplication by $\mathbb{Z}[x]$ and are additive subgroups. Another way of saying this is:

We want to find subsets of $\mathbb{F}_p[x]/\overline{f(x)} \mathbb{F}_p[x]$ that are both additive subgroups and closed under *any* outside multiplication from the whole ring $\mathbb{F}_p[x]/\overline{f(x)} \mathbb{F}_p[x]$ itself. *Yes: this quotient is a ring—cosets multiply:* $(a + H) \cdot (b + H) = (a \cdot b) + H$.

Notice that we are requiring these subsets to swallow all multiplications! As a different example of such an idea, think of $3\mathbb{Z}$ —the multiples of 3. If you multiply any multiple of 3 by anything in the bigger ring \mathbb{Z} , we are stuck in $3\mathbb{Z}$.

Now if we took all the elements in such a subset, do they have a greatest common factor? Well $\mathbb{F}_p[x]$ has a nice division algorithm just like $\mathbb{Q}[x]$ does since \mathbb{F}_p is a field. This means we can apply the Euclidean algorithm and find greatest common factors. Hence, additive subgroups that are multiplicatively closed in $\mathbb{F}_p[x]$ take on the form $\overline{r(x)} \mathbb{F}_p[x]$ where $\overline{r(x)}$ is the greatest common factor of *all the elements in the set*.

We still need to mod out by $\overline{f(x)}$. When we do, remember that adding by zero—that is multiples of $\overline{f(x)}$ —needs to be able to happen in each subset.

So we should think that $\overline{r(x)}$ should also be a factor of $\overline{f(x)}$.

This means that when we look at our desired subsets in the quotient $\mathbb{F}_p[x]/\overline{f(x)} \mathbb{F}_p[x]$, we consider subsets that are all multiples of $\overline{r(x)} + \overline{f(x)} \mathbb{F}_p[x]$ where $\overline{r(x)}$ is a factor of $\overline{f(x)}$.

Pulling Back

When we “*unmod*” one of these subsets all the way back to \mathcal{O}_K we get something of the form

$$p \cdot \mathcal{O}_K + r(\alpha) \cdot \mathcal{O}_K$$

where $r(x)$ is *any* polynomial such that $r(x)$ is a factor of $f(x)$. Remember when we mod we take a chunk. When we “*unmod*,” we look at all the elements in the chunks we are considering.

Unmodding

To *unmod* is to replace cosets by the elements in the coset. To *mod* is to replace elements in a coset chunk with the coset label itself. *We back out of a quotient when we unmod and go into a quotient when we mod.*

In particular, whenever we unmod a set, we must have a set addition by the zero coset somewhere—because that is how you get from one element in a coset to another—by adding by a zero coset element!

9.3.3 Factorization into Ideals

Ideals

The types of subsets that we have arrived at in \mathcal{O}_K are examples of what are called *ideals*. These are additive subgroups which are closed by any outside multiplication of elements in the ring \mathcal{O}_K . For instance, $3\mathbb{Z}$ is an ideal of \mathbb{Z} .

The set $p \cdot \mathcal{O}_K + r(\alpha) \cdot \mathcal{O}_K$ is an ideal in \mathcal{O}_K which contains p . It is like the sum of two \mathcal{O}_K spans so is clearly closed with respect to multiplication by elements of \mathcal{O}_K . It also is not too difficult to see that it is an additive subgroup. Yet, this particular type of ideal that we found in the “*unmodding*” process is used in finding a factorization of p itself. In the integers, this is like saying that 20 is contained in the ideal $2\mathbb{Z}$ so that $2\mathbb{Z}$ contains a factor of 20—namely 4 itself.

Containment and Factorization

If an element is contained in an ideal, that ideal has a factor of that element.

Let’s dive into an example where we find a factorization in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. As we do so...

Remember that we need to be able to find a $r(x)$ which is a factor of a minimal polynomial considered mod p .

Example 4. Let's see if we can factor 11 nontrivially in $\mathbb{Q}(\sqrt{5})$. Let's take $\alpha = \sqrt{5}$ which has a minimal polynomial of $f(x) = x^2 - 5$. Let's try to factor $x^2 - 5$ in mod 11. To do so, we try to find a root of $x^2 - 5$ mod 11.

Through trial and error, we notice that $g(4) = 11$ which is equivalent to 0 mod 11. Then, we can do synthetic or regular division in mod 11 arithmetic. We divide $(x - 4)$ into $x^2 - 5$ to get a quotient of $(x + 4)$ where the remainder is equivalent to 0. Hence:

$$x^2 - x - 1 \equiv (x - 4)(x + 4) \pmod{11}$$

In our case we are lucky. Simply replace the x 's with $\sqrt{5}$ without adding any multiple of 11 and we get a factorization (after multiplying by -1)

$$11 = -(\sqrt{5} - 4)(\sqrt{5} + 4)$$

So we see that the integer prime 11 factors nontrivially into two numbers in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$.

The number $-(\sqrt{5} - 4)$ comes from the ideal $r_1(\sqrt{5}) \cdot \mathcal{O}_{\mathbb{Q}(\sqrt{5})} + 11 \cdot \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ where $r_1(x) = x - 4$ and $(\sqrt{5} + 4)$ comes from the ideal $r_2(\sqrt{5}) \cdot \mathcal{O}_{\mathbb{Q}(\sqrt{5})} + 11 \cdot \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ where $r_2(x) = x + 4$. Both $r_1(x)$ and $r_2(x)$ are factors of $x^2 - x - 1$ considered as a polynomial in $\mathbb{F}_{11}[x]$.

Factoring in \mathcal{O}_K

When we talk about factoring in \mathcal{O}_K we usually mean in terms of *ideals* instead of elements. The multiplication is *set multiplication*. So we are really *factoring sets* instead of elements. Yet in reality we do this all of the time in \mathbb{Z} . For instance, $10 = 2 \cdot 5$ is the same thing as $10\mathbb{Z} = 2\mathbb{Z} \cdot 5\mathbb{Z}$.

Question

Sometimes we are worried about the repetition of ideals in a factorization. When do we see repetitions and when will we not?

To answer this question, we must delve into ideals a little.

Theorem 9.3.12

Let A be an ideal of a ring R . Then R/A is a ring.

Proof. We already know that since R is a commutative additive group, that the quotient R/A for the additive

subgroup A ends up also being an additive subgroup. Is it a ring? Take two elements $x + A$ and $y + A$. Let's see if no matter what representative $x + a_1$ we choose in the chunk $x + A$ and representative $y + a_2$ if the process

$$((x + a_1) + A) \cdot ((y + a_2) + A) = (x + a_1)(y + a_2) + A$$

always return the same coset of A . Consider:

$$(x + a_1)(y + a_2) = xy + \underbrace{xa_2 + a_1 + a_1a_2}_{\in A}$$

since every multiple of an element in A even by things not in A like x and y are still in A . This is because A is an ideal. This means that $(x + a_1)(y + a_2) - xy \in A$. That is, the difference of the two cosets $(x + a_1)(y + a_2) + A$ and $xy + A$ is the zero coset in the additive group. So the cosets are the same. Hence, multiplication is well defined between additive cosets of A by just considering the multiplication of coset representatives. The other ring properties will transfer over immediately from R . \square

If we had a "proper inclusion" (i.e. \subsetneq) chain of ideals

$$p\mathcal{O}_K \subsetneq A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_m \subsetneq \mathcal{O}_K$$

then

$$1 = [\mathcal{O}_K : \mathcal{O}_K] < [\mathcal{O}_K : A_m] < \cdots < [\mathcal{O}_K : A_2] < [\mathcal{O}_K : A_1] \leq [\mathcal{O}_K : p\mathcal{O}_K] = p^n$$

If we let " $a \mid b$ " mean " a is a factor of b " which can also be said as " a divides b ," then we have:

$$1 = [\mathcal{O}_K : \mathcal{O}_K] \mid [\mathcal{O}_K : A_m] \mid \cdots \mid [\mathcal{O}_K : A_2] \mid [\mathcal{O}_K : A_1] \mid [\mathcal{O}_K : p\mathcal{O}_K] = p^n$$

There is a point where it will be impossible to insert another ideal between one of our K_i and \mathcal{O}_K because it is impossible to go strictly between an ideal M and \mathcal{O}_K if $[\mathcal{O}_K : M]$ is a prime number.

Maximal Ideal

Let M be an ideal of a ring R such that there is no ideal A such that $M \subsetneq A \subsetneq R$. Then M is called a maximal ideal.

Theorem 9.3.13

Let M be a maximal ideal of a ring R . Then the quotient ring R/M is a field. Conversely, if R/M is a field, then M is maximal.

Proof. Let $(x + M) \in R/M$ such that $x + M$ is *not* the zero coset. Multiplication by $x + M$ is a ring homomorphism $R/M \rightarrow R/M$. The kernel of this map is an ideal of R/M .

This is because “anything times zero is zero” translates in the *preimage* to: “anything multiplied to the kernel is in the kernel” since the map is multiplicative.

This ideal “unmods” to an ideal of R that contains M (since it had to contain zero in the quotient). Call this unmodded ideal Y . We know that $M \subset Y \subset R$. Remember that M is maximal. Hence, $Y = M$ or $Y = R$. Since $x + M$ is not in the zero coset, this is not the zero map. Hence, $Y = M$. That is, our multiplication map $R/M \rightarrow R/M$ has zero kernel so is injective.

A similar argument can be done for surjectivity. We realize that the range of our map $R/M \rightarrow R/M$ also unmods to an ideal between M and R . Again, because our map is not the zero map, the range unmodded is R . Modding back, we see that our map is surjective. This means that multiplication by $x + M$ is an isomorphism.

The preimage of the multiplicative identity element $1 + M$ is the inverse of $x + M$. Since every nonidentity element has an inverse, R/M is a field.

Now, suppose that R/M is a field. Then, if Y is an ideal such that $M \subsetneq Y \subsetneq R$ and $y \in Y \setminus M$ (that is y is in Y but not in M), then $Ry + M \subset Y \neq R$. We know that $1 + M \notin Y$ since this would imply that $R \cdot 1 + Y \subset Y$ which would force $Y = R$. Therefore, $1 + M \notin Ry + M = R$ which says that $y + M$ does not have an inverse in R/M . This is because $Ry + M$ is a way of describing all coset multiples of $y + M$ since multiplication in R/M is done right at the representatives: $(a + M)(b + M) = (ab) + M$. This contradicts the fact that we suppose that R/M is a field. Therefore, no such Y exists and M is maximal. \square

Maximal ideals are just examples of the types of ideals we are interested in:

Prime Ideal

A prime ideal is an ideal P of R such that the zero coset is *not* a multiple of a nonzero element (i.e. coset) in the quotient R/P .

Theorem 9.3.14

Maximal ideals are prime ideals.

Proof. Clearly maximal ideals fit into this since you cannot multiply two nonzero field elements and get zero. Especially since multiplication by a nonzero field element is a ring homomorphism which has an inverse—multiplication by the multiplicative inverse of our nonzero element. Hence, the multiplication map is injective with zero kernel. That is, the only thing you can plug into the multiplication and get out zero is zero itself. \square

Our description of a prime should make sense. For instance, since $6 \cdot 3$ is a multiple of 2 which is prime, then either 6 is a multiple of 2 or 3 is a multiple of 2. That is because the prime number 2 has to be in the factorization somewhere and it is one of the “smallest and indivisible parts” of the factorization.

This is the same as saying $6 \cdot 3 \in 2\mathbb{Z}$ implies that either $6 \in 2\mathbb{Z}$ or $3 \in 2\mathbb{Z}$. Let $\underline{\quad}$ describe $\mathbb{Z}/2\mathbb{Z}$. Then we could again rephrase this as: $\underline{6 \cdot 3} = \underline{2}$ implies that $\underline{6} = \underline{0}$ or $\underline{3} = \underline{0}$. That is, either $\underline{6}$ or $\underline{3}$ must be 0.

This prime condition for P gives that R/P is close to being a field—except that we did not guarantee that nonzero elements had inverses—just that they weren’t something called *zero divisors*.

Zero Divisor

A zero divisor a in a ring R is a nonzero element such that some multiple of it like ab where $b \in R$ is equal to zero.

So we could say that an ideal P is prime in R if no element of (i.e. coset in) R/P is a zero divisor.

When we are in \mathcal{O}_K and consider factorizations of ideals into set multiplications of *prime ideals*, we have the following important result. We provide a link to the proof which involves the use of “Zorn’s lemma” and other machinery.

Theorem 9.3.15

Each ideal in \mathcal{O}_K is a set. Every ideal of \mathcal{O}_K is a *set product* of prime ideals. This product is unique.



Proof. See: [Video](#)

□

Corollary 9.3.16

Let p be a prime number in \mathbb{Z} . Then we have the *unique* factorization:

$$p\mathcal{O}_K = P_1^{e_1} \cdots P_k^{e_k}$$

where P_1, \dots, P_k are the distinct prime ideals that contain p .

The following idea helps us to think about prime ideals in \mathcal{O}_K that contain $p \in \mathbb{Z}$:

Theorem 9.3.17

Suppose that K/\mathbb{Q} is a normal extension. Let ϕ be an element of the Galois group of this extension. If P is a prime ideal in \mathcal{O}_K that contains $p \in \mathbb{Z}$ (so could contain factors of p), then $\phi(P)$ is another prime ideal of \mathcal{O}_K that also contains p . Further, \mathcal{O}_K/P and $\mathcal{O}_K/\phi(P)$ are isomorphic.

Proof. Notice that the map $\mathcal{O}_K \rightarrow \mathcal{O}_K/\phi(P)$ defined by first applying ϕ and then taking a quotient (grouping into chunks) has P as its kernel and is surjective. Hence: \mathcal{O}_K/P and $\mathcal{O}_K/\phi(P)$ are isomorphic. This shows that both P and $\phi(P)$ are prime ideals. We know that $p \in \phi(P)$ since ϕ fixes all of the elements of \mathbb{Q} and \mathbb{Z} is contained in \mathbb{Q} . \square

Corollary 9.3.18

$$[\mathcal{O}_K : P] = [\mathcal{O}_K : \phi(P)]$$

Corollary 9.3.19

There is a number e such that our factorization of the ideal $p\mathcal{O}_K$ becomes:

$$p\mathcal{O}_K = P_1^e \cdots P_k^e$$

Proof. The automorphism ϕ fixes $p\mathcal{O}_K$ since it sends roots of monic polynomials to roots of those same monic polynomials and because it fixes $p \in \mathbb{Q}$. Thus, ϕ fixes the unique factorization of $p\mathcal{O}_K$ but sends $P_i^{e_i}$ to

$$\underbrace{\phi(P_i)}_{\text{some } P_j}^{e_i}$$

Hence, $e_i = e_j$. \square

Theorem 9.3.20

All prime ideals in \mathcal{O}_K are maximal.

Proof. Let $\beta \in P$ where $\beta \neq 0$. Then $\beta\mathcal{O}_K \subset P$. Multiplication by β is an injective linear transformation expressible as a matrix with entries in \mathbb{Z} when written with respect to the same basis in which we write the column interpretation map g . It has nonzero determinant which is equal to $[\mathbb{Z}^2 : g(\beta\mathcal{O}_K)]$. We know that

$$[\mathcal{O}_K : P] \mid [\mathcal{O}_K : \beta\mathcal{O}_K] = [g(\mathcal{O}_K) : g(\beta\mathcal{O}_K)] \mid [\mathbb{Z}^2 : g(\beta\mathcal{O}_K)]$$

so that the quotient \mathcal{O}_K/P is finite. We also know that it has no zero divisors. This means that multiplication by any nonzero element in this quotient must be an injective ring homomorphism. (*The statement that it has no zero divisors implies that the kernel of such a map must be zero because zero divisors arise when the kernel is nonzero.*) Yet an injective ring homomorphism whose domain is finite and whose codomain is the same as its domain, must also be surjective. This is just a counting idea. Every one of k things has to go to k distinct things. There are only k total things to choose from so that they all must be chosen. So multiplication by a nonzero element of the quotient \mathcal{O}_K/P is an isomorphism. The preimage of $1+P$ is the multiplicative inverse of this nonzero element. Therefore, \mathcal{O}_K/P must be a field. That is, P is a maximal ideal. \square

Theorem 9.3.21

Let p be a prime element of \mathbb{Z} and suppose that $p \in P$ where P is a prime ideal of \mathcal{O}_K . Then, the field $\mathbb{Z}/p\mathbb{Z}$ sits injectively inside of \mathcal{O}_K/P . In particular, there is only one integer prime p which can live in P .

Proof. Consider the ring homomorphism $\mathbb{Z} \rightarrow \mathcal{O}_K/P$ which takes an integer to the chunk it would live in when we chunk \mathcal{O}_K into shifts of P . The kernel of this ring homomorphism is an ideal of \mathbb{Z} since “zero times anything is zero” translates back in the preimage to “the kernel is an ideal” when the map is multiplicative. The ideals in \mathbb{Z} look like $m\mathbb{Z}$ for some m . Now if we mod \mathbb{Z} by this kernel $m\mathbb{Z}$ and look at our map again we get an injection because modding out by the kernel makes it zero:

$$\mathbb{Z}/m\mathbb{Z} \rightarrow \mathcal{O}_K/P$$

Wait! This means that $\mathbb{Z}/m\mathbb{Z}$ cannot have any zero divisors. This only happens when m is a prime number. Since the kernel is unique, m is a unique prime p . \square

Still we let d be the discriminant of the basis $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ for K as a vector space over \mathbb{Q} . Recall that d is a product of differences of roots $(\alpha_i - \alpha_j)$ of the minimal polynomial f for α .

Again, we assume that $p \nmid d$.

Further we keep the assumption that K is a normal extension of \mathbb{Q} since factorizations in \mathcal{O}_K are just further factorizations of what we have in \mathcal{O}_L where L is an intermediate field. This assumption allows us to think of all the roots α_i as living in \mathcal{O}_K .

So if we know that $d \notin p\mathbb{Z}$, then $d \notin P$ which means that d represents a nonzero product in the field \mathcal{O}_K/P . Hence, none of the elements of this product can be zero in this field.

All of the coset chunks $\alpha_i + P$ which are elements in the field \mathcal{O}_K/P are distinct under our current assumption that $p \nmid d$.

$F = \mathcal{O}_K/P$ is a field extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. It is algebraic field extension

$$F = \mathbb{F}_p(\alpha_1, \dots, \alpha_n)$$

Even though the root cosets $\alpha_1 + P, \dots, \alpha_n + P$ are distinct, the cosets may not be linearly independent any more! This means that we might need fewer of them to be a spanning set.

Using the same reasoning as we did over \mathbb{Q} , all algebraic extensions of \mathbb{F}_p are primitive meaning generated by a single element.

In particular, $F = \mathcal{O}_K/P$ can be thought of as $\mathbb{F}_p(\alpha_j + P)$ for one of the root cosets $\alpha_j + P$. Without loss of generality, let's just name α_j as α . *They are both roots—so why not?*

$$F = \mathbb{F}_p(\alpha + P)$$

But keep in mind that the dimension of F over \mathbb{F}_p may be less than n .

Theorem 9.3.22

All finite dimensional field extensions of \mathbb{F}_p have Galois groups.

Proof. A field extension of dimension m has p^m elements just thinking of the number of elements in

$$\underbrace{\mathbb{F}_p \times \mathbb{F}_p \times \cdots \times \mathbb{F}_p}_{p \text{ times}}$$

Let's just imagine that α is above all the polynomials we mention in this proof. Now if you take out the zero of this field, you get a multiplicative group with $p^m - 1$ elements. This multiplicative group is commutative. If you raise any element of this group to the power of $p^m - 1$ you get 1. That is, everything nonzero is a root of $x^{p^m-1} - 1$. If you want to include zero, everything is a root of $x^{p^m} - x$. This means that the irreducible polynomial $r(x)$ of $\alpha + P$ must be a factor of $x^{p^m} - x$. To get all the roots we simply use the cyclotomic polynomial describing primitive $(p^m - 1)$ st roots of unity. Because we are including all of the roots of an irreducible polynomial, then $\mathbb{F}_p(\alpha + P)$ is a normal extension.

Notice that the derivative of $x^{p^m} - x$ over \mathbb{F}_p is $p^m x^{p^m-1} - 1 \equiv -1 \pmod{p}$ which shares no common factor with $x^{p^m} - x$. Hence, there are *no repeated roots* to this polynomial. This means that there are no repeated roots in $r(x)$. With no repetition in $r(x)$ and the extension being normal, everything that we discussed for Galois groups of finite extensions of \mathbb{Q} carries right over! \square

Corollary 9.3.23

Irreducible polynomials over \mathbb{F}_p have no repeated roots.

Proof. Adjoining a root of an irreducible polynomial to \mathbb{F}_p produces a finite dimensional field extension of some dimension m . The minimal polynomial of that root is the irreducible polynomial in question itself. This minimal polynomial must be a factor of $x^{p^m} - x$ which in the previous proof was shown to not have any repeated roots. \square

- Let $r(x)$ denote the minimal polynomial of $\alpha + P$ over \mathbb{F}_p . We must have that $r(x)$ is an irreducible monic factor of $f(x)$.
 - Let G denote the Galois group of the extension K over \mathbb{Q} .
 - Let D_P denote the subgroup of G discussed in the following theorem.

Theorem 9.3.24

The automorphisms of G that send roots $\alpha_j + P$ of $r(x)$ to other roots $\alpha_i + P$ of $r(x)$ make up a subgroup of G . We denote it as D_P . It is isomorphic to the Galois group of \mathcal{O}_K/P over \mathbb{F}_p . We are still assuming that $p \nmid d$.

Proof. Remember that all of the roots α_i of $f(x)$ result in distinct elements $\alpha_i + P$ in \mathcal{O}_K/P . The automorphisms in G are uniquely determined by which root α is sent to. Assuming that $\alpha + P$ is a root of $r(x)$, then the automorphisms we are considering are those such that $\alpha + P \mapsto \alpha_j + P$ where $\alpha_j + P$ is another root of $r(x)$. Yet we know that this collection of automorphisms is in bijective correspondence to the Galois group of the field \mathcal{O}_K/P over \mathbb{F}_p . Since the roots stay distinct when we mod by P , a subgroup of root permutations after the mod is also a subgroup before the mod. Therefore, D_P is a subgroup of G . \square

Theorem 9.3.25

Consider the field extension $\mathcal{O}_K/P = F(\alpha)$ of \mathbb{F}_p where $r(x)$ is the minimal polynomial of α . Then $P = p\mathcal{O}_K + r(\alpha)\mathcal{O}_K$.

Proof. In the spirit of our discussion, \mathcal{O}_K/P is isomorphic to $\mathbb{F}_p[x]/r(x)$. “Unmodding” reveals the result. \square

The isomorphism in this last proof shows:

Corollary 9.3.26

The dimension of \mathcal{O}_K/P over $\mathbb{F}_p(\alpha)$ is the same as the degree of $r(x)$.

Theorem 9.3.27

Suppose that $r_1(x)$ and $r_2(x)$ are two *distinct* irreducible factors of $f(x)$. Then, the two prime ideals $P_1 = p\mathcal{O}_K + r_1(\alpha)\mathcal{O}_K$ and $P_2 = p\mathcal{O}_K + r_2(\alpha)\mathcal{O}_K$ are also distinct.

Proof. First, $r_1(x)$ and $r_2(x)$ cannot be the same since $f(x)$ has no repeated roots. Next, $r_1(x)$ and $r_2(x)$ have a greatest common factor of 1. Therefore, there are polynomials $a(x)$ and $b(x)$ so that

$$a(x) r_1(x) + b(x) r_2(x) = 1$$

Isomorphically in \mathcal{O}_K , this equation becomes:

$$a(\alpha)r_1(\alpha) + b(\alpha)r_2(\alpha) \equiv 1 \pmod{P}$$

This idea provides a contradiction if

$$a(\alpha)r_1(\alpha) \equiv b(\alpha)r_2(\alpha) \equiv 0 \pmod{P_1}$$

Therefore,

$$r_2(\alpha) \not\equiv 0 \pmod{P_1}$$

Hence, from our above results, $P_1 \neq P_2$. □

Chinese Remainder Theorem for Ideals

$$\mathbb{F}_p^n = \mathbb{Z}^n/p\mathbb{Z}^n \cong \mathcal{O}_K/p\mathcal{O}_K = \mathcal{O}_K/P_1^e \cdots P_k^e \cong \mathcal{O}_K/P_1^e \times \cdots \times \mathcal{O}_K/P_k^e$$

Proof. Realize that the P_i are distinct and maximal. Let's take P_1 and P_2 . We know that $P_1 + P_2$ is an ideal that contains P_1 and yet is larger than P_1 since $P_2 \neq P_1$. By maximality, $P_1 + P_2 = \mathcal{O}_K$. This means that we can find elements $a_1 \in P_1$ and $a_2 \in P_2$ so that $a_1 + a_2 = 1$. Consider the following expansion of $(a_1 + a_2)^{2e+1}$ which uses binomial coefficients:

$$(a_1 + a_2)^{2e+1} = a_1^{2e+1} + \binom{2e+1}{1} a_1^{2e} a_2 + \binom{2e+1}{2} a_1^{2e-1} a_2 + \cdots + a_2^{2e+1}$$

Notice that every element of this sum is in P_1^e or in P_2^e . This means that $1 \in P_1^e + P_2^e$. Now, suppose that $a \in P_1^e$ and $b \in P_2^e$ such that $a + b = 1$. Then $1 - a \equiv 1 \pmod{P_1^e}$ and $1 - a \equiv 0 \pmod{P_2^e}$. We could have similarly found $a' \in P_1^e$ and $c' \in P_2^e$ so that $a' + c' = 1$. Then we have:

$$\begin{aligned} (1 - a)(1 - a') &\equiv 1 \pmod{P_1^e} \\ (1 - a)(1 - a') &\equiv 0 \pmod{P_2^e} \\ (1 - a)(1 - a') &\equiv 0 \pmod{P_3^e} \end{aligned}$$

What good does this do? If we form a ring homomorphism which just sends an element to its chunk per component:

$$\mathcal{O}_K \rightarrow \mathcal{O}_K/P_1^e \times \cdots \times \mathcal{O}_K/P_k^e,$$

then continuing this process yields an element in $e_1 \in \mathcal{O}_K$ that is sent to $(\bar{1}, \bar{0}, \dots, \bar{0})$ where \bar{x} denotes a chunk representative in the respective components.

This same idea can help us get an element $e_2 \in \mathcal{O}_K$ that is sent to $(\bar{0}, \bar{1}, \bar{0}, \dots, \bar{0})$. We eventually obtain analogous elements e_1, e_2, \dots, e_k all in \mathcal{O}_K . Now take an arbitrary element of the codomain $(\bar{t}_1, \dots, \bar{t}_r)$. An element of the fiber over this element is: $t_1 e_1 + \cdots + t_r e_k$. That is, every fiber is nonempty. This map is surjective!

To make an injective map out of this, we simply mod the domain by the kernel of the map (to force a zero kernel). The kernel is simply $Y = P_1^e \cap \cdots \cap P_k^e$ since this is the set of everything that will map to $(\bar{0}, \dots, \bar{0})$.

Now notice that $P_1^e P_2^e \cdots P_k^e \subset Y$. Also realize that $Y \subset P_i^e$ for each i . The unique factorization of Y must have each P_i^e in its factorization. This tells us that $Y \subset P_1^e P_2^e \cdots P_k^e$. Therefore, $Y = P_1^e P_2^e \cdots P_k^e$. This proves the theorem. \square

Corollary 9.3.28

In our case when $p \nmid d$, then $e = 1$. That is, there are no repeated factors in the ideal factorization of $p\mathcal{O}_K$.

Proof. Note that \mathcal{O}_K/P_i is isomorphic as a vector space to $\mathbb{F}_p^{\deg(r_i(x))}$ where $r_i(x)$ ranges through the distinct irreducible factors mod p of $f(x)$. The degrees of these distinct factors all add up to n so that the dimensions of all of the \mathcal{O}_K/P_i for $i \in \{1, \dots, k\}$ all add up to n . If $e > 1$, consider \mathcal{O}_K/P_1^e . By unique factorization of ideals:

$$P_1^e \subsetneq P_1^{e-1} \subsetneq \cdots \subsetneq P_1^2 \subsetneq P_1 \subsetneq \mathcal{O}_K$$

Notice that the quotient P_1/P_1^2 is a \mathbb{F}_p vector space since it is closed under addition and scalar multiplication by \mathcal{O}_K , hence \mathbb{Z} and multiplication by $p \in P_1$ brings elements of P_1 to P_1^2 (which is 0).

Take an element x in P_1 that is not in P_1^2 . Then, multiplication by x gives a linear transformation $\mathcal{O}_K/P_1 \rightarrow P_1/P_1^2$. The range and the kernel of this map “unmod” to ideals of \mathcal{O}_K which are forced by unique factorization to be either P_1 or P_1^2 . Our choice of x guarantees a nonzero map. Hence the linear transformation is forced to be an isomorphism.

Continuing this idea we find that the number of elements in \mathcal{O}_K/P_1^e is the product

$$|\mathcal{O}_K/P_1| \cdot |P_1/P_1^2| \cdots |P_1^{e-1}/P_1^e| = |\mathcal{O}_K/P_1|^e = (p^{\deg(r_1(x))})^e$$

Hence, by our Chinese remainder theorem,

$$p^n = |\mathcal{O}_K/p\mathcal{O}_K| = |\mathcal{O}_K/P_1^e| \cdots |\mathcal{O}_K/P_k^e| = (p^{\deg(r_1(x))})^e \cdots (p^{\deg(r_k(x))})^e$$

Hence,

$$n = (\deg(r_1(x)) + \cdots + \deg(r_k(x))) \cdot e$$

Yet we know that all of the $r_i(x)$ are distinct and that their product is $f(x)$ which has degree n . This forces $e = 1$. \square

9.3.4 More on Repetitions in Ideal Factorization.

We have been considering the case when d is the discriminant of a power basis and $p \nmid d$. We have also been assuming that K is a normal extension of \mathbb{Q} .

Now let's assume that d is the discriminant of a basis $\{b_1, \dots, b_n\}$ whose \mathbb{Z} -span is all of \mathcal{O}_K . Let's keep our assumption of K over \mathbb{Q} being normal.

For this case we need to think of discriminants not only applying to fields, *but we need to relax to rings which are vector spaces. It is the same idea.*

Discriminant of a Basis of a Vector Space That is Also a Ring.

Take a vector space V over a field F which is also a ring. Let a basis for V over F be $\{b_1, \dots, b_k\}$. Let $T : V \times V \rightarrow F$ be the bilinear map defined the same as we had before: $T(v, w) = \text{tr } M_{v \cdot w}$ where $M_{v \cdot w}$ is the matrix representing the linear transformation $V \rightarrow V$ given by multiplication by $(v \cdot w)$. No matter which basis or interpretation we choose in expressing the matrix $M_{v \cdot w}$, the trace is the same. Hence, this is a well defined map. Now the discriminant of the basis $\{b_1, \dots, b_k\}$ of V is the determinant of the matrix which describes the bilinear transformation T with respect to the basis $\{b_1, \dots, b_k\}$. *This is really what we had before!*

Theorem 9.3.29

Take two rings R_1 and R_2 which are also vector spaces and consider their set product $R_1 \times R_2$ as a ring and a vector space with multiplication and addition being defined component-wise. Let \mathcal{B}_1 be a basis for R_1 and \mathcal{B}_2 be a basis for R_2 . Then let $\tilde{\mathcal{B}}_1$ be the elements $b \times 0_{R_2}$ for $b \in \mathcal{B}_1$. Similarly, we define $\tilde{\mathcal{B}}_2$. Then $\tilde{\mathcal{B}}_1 \cup \tilde{\mathcal{B}}_2$ is a basis for $R_1 \times R_2$. The discriminant of this basis is the product of the discriminants of \mathcal{B}_1 and \mathcal{B}_2 .

Proof. Any element of $\tilde{\mathcal{B}}_1$ can be written as $x = \underbrace{b}_{\in \mathcal{B}_1} \times 0_{R_2}$ and any element of $\tilde{\mathcal{B}}_2$ can be written as $y = 0_{R_1} \times \underbrace{c}_{\in \mathcal{B}_2}$. Because of component wise multiplication, $xy = 0$ so that the trace of the multiplication matrix

M_{xy} is also 0. This tells us that the matrix for the bilinear form T is a *block diagonal matrix*:

$$\begin{pmatrix} A & 0's \\ 0's & B \end{pmatrix}$$

where A is the same as the matrix for T for just the ring R_1 and B for R_2 . That is, $\det(A)$ is the discriminant of \mathcal{B}_1 and $\det(B)$ is the discriminant of \mathcal{B}_2 . The determinant of this block diagonal matrix is both the discriminant of $\tilde{\mathcal{B}}_1 \cup \tilde{\mathcal{B}}_2$ and the product of the determinants $\det(A)$ and $\det(B)$. This proves the theorem. \square

Theorem 9.3.30

The quotient ring $\mathcal{O}_K/p\mathcal{O}_K$ though not a field is a \mathbb{F}_p vector space of dimension n over \mathbb{F}_p . It is the set product of the rings \mathcal{O}_K/P_i^e each of which in turn is a \mathbb{F}_p vector space.

Proof. Notice that since multiplication by p in all of the rings in question is in P_i^e , P_i and \mathcal{O}_K . This means that \mathbb{Z} -scalars themselves can be considered mod p . All of these are vector spaces. In particular, we know from above that the size of $\mathcal{O}_K/p\mathcal{O}_K$ is p^n so that its dimension over \mathbb{F}_p must be n . \square

So now, it makes sense to think of the discriminant of all of these quotient rings thinking of them as vector spaces over \mathbb{F}_p .

Theorem 9.3.31

Suppose that $\{b_1, \dots, b_n\}$ is a basis for K over \mathbb{Q} whose \mathbb{Z} -span is all of \mathcal{O}_K . Then, $\mathcal{B} = \{b_1 + p\mathcal{O}_K, \dots, b_n + p\mathcal{O}_K\}$ is a basis for $\mathcal{O}_K/p\mathcal{O}_K$ as a \mathbb{F}_p vector space.

Proof. We have n spanning elements in a vector space $\mathcal{O}_K/p\mathcal{O}_K$ that we already know has dimension n . \square

Using the Chinese remainder theorem, we can write the vector space $\mathcal{O}_K/p\mathcal{O}_K$ as a set product of rings \mathcal{O}_K/P_i^e which are also vector spaces. Take bases of these and expand to basis of $\mathcal{O}_K/p\mathcal{O}_K$ as described in our result above for $\tilde{\mathcal{B}}_i$. Call this expanded basis $\tilde{\mathcal{B}}$.

Changing our basis from $\{b_1 + p\mathcal{O}_K, \dots, b_n + p\mathcal{O}_K\}$ to $\tilde{\mathcal{B}}$ just multiplies the discriminant by a square. Go back above and see how we when we change the basis, the matrix—call it A —for the bilinear form changes by $U^T A U$ for an unpretending matrix U with nonzero determinant. Hence, we can be sure that changing our basis over \mathbb{F}_p only multiplies the old discriminant by a nonzero element of \mathbb{F}_p . *Traces here are in \mathbb{F}_p .*

Keep in mind further that the discriminant of $\{b_1 + p\mathcal{O}_K, \dots, b_n + p\mathcal{O}_K\}$ will match the discriminant of $\{b_1, \dots, b_n\}$ after we mod this latter one by p .

We have a way of relating the discriminant of $\{b_1, \dots, b_n\}$ to $\tilde{\mathcal{B}}$. We have:

Theorem 9.3.32

The discriminant d of $\{b_1, \dots, b_n\}$ is $\equiv 0 \pmod{p}$ if and only if the discriminant of $\tilde{\mathcal{B}}$ is 0 in \mathbb{F}_p if and only if the part of $\tilde{\mathcal{B}}$ corresponding to \mathcal{O}_K/P_i^e for one of the i 's has a discriminant of 0 in \mathbb{F}_p .

Now, if $e = 1$, then $\mathcal{O}_K/P_i^e = \mathcal{O}_K/P_i$ which is a field extension of \mathbb{F}_p produced by a polynomial over \mathbb{F}_p with nonrepeating roots. Hence the discriminant with a power basis $\{1, \alpha + P_i, \alpha^2 + P_i, \dots\}$ built off of one of those roots $\alpha + P_i$ will be nonzero by our results above. Changing the basis keeps the discriminant nonzero. Hence, none of the parts of $\tilde{\mathcal{B}}$ corresponding to \mathcal{O}_K/P_i^e for any of the i 's has a zero discriminant. This can be traced back in this last theorem to saying that $p \nmid d$.

Now if $e > 1$, we know that if we take an element t of $P_1 \setminus P_1^2$ that $(t + P_1^e)^e \in P_1^e$ (that is, it is equal to 0 in \mathcal{O}_K/P_i^e) but $t + P_1^e$ is nonzero in \mathcal{O}_K/P_i^e . This means that the minimal polynomial of matrix which represents multiplication by $t + P_1^e$ in \mathcal{O}_K/P_i^e is a factor of x^e . This matrix has *zero trace*. Not only that, but any multiple of $(t + P_1^e)$ also is a root of x^e having zero trace. So, if we took a basis of \mathcal{O}_K/P_i^e which used $t + P_1^e$ as one of its elements, we would have a whole row of zeros in the bilinear matrix for T with respect to our basis for \mathcal{O}_K/P_i^e . The determinant, namely the discriminant, of this little basis for \mathcal{O}_K/P_i^e would then be 0 in \mathbb{F}_p . Tracing back the equivalences again of our last theorem, we have that $p \mid d$.

Theorem 9.3.33

Let d correspond to our basis $\{b_1, \dots, b_n\}$ whose \mathbb{Z} span is all of \mathcal{O}_K . Then, we have that $e = 1$ if and only if $p \nmid d$ and $e > 1$ if and only if $p \mid d$.

9.3.5 Quadratic Reciprocity

Notice that $3 \equiv 4^2 \pmod{13}$ so that 3 is a *square* mod 13. Also notice that $13 \equiv 1^2 \pmod{3}$ so that 13 is also a square mod 3. This is an example of the idea called quadratic reciprocity. We have nearly all of the machinery to prove that such a thing works. *We use field extensions!*

Let p and q be two different primes not equal to 2. Then how is the idea of p being a square mod q related to the idea of q being a square mod p ?

We need a couple preliminary results:

Lemma 9.3.34

The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$.

Proof. The proof of our earlier result, when we were discussing cyclotomic polynomials, that primitive roots of unity exist in \mathbb{C} works for the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ if we are taking about primitive $(p - 1)$ st roots of unity. If $\zeta \in \mathbb{F}_p$ is such a primitive root, then the smallest exponent such that $\zeta^m = 1$ is $m = p - 1$. We can label $(\mathbb{Z}/p\mathbb{Z})^\times$ as $\{\zeta, \zeta^2, \dots, \zeta^{p-1}\}$. Multiplication is the same as the addition of exponents where $p - 1$ is the smallest exponent that behaves like 0. This exponent group is isomorphic to the multiplicative group and is of the form $\mathbb{Z}/(p - 1)\mathbb{Z}$. \square

Lemma 9.3.35

Let m be a factor of $p - 1$. Then there is a unique subgroup B of $A = \mathbb{Z}/(p - 1)\mathbb{Z}$ such that $|A/B| = m$.

Proof. All subgroups of A are given as multiples of a factor of $p - 1$. For instance, if $p = 11$ then a subgroup $\mathbb{Z}/10\mathbb{Z}$ can be given as $\{ \underline{0}, \underline{2}, \underline{4}, \underline{6}, \underline{8} \}$ (multiples of 2). There is a unique subgroup B for each factor m and there are precisely $\frac{p-1}{m}$ multiples of m . The size of A/B is

$$m = \frac{p-1}{\frac{p-1}{m}}$$

 \square

Let's first assume that q is a square mod p . Let ζ_p be a p th root of unity in \mathbb{C} . Then there are $p - 1$ primitive p th roots of unity in \mathbb{C} . The extension $\mathbb{Q}(\zeta_p)$ over \mathbb{Q} has a Galois group. The automorphisms in this Galois group are given by $\zeta_p \mapsto \zeta_p^k$ for $k \in \{1, \dots, p-1\}$. Such a replacement is the same as multiplication among the exponents. Now the exponents of ζ_p live in $\mathbb{Z}/p\mathbb{Z}$ since $\zeta_p^p = 1$ with p behaving like 0. The automorphisms are given uniquely by an exponent multiplier—i.e. an element of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. Composition is the same as multiplying the two exponent multipliers together. That is, the Galois group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ which is isomorphic to $A = \mathbb{Z}/(p - 1)\mathbb{Z}$. *Already the elements of $\mathbb{Z}/p\mathbb{Z}$ represent the exponents of ζ_p .* When we move to $(\mathbb{Z}/p\mathbb{Z})^\times$ and think of it isomorphically as $\mathbb{Z}/(p - 1)\mathbb{Z}$ we have moved to the exponents of these exponents of ζ_p .

Now to discuss the “exponents of the exponents:”

We know that A which has size $p - 1$, which is even, has a unique subgroup B such that $|A/B| = 2$. This subgroup corresponds to multiples of 2. So the exponents of the exponents of ζ_p are multiples of 2 if those exponents of ζ_p (which live in $\mathbb{Z}/p\mathbb{Z}$) correspond to the elements of B . That is, B considers those elements of $\mathbb{Z}/p\mathbb{Z}$ (which are exponents of ζ_p) which are squares in $\mathbb{Z}/p\mathbb{Z}$.

If q is a square mod p , the automorphism given by $\zeta_p \mapsto \zeta_p^q$ lives in this subgroup B .

The field that B fixes has dimension 2 over \mathbb{Q} . Now, A is isomorphic to the Galois group. Since B is

unique subgroup such that $|A/B| = 2$, there is exactly one dimension 2 field over \mathbb{Q} that is contained in $\mathbb{Q}(\zeta_p)$. To find out what this field is we appeal to a discriminant calculation of the basis $\{1, \zeta_p, \dots, \zeta_{p-2}\}$ of $\mathbb{Q}(\zeta_p)$ over \mathbb{Q} (there are $p - 1$ elements in this basis since the Galois group has size $p - 1$).

Theorem 9.3.36

The discriminant of the basis $\{1, \zeta_p, \dots, \zeta_{p-2}\}$ of $\mathbb{Q}(\zeta_p)$ for $\mathbb{Q}(\zeta_p)$ over \mathbb{Q} if $p \neq 2$ is $(-1)^{\frac{p-1}{2}} p^{p-2}$

Proof. See



□

Remember that the discriminant is a square in $\mathbb{Q}(\zeta_p)$. If the square root of the discriminant is not in \mathbb{Q} , then adjoining something that will give this square root to \mathbb{Q} will yield the unique dimension 2 extension.

Since $p - 2$ is odd, to get this square root we could simply append

$$\sqrt{(-1)^{\frac{p-1}{2}} p}$$

since

$$p^{p-2} = p \cdot \underbrace{p^{p-1}}_{\text{has square root in } \mathbb{Q}}$$

This element has minimal polynomial

$$f(x) = x^2 - (-1)^{\frac{p-1}{2}} p$$

Now, let Q be a prime ideal of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ in the ideal factorization of $p\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Then $\mathcal{O}_{\mathbb{Q}(\zeta_p)}/Q$ is an extension of \mathbb{F}_q . Let's think about the Galois group of this extension of finite fields. The map $x \mapsto x^q$ is actually an automorphism of this field extension that fixes \mathbb{F}_q . This is because $x^q = x$ implies that x is a root of $x^q - x$ and so lives in \mathbb{F}_q and because

$$(x + y)^q = x^q + \underbrace{\dots}_{\text{All of the coefficients}} + y^q = x^q + y^q$$

All of the coefficients
(using binomial
coefficients) are
multiples of q .

since multiplication by q is the same as multiplication by 0. We are looking at an additive map. Exponentiation is also multiplicative.

If our extension has dimension m , then all the elements of this extension field are given as roots of $x^{q^m} - x$.

All of these roots are distinct and describe every element of this extension field. This means that the smallest m such that $x^{q^m} = x$ for all x in this field is m . Wait! this gives m distinct automorphisms $x \mapsto x^{q^k}$ where $k \in \{1, \dots, m\}$ and we know that the dimension of this normal extension is m . This means we have the whole Galois group simply from the automorphism $x \mapsto x^q$.

We know that the automorphism $x \mapsto x^q$ is also an automorphism of $\mathbb{Q}(\zeta_p)$. Since $q \nmid d$ where d is our discriminant, then the roots the minimal polynomial of ζ_p over \mathbb{Q} are all distinct when we mod out by Q . The Galois automorphisms both over \mathbb{Q} and over \mathbb{F}_q are uniquely defined by where they send these roots. Hence, modding the automorphism $x \mapsto x^q$ over \mathbb{Q} yields the corresponding automorphism $x \mapsto x^q$ over \mathbb{F}_q .

Let $K = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$. If we want to know how $q\mathcal{O}_K$ factors, realize that K is Galois over \mathbb{Q} and that $x \mapsto x^q$ fixes K because it corresponds to the subgroup B . The whole Galois group of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}/Q$ over \mathbb{F}_q then fixes $\mathcal{O}_K/\tilde{Q}_i$ for a prime ideal \tilde{Q} in the factorization of $q\mathcal{O}_K$. But the fixed field of the this Galois group is \mathbb{F}_q . Fixed fields are unique. Hence, $\mathcal{O}_K/\tilde{Q}_i$ is the same as \mathbb{F}_q . The dimension of the extension $\mathcal{O}_K/\tilde{Q}_i$ over \mathbb{F}_q is 1.

Also, we know in the factorization of $q\mathcal{O}_K$ that $e = 1$ since q is not a factor of the discriminant of the power basis above. From our element counting we had above when we thought of the number of elements (q^2) in $\mathcal{O}_K/q\mathcal{O}_K$ (since the dimension of this extension is $n = 2$) and how we could think about it across the Chinese remainder theorem, we had that

$$2 = emk$$

where k is the number of distinct prime ideal factors P_i of $q\mathcal{O}_K$ and m is the dimension of \mathcal{O}_K/P_i over \mathbb{F}_q which is 1. This forces $k = 2$. In fact, $k = 2$ if and only if q is in the subgroup B if and only if q is a square mod p .

Now since $q \nmid d$, we know how to factor $q\mathcal{O}_K$. We use the minimal polynomial $f(x)$ of $\sqrt{(-1)^{\frac{p-1}{2}} p}$ over \mathbb{Q} and then factor it mod q . The polynomial $x^2 - (-1)^{\frac{p-1}{2}} p$ is only factorable nontrivially so $k = 2$ if it factors as $(x - t)(x + t)$ for some $t \in \mathbb{F}_p$. Realize that

$$t^2 \equiv (-1)^{\frac{p-1}{2}} p \pmod{q}$$

so that $(-1)^{\frac{p-1}{2}} p$ is a square mod q . Since the implications we have made above are reversible, we have the following logical equivalence:

Theorem 9.3.37 Quadratic Reciprocity

Let p and q be two odd primes (i.e. not $= 2$). Then, q is a square mod p if and only if $(-1)^{\frac{p-1}{2}} p$ is a square mod q .

Where did we switch from mod p to mod q ?

We started in mod p with the exponents of ζ_p . The prime q is thought of as an exponent of ζ_p . It gives the automorphism $x \mapsto x^q$ of the Galois group of $\mathbb{F}_q(\zeta_p + Q)$ (for a prime ideal Q of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ that contains q) over $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$. This is the switch!

Theorem 9.3.38

$$(-1)^{\frac{p-1}{2}} = 1 \iff p \equiv 1 \pmod{4}$$

Proof. For $\frac{p-1}{2}$ to be even we must have that $p - 1$ is divisible by 4 which means that $p \equiv 1 \pmod{4}$. \square

9.3.6 Sums of Squares

We prove that if $p \equiv 1 \pmod{4}$, then p is the sum of two squares. For instance, $5 = 1^2 + 2^2$ and $13 = 2^2 + 3^2$. But this always works. Why? How? That is what we walk through.

First notice that $5 = (1+2i)(1-2i)$ and $13 = (2+3i)(2-3i)$. Hence, our question is really one about factorization in $\mathbb{Z}[i]$. We will need the following lemma:

Lemma 9.3.39

We can find gcd's in the Gaussian integers.

Proof. The Euclidean algorithm works if we can apply the division process in a natural way. Given $x, y \in \mathbb{Z}[i]$ where $|x| > |y|$, we would like to be able to write:

$$x = q \cdot y + r$$

for a quotient q and a remainder r so that $|r| < |y|$. If we divide this by y , this looks like:

$$\frac{x}{y} = q + \frac{r}{y}$$

or

$$q = \frac{x}{y} - \frac{r}{y}$$

That is, we need to be able to find $q \in \mathbb{Z}[i]$ that is within $\frac{r}{y}$ of the actual division $\frac{x}{y}$ carried out in \mathbb{C} . If we were to find $q \in \mathbb{Z}[i]$ (an integer coordinate pair in the complex plane) that was within 1 unit length of $\frac{x}{y}$ (a coordinate pair of rational numbers in the complex plane), then $|\frac{x}{y} - q| < 1$. Yet this is always possible! Every coordinate in the complex plane is within one unit of a point described by integer coordinates.

Notice that $\frac{x}{y} - q = \frac{x-qy}{y}$ so that we could take r as $x - qy \in \mathbb{Z}[i]$ where $|r| < |y|$. Since this inequality is strict and the absolute values (magnitudes) of complex numbers belong to $\{\sqrt{n} : n \in \mathbb{Z}^{\geq 0}\}$ (a set with a minimum), the remainder eventually goes to 0 so that the one right before it is the gcd. \square

Suppose that $p \equiv 1 \pmod{4}$. In particular, p is not 2 and is not a factor of the discriminant $d = 4$ of the

power basis $\{1, i\}$ of $\mathbb{Q}(i)$ over \mathbb{Q} . Also, $i^p = \sqrt{-1}^p = i$ by considering the sequence of powers

$$i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1, i^5 = i, i^6 = -1, \dots$$

Then for $x, y \in \mathbb{Z}$, we have:

$$(x + y \cdot i)^p = x^p + \underbrace{\dots}_{\text{All of the coefficients}} + y^p i^p \equiv x^p + y^p i^p \equiv x^p + y^p i \pmod{p}$$

(using binomial
coefficients) are
multiples of p .

Yet, we also know that mod p , \underline{x} and \underline{y} are in \mathbb{F}_p and all elements of \mathbb{F}_p are roots of the polynomial $x^p - x$. Therefore, $\underline{x}^p + \underline{y}^p i = \underline{x} + \underline{y}i$. Let P be a prime ideal in $\mathcal{O}_{\mathbb{Q}(i)}$ that contains p . The Galois group of $\mathcal{O}_{\mathbb{Q}(i)}/P_j$ is precisely all powers of the automorphism $(x + yi) + P_j \mapsto (x + yi)^p + P_j$. Yet we just saw that this automorphism is the identity. This tells us that the dimension of $\mathcal{O}_{\mathbb{Q}(i)}/P_i$ over \mathbb{F}_p is $m = 1$. Yet we also know that since $p \nmid 4 = d$ that $e = 1$ in this factorization. Therefore, we know for sure since the dimension $n = 2$ for this extension that

$$n = 2 = emk = 1 \cdot 1 \cdot k$$

where k is the number of distinct prime ideal factors P_j . So $k = 2$.

We know that these ideals come from the factors of the minimal polynomial $f(x) = x^2 + 1$ of i considered mod p . Namely,

$$x^2 + 1 \equiv (x - r_1)(x - r_2) \pmod{p} \implies P_j = p\mathcal{O}_{\mathbb{Q}(i)} + (i - r_j)\mathcal{O}_{\mathbb{Q}(i)}$$

But wait! We can take the gcd of p and $i - r_j$ in $\mathbb{Z}[i] = \mathcal{O}_{\mathbb{Q}(i)}$ by our lemma above. Let $a_j + b_j i$ be this gcd.

Then since $p \in P_1 P_2$, we know that

$$p\mathbb{Z}[i] = (a_1 + b_1 i)(a_2 + b_2 i)\mathbb{Z}[i]$$

which forces:

$$p = u(a_1 + b_1 i)(a_2 + b_2 i)$$

where u is a Gaussian unit. Remember what the norm $N(y)$ of an element y in $\mathbb{Z}[i]$ is? It is the determinant of the multiplication map of that element on $\mathbb{Q}(i)$ with respect to any basis. In particular, let that basis be $\{1, i\}$. This norm is multiplicative just like the determinant. Realize that multiplication by $p : \mathbb{Q}(i) \rightarrow \mathbb{Q}(i)$ is give by

$p \cdot \text{id}_{2 \times 2}$ with determinant p^2 . The element $a_1 + b_1i$ has multiplication matrix

$$a_1 + b_1i : \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix}$$

with determinant $a_1^2 + b_1^2$. So think of the equation $p = u(a_1 + b_1i)(a_2 + b_2i)$ as a matrix equation of matrices which represent the multiplication maps. Taking determinants (i.e. applying N) is multiplicative. So we have:

$$N(p) = N(u)N(a_1 + b_1i)N(a_2 + b_2i)$$

which is:

$$p^2 = \underbrace{(\pm 1)}_{u \text{ has an inverse}} \cdot (a_1^2 + b_1^2) \cdot (a_2^2 + b_2^2)$$

Since $(a_1 + b_1i)$ generates a prime ideal in $\mathbb{Z}[i]$, it does not generate all of $\mathbb{Z}[i]$ so that it does not have an inverse in $\mathbb{Z}[i]$. Therefore, the matrix describing multiplication by $(a_1 + b_1i)$ with respect to the basis 1 and i *cannot* have a determinant of ± 1 . If it did, then by our adjugate formula, we could find an inverse matrix with entries in \mathbb{Z} . The first column of this inverse matrix (the image of multiplying by 1) would represent an inverse element in $\mathbb{Z}[i]$ —a contradiction. The same is true of $a_2 + b_2i$. Therefore, the norms of these elements must be nontrivial factors of p^2 . We also know that $a_j^2 + b_j^2 > 0$. This tells us:

$$p = a_j^2 + b_j^2 \text{ for } j \in \{1, 2\}$$

Theorem 9.3.40 (Fermat)

if $p \equiv 1 \pmod{4}$, then p is the sum of two squares.

Analyzing our above proof, we have the following:

Method For Writing p as a Sum of Two Squares

If $p \equiv 1 \pmod{4}$, we can do the following:

- First factor $x^2 + 1 \pmod{p}$ as $(x - r)(x + r)$.
- Find the gcd $a + bi$ of $i + r$ and p in $\mathbb{Z}[i]$
- We will have that $p = a^2 + b^2$.

Suppose that we would like to follow these steps for the prime 13. Notice that

$$x^2 + 1 \equiv (x - 5)(x + 5) \pmod{13}$$

Therefore, we need to use the Euclidean algorithm in $\mathbb{Z}[i]$ to find the gcd of $i + 5$ and 13. The following code illustrates how we could about such a task:



[Link to run the code.](#)

```
#Euclidean Algorithm between I+5 and 13
#Since 5^2 is -1 mod 13.
#First find quotient:
print("First quotient in Complex:", (13/(I+5)).n())
print("Distance to 3 is less than 1:", (abs(13/(I+5)-3)).n())
#The quotient is within $1$ of the Gaussian Integer 3
#So compute remainder:
r=13-3*(I+5)
print("Remainder with quotient 3:", r)
print("This is a Gaussian integer.")
#Find new quotient:
print("Next quotient is Gaussian Integer:", ((I+5)/(r)).n())
print("So next remainder is 0.")
print("The previous remainder r is the gcd and so is a factor of 13.")
#This is a Gaussian integer so the new remainder is 0.
#Hence the first remainder is the gcd.
#Now try:
print("Multiply r and its conjugate:", r*conjugate(r))
#Notice that this factors 13.
#Take real^2+imag^2=4+9=13
print("The real and imaginary parts of the gcd give the result!")
print("2^2 and 3^2")
```

We have that

$$13 = 2^2 + 3^2$$

Comparison of Proofs

Notice that both in proving the sum of squares theorem and quadratic reciprocity there was a similar theme:

- Relate our desired result to a factorization in a ring of integers.
- Use a power basis for the ring of integers and have $p \nmid d$ so that we both know how to factor and that $e = 1$.
- Go to finite fields when we mod out by our relevant prime and learn about the relevant Galois group by considering $x \mapsto x^{\text{prime}}$ which generates the Galois group to determine m .
- Use the idea that $n = emk$ to find k and relate it to the factorization and make the statement we are interested in.

Which Fields in Which Proofs?

- In the proof of quadratic reciprocity, we used the fields $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$.
- In the proof of the sum of squares, we used $\mathbb{Q}(i)$.

9.3.7 Using Squares in Modular Arithmetic to Factor Large Numbers

Consider working in mod 65 arithmetic. There are four square roots of 9:

$$3^2 \equiv 23^2 \equiv 42^2 \equiv 62^2 \pmod{65}$$

There are pairs of these which are \pm in mod 65:

$$(3, 62) \quad (23, 42)$$

Naturally,

$$0 \equiv 62^2 - 3^2 \equiv (62 - 3)\underbrace{(62 + 3)}_{=65} \pmod{65}$$

If we choose two square roots a and b of 9 which are not \pm each other mod 65, then $65 \nmid a + b$ and

$65 \nmid a - b$. But, we know that $a^2 \equiv b^2 \pmod{65}$ so that $a^2 - b^2 \equiv 0 \pmod{65}$. That is, 65 is a factor of $a^2 - b^2 = (a+b)(a-b)$ yet neither a factor of $(a+b)$ nor $(a-b)$. This tells us that $\gcd(65, a+b) \neq 1$. Hence using the Euclidean algorithm between 65 and $a+b$ will reveal a factor of 65. For instance, $23+3=26$ which shares a factor of 13 with 65. Also, $23-3=20$ which shares a factor of 5 with 65.

So the question of finding factors of a number N can be reduced to finding different square roots of a number $m \pmod{N}$. Finding a good m and some of its square roots is the basis of a number of factorization techniques.

One way of finding square roots is to establish a ring homomorphism ϕ from $\mathcal{O}_K \rightarrow \mathbb{Z}$ for an extension K of \mathbb{Q} .

If we can find square roots in \mathcal{O}_K , then we can transfer them down to $\mathbb{Z}/N\mathbb{Z}$ via this ring homomorphism. Ring homomorphisms preserve multiplication and so therefore preserve the property of being a square root.

Here is an example. We follow the technique of [9, p. 503]. Other techniques are given in [6]. Suppose that we choose to look at a field extension $K = \mathbb{Q}(\alpha)$ where α has a minimum polynomial of $g(x)$. Let $\phi : \mathcal{O}_K \rightarrow \mathbb{Z}/N\mathbb{Z}$ be a ring homomorphism defined as $\phi(t(\alpha)) = dw \cdot t(m)$ where $t(\alpha) \in \mathbb{Z}[\alpha]$, d is the discriminant of the power basis $\{1, \alpha, \alpha^2, \dots\}$ and w is an integer which is a multiplicative inverse of d mod N . Such a map is well-defined if we ensure zero is sent to zero. That is, if we ensure that $g(m)$ is 0, then $g(\alpha)$ is sent to 0. We recall that $\mathcal{O}_K \subset \frac{1}{d}\mathbb{Z}[\alpha]$. The way we define ϕ is to multiply the input by d to get something in $\mathbb{Z}[\alpha]$. Then we replace α by m which is a ring homomorphism to $\mathbb{Z}/N\mathbb{Z}$. But to make this a ring homomorphism from $\frac{1}{d}\mathbb{Z}[\alpha]$ requires us to multiply by d^{-1} so that $1 \mapsto 1$. Yet we restrict the domain to \mathcal{O}_K .

Say we find an element that is a square in the ring of integers of the form $a\alpha + b$. Let M_α be the matrix for the multiplication map $K \rightarrow K$ of α . Then $a \cdot M_\alpha + b \cdot \text{id}$ is the matrix for the multiplication map $K \rightarrow K$. Finding the minimal polynomial of this matrix, we get the minimal polynomial $f(x)$ for $a\alpha + b$.

If $a\alpha + b$ has a square root γ in K , then $\alpha = \frac{\gamma^2 - b}{a} \in K$ so that $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\gamma)$. Let $s(x)$ be the minimal polynomial of γ . Then,

$$\deg(s(x)) = \deg(g(x))$$

We also know that γ is a root of $f(x^2)$. This tells us that $s(x)$ is a nontrivial factor of $f(x^2)$ of half the degree.

In fact, since the constant term of $f(x)$ (being irreducible) is nonzero, every root of $f(x)$ expands to 2 distinct roots of $f(x^2)$ (the two \pm square roots of roots of $f(x)$). The automorphism $K \rightarrow K$ that sends γ to another root γ' of $f(x)$ sends a square root of γ to a square root of γ' . This tells us that $s(x)$ has one of the \pm square roots of the roots of $f(x)$ as its own roots and $s(-x)$ has the other set. This tells us that:

$$f(x^2) = s(x)s(-x)$$

Now, $x^2 - (a\alpha + b) \in K[x]$ factors as $(x - \gamma)(x + \gamma)$. Since $(x - \gamma)$ and $(x + \gamma)$ have a gcd of 1 in $K[x]$,

we can find polynomials $r_1(x)$ and $r_2(x)$ so that

$$r_1(x)(x - \gamma) + r_2(x)(x + \gamma) = 1$$

Notice that $(x - \gamma)$ is a factor of $s(x)$ but $x + \gamma$ is not a root of $s(x)$. It is a root of $s(-x)$. Now notice by multiplying our equation by $s(x)$:

$$r_1(x)(x - \gamma)s(x) + \underbrace{r_2(x)(x + \gamma)s(x)}_{\text{multiple of } x^2 - (a\alpha + b)} = s(x)$$

Thus,

$$s(x) \equiv r_1(x)(x - \gamma)s(x) \pmod{x^2 - (a\alpha + b)}$$

This tells us that

$$s(\gamma) \equiv 0 \pmod{x^2 - (a\alpha + b)}$$

This is the key for how we will find the square root of $a\alpha + b$ in K . We look at a simple representative of the coset $s(x) + (x^2 - (a\alpha + b))K[x]$ and then solve for the x value in $K[x]$ that would make this 0.

We find the simple representative via division. Suppose that $s(x) = x^3 + b_1x^2 + b_2x + b_3$. Then, we can use generalized synthetic division to divide $s(x)$ by $x^2 - (a\alpha + b)$:

$$\begin{array}{c|cccc} & 1 & b_1 & b_2 & b_3 \\ 0 & & 0 & 0 & \\ (a\alpha + b) & & & (a\alpha + b) & b_1(a\alpha + b) \\ \hline 1 & b_1 & b_2 + (a\alpha + b) & b_3 + b_1(a\alpha + b) \\ & & (b_2 + (a\alpha + b))x + (b_3 + b_1(a\alpha + b)) \\ & & & \text{remainder} \end{array}$$

Now we set the remainder equal to 0 and solve for x :

$$(b_2 + (a\alpha + b))x + (b_3 + b_1(a\alpha + b)) = 0$$

$$x = \frac{-(b_3 + b_1(a\alpha + b))}{(b_2 + (a\alpha + b))}$$

This is γ . That is, we just found a square root of $a\alpha + b$ in K . Is this element in \mathcal{O}_K ? We know that $s(x)$ is its minimal polynomial. Remember that \mathcal{O}_K is a ring. This implies that $a\alpha + b \in \mathcal{O}_K$ so its minimal polynomial $f(x)$ is in $\mathbb{Z}[x]$. We found $s(x)$ as a factor of $f(x^2)$ in $\mathbb{Z}[x]$. So yes it is in \mathcal{O}_K .

What about its denominator? Call the denominator d' . If we only use ϕ once or we just want a homomorphism to $\mathbb{Z}/N\mathbb{Z}$ that has γ in its domain, it does not matter that we find d' to define ϕ . Why don't we *redefine*

ϕ as:

$$\phi : \frac{1}{d'}\mathbb{Z}[\alpha] \rightarrow \mathbb{Z}/N\mathbb{Z} \quad \phi(t(\alpha)) = \underline{d'w \cdot t(m)}$$

where $t(\alpha) \in Z[\alpha]$.

With

$$\gamma = \frac{-(b_3 + b_1(a\alpha + b))}{(b_2 + (a\alpha + b))}$$

we have that $\phi(\gamma)$ is a square root of $\phi(a\alpha + b) = \underline{am + b}$ in $\mathbb{Z}/N\mathbb{Z}$.

The following code illustrates how we can use these ideas to find square roots of $9 \pmod{65}$ without specifically ever using knowledge of how 65 factors. It outputs 3 of the square roots of $9 \pmod{65}$ which is all we need!



[Link to run the code.](#)

```
#Set things up. We are looking for square roots of 9 mod 65.
#This x will be an algebraic integer giving a field extension K=Q(x)
x = polygen(QQ, 'x')
#This X represents the square root we are looking for
X = polygen(QQ, 'X')
N=65
t=9

#Each m determines a homomorphism phi:x->m from O_K to Z/NZ
for m in range(30)[2:]:
    #Cycle Through different number fields K=Q(x) where x->m
    #gives a homomorphism from the ring of integers to Z/NZ
    for a1 in [-3..0]:
        for a2 in [-3..3]:
            a3=65-m^3+a1*m^2-a2*m
            #g is the minimal polynomial giving the field extension
            g=x^3-a1*x^2+a2*x+a3
            #We of course make sure that this minimal polynomial is irreducible:
            if len(g.factor())==1:
                #Cycle through ax+b in the field that map to t=9 via phi
                for a in range(20):
                    #This ensures ax+b will map to 9:
                    b=t-a*m
                    q=a*x+b
                    #Compute the minimal polynomial f(X) of ax+b and replace X with X^2
                    #So X^2=ax+b
                    f=(a*companion_matrix(g)+b*matrix.identity(3)).minpoly()(x=X^2)
                    #Finding the square root of ax+b is transferred to factoring the polynomial f(X):
                    F=factor(f)
                    if (f).degree()>3 and len(F)>1:
                        #Find s(x)
                        s=F[0][0]
                        #Extract the coefficients of s(X)
                        b1=derivative(s,X,2)(X=0)/2
                        b2=derivative(s,X)(X=0)
                        b3=s(X=0)
                        #We use our calculation in the text to get the square root of ax+b
                        #from s(X). Then we send it through phi:
                        if gcd((a*x+b+b2)(x=m),65)==1:
                            sr=mod(inverse_mod(int(-(a*x+b+b2)(x=m)),65)*int(b1*q(x=m)+b3),65)
                            print("square root of 9 mod 65: "+str(sr))
```

Notice that $(-3)^2 = 3^2 = 9$ gives two obvious square roots ± 3 of $9 \bmod 65$. The other square roots are a result of some square integer larger than 65 being reduced mod 65 down to 9. *We need some of these “wrapping” kinds of squares mod 65 so that we can find a factor of 65.* The first two square roots in the above code find come from this “wrapping around” in the mod. They are found by a homomorphism ϕ that takes squaring in a subset of \mathbb{C} (we are in field extensions of \mathbb{Q}) down to $\mathbb{Z}/65\mathbb{Z}$.

This is kind of amazing! We take an algebraic complex number with the right map down to a square root of 9 in $\mathbb{Z}/65\mathbb{Z}$. The homomorphism itself is a kind of symmetry that allows us to pass from subsets of the complex numbers down to $\mathbb{Z}/65\mathbb{Z}$ to give us useful information about it.

Computationally in our code, however, we are just working with polynomials!

9.3.8 General Number Field Sieve

How easy is it to find algebraic integers with square roots in field extensions of \mathbb{Q} just randomly as we did in the code above *paired with a corresponding homomorphism to $\mathbb{Z}/N\mathbb{Z}$ that is well-defined?*

Maybe we should ask first:

How many squares are there in $\mathbb{Z}/N\mathbb{Z}$ as N gets large?

Let's just assume momentarily that N is the product of just two primes which are about \sqrt{N} in magnitude. As $N \rightarrow \infty$, this assumption tells us that the ratio of $\phi(N)$ (which is about $(\sqrt{N} - 1)^2$ in magnitude) to N becomes “about” 1. This means that almost all numbers share no common factors with N . Among these, with a margin of error proportional to $\sqrt{N} \log(N)$, there are nearly $\frac{N}{2}$ squares [7, p. 135]. This is a lot of squares!

But the problem we are dealing with is not which ones are squares as much as how to *coordinate* elements of \mathcal{O}_K and their square roots to $\mathbb{Z}/N\mathbb{Z}$. We are linking elements in subsets of \mathbb{C} like \mathcal{O}_K to elements in $\mathbb{Z}/N\mathbb{Z}$ via homomorphisms.

- Find a field extension so that the ring of integers has a nice homomorphism to $\mathbb{Z}/N\mathbb{Z}$.
- Find an element of this ring of integers that is a square and maps to a coset of $\mathbb{Z}/N\mathbb{Z}$ that contains a known square integer.
- Now find the square roots. We can just find the integer square root using ordinary means.
- To find the other, we take the square root of the element in the field extension thinking about it being in a ring of integers of a field extension of \mathbb{Q} . Then we use the coordinating homomorphism to send it to hopefully a different square root in $\mathbb{Z}/N\mathbb{Z}$ that is not \pm the other.

Just finding a square root mod N without going to a field extension may be just as hard as factoring N itself! Making this coordination can be challenging too! Still, even taking the square root of an element using polynomials in the way we have described involves one necessary polynomial factorization. What if the coefficients or the degree is too large? See [6] for alternate square root techniques in \mathcal{O}_K . Yet still it pays off and yields a very fast technique even for very large numbers! In general, a “sieving” technique is used.

A “sieve” or a “strainer” strains out what we don’t want and focuses on what we do want.

The main idea is to go through elements $a\alpha + b$ in \mathcal{O}_K for some field K and determine if $(a\alpha + b)\mathcal{O}_K$ factors into a product of ideals from a list we have chosen *with no repetitions*. We also want to know if $\phi(a\alpha + b)$ where ϕ is as above is an integer which factors into primes from a list we have chosen (with no repetition).

If we find such a $a\alpha + b$ in our sieving, then we add in a few more checks to create a vector of “exponents” for $a\alpha + b$ corresponding to the prime ideals in \mathcal{O}_K , our primes in \mathbb{Z} , or to our checks that we made. The entries in this vector will be 0’s or 1’s. When we multiply different $a\alpha + b$ to make one product and different $\phi(a\alpha + b) = a \cdot m + b$ together to make another product, these exponents add. We are interested in both products being squares. So we want all these exponents to be even—that is, 0’s in $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$.

Now line all the vectors as rows in a matrix. We are interested in finding row vectors for which when we send them into this row matrix function we get a zero vector. We want a vector in the row interpretation kernel of this matrix.

This kernel vector will tell us which rows to add to get 0’s. That is, it tells us which elements to multiply so that both of our products are squares. Realize that both our products are linked via the homomorphism ϕ . *This ϕ hopefully will introduce a mod N wrap around to get a different square root!*

Now, let’s discuss the prime ideals that we select from \mathcal{O}_K .

We choose prime ideals P in \mathcal{O}_K such that if the integer prime $p \in P$, then $p \nmid d$ where d is the discriminant of the power basis $\{1, \alpha, \alpha^2\}$. We further assume that these ideals P come from factors $(x - r)$ of the minimal polynomial $f(x)$ of α considered mod p . That being the case, the ideals are thought of as being pairs (r, p) where

$$f(r) \equiv 0 \pmod{p}$$

These ideals are of the form:

$$p\mathcal{O}_K + (\alpha - r)\mathcal{O}_K$$

Norm of Ideal

Let the norm of an ideal A , denoted as $N(A)$ in \mathcal{O}_K be the index $[\mathcal{O}_K : A]$

Norm of an Element

Let $N(w)$ denote the norm of the element w . This is given by the determinant of a matrix for the multiplication \mathbb{Q} -linear transformation $K \rightarrow K$ given by w —and equivalently this is given as the product of $\phi_i(w)$ where ϕ_i ranges through the ring homomorphisms $K \rightarrow \mathbb{C}$ which fix \mathbb{Q} .

Theorem 9.3.41

Let $w \in \mathcal{O}_K$. Then:

$$N(w\mathcal{O}_K) = N(w)$$

Proof. The determinant of the multiplication map for w is the index $[\mathcal{O}_K : w\mathcal{O}_K]$. \square

Theorem 9.3.42

Let P be the type of prime ideal of \mathcal{O}_K we mentioned above that we are considering. These are of the kind $p\mathcal{O}_K + (\alpha - r)\mathcal{O}_K$ where $p \nmid d$. Then, $N(P) = P$.

Proof. Just note that

$$[\mathcal{O}_K : P] = [\mathbb{F}_p[x] : (x - r)\mathbb{F}_p[x]]$$

We know that $\mathbb{F}_p[x]/(x - r)\mathbb{F}_p[x]$ is a one dimensional \mathbb{F}_p vector space with p elements. Hence, $[\mathcal{O}_K : P] = p$. \square

Theorem 9.3.43

To check to see if we have a complete factorization of $(a\alpha + b)\mathcal{O}_K$ into prime ideals $p_i\mathcal{O}_K + (\alpha - r_i)\mathcal{O}_K$ of the kind we desire, we check to see if:

$$(-a)^d \cdot f\left(-\frac{b}{a}\right) = \underbrace{\prod}_{\text{product}} p_i$$

where d is the degree of $f(x)$.

Proof. Let's assume that $d = 3$. Suppose that α, α_1 , and α_2 are the roots of $f(x)$. Then $f(x) = (x - \alpha)(x - \alpha_1)(x - \alpha_2)$.

$$N(a\alpha + b) = (a\alpha + b)(a\alpha_1 + b)(a\alpha_2 + b)$$

because the ring homomorphisms are completely determined by the image of α which can only come from the α_i . When we factor $(-a)^3$ out of this product, $(-a)$ from each factor, we arrive at:

$$\begin{aligned} & (-a)^d \cdot \left(\frac{b}{a} - \alpha \right) \left(\frac{b}{a} - \alpha_1 \right) \left(\frac{b}{a} - \alpha_2 \right) \\ & = (-a)^d \cdot f \left(-\frac{b}{a} \right) \end{aligned}$$

Yet this norm should also be equal to the index of $(a\alpha + b)\mathcal{O}_K$ in \mathcal{O}_K .

Suppose that we have two distinct prime ideals P_1 and P_2 . Let $y \in P_1 \setminus P_1P_2$. Then define the map $\mathcal{O}_K \rightarrow P_1/P_1P_2$ by

$$x \mapsto (xy + P_1P_2) \in P_1/P_1P_2$$

The range “unmods” to an ideal of \mathcal{O}_K . By unique factorization by prime ideals and since this map is nonzero, the range must be all of P_1/P_1P_2 . The kernel contains all of P_2 . If $x \notin P_2$, then $xy \notin P_1P_2$ so that the kernel is P_2 . We are already assuming that $y \notin P_2$. So we are saying if neither x nor y are in P_2 , then $xy \notin P_2$. This is logically equivalent to the definition of a prime ideal—just applied to P_2 .

Hence, modding \mathcal{O}_K by this kernel, \mathcal{O}_K/P_2 is isomorphic to P_1/P_1P_2 . We have:

$$[\mathcal{O}_K : P_1P_2] = [\mathcal{O}_K : P_1] \underbrace{[P_1 : P_1P_2]}_{[\mathcal{O}_K : P_2]}$$

The norm of ideals defined as indices is multiplicative!

Since we know that the norm of each prime ideal P of the form we are considering which divides $(a\alpha + b)\mathcal{O}_K$ has $[\mathcal{O}_K : P] = p$ where p is a prime integer in P , then if the factorization of $(a\alpha + b)\mathcal{O}_K$ is complete with these without repetition,

$$N((a\alpha + b)\mathcal{O}_K) = \prod_{\text{product}} p_i$$

as desired. □

General Number Field Sieve

This is the algorithm that steps through the above process to find two integers that represent the same square mod N . The gcd of the difference of these two integers with N hopefully reveals a factor of N .

The following code gives an example of this process. See [9] for a complete description. A link is given to

an environment where you can run and modify the code as desired.



[Link to run the code.](#)

```
#Let's See if we can find a factor of a number we already
#know how it factors using the General Number Field Sieve:
N=101*97*23
print("Factor N =", N)

#We will choose an algebraic field extension K=Q(x)
#where our homomorphism phi:O_K-->Z/NZ will have x |-> m
#We will adjust phi as necessary in the future so:
#phi(fraction)=phi(dd*numerator)*phi(dd*(inverse of denominator))*Inversemod(dd)
#where dd=appropriate integer.
m=34
print("Use m =",m)
a1=int((N-m^3)/m^2)
a2=int((N-m^3-a1*m^2)/m)
a3=N-m^3-a1*m^2-a2*m

RQ.<x> = PolynomialRing( QQ )
#This is the minimal polynomial of x:
g=x^3+a1*x^2+a2*x+a3
f(x)=x^3+a1*x^2+a2*x+a3
d=f.degree(x)
print("Minimal Polynomial of Primitive Element of Field Extension:",g)
```

```
#We choose prime integers in Z:  
#Rational Factor Base:  
R=prime_range(2,40)#Primes()[:10]  
print("Rational Factor Base:", R)  
  
  
#We choose prime ideals in O_K.  We are choosing  
#prime ideals of the form pO_K+(x-i)O_K.  Choosing integer primes p  
#that do not divide the discriminant, this comes from a factor (x-i) of  
#g(x)=f(x) mod p.  So i is a root mod p of f(x).  We represent these ideals  
#as pairs (i,p):  
#We do no discriminant check--just probabilistically, we assume we are ok...  
#Algebraic Factor Base:  
A=[]  
for p in prime_range(90):  
    for i in range(p):  
        if int(f(i))%p==0:  
            A+=[(i,p)]  
  
print("Algebraic Factor Base:", A)  
  
#We choose even more prime ideals in O_K  
#These will serve to ensure what we find are squares.  
#Quadratic Factor Base:  
R2=prime_range(96,120)  
Q=[]  
for p in R2:  
    for i in range(p):  
        if int(f(i))%p==0:  
            Q+=[(i,p)]  
  
print("Quadratic Factor Base:", Q)
```

```

#Checks if phi(ax+b) for ax+b in O_K has
#only small integer prime factors--that is only from our list
#and exactly one of them (called smooth numbers)
def check_rational(a,b):
    t=a*m+b
    for i in range(len(R)):
        p=R[i]
        while t%p==0 and t!=0:
            t=t/p
    if t==1 or t==-1:
        return true
    return false

#Checks to see if (ax+b)O_K factors completely
#into the prime ideals of our algebraic factor base.
#We check if the norm(ax+b) matches the product of
#norms of the primes (i,p) of the factor base
#Norm(i,p)=p
#If r_1, r_2, r_3 are the roots of f(x),
#Norm(ax+b)=(ar_1+b)(ar_2+b)(ar_3+b)
#for which (-a)^d*f(-b/a) is just a rearrangement.
def check_algebraic(a,b):
    Y=[]
    for i in range(len(A)):
        h=A[i]
        if (a*h[0]+b)%h[1]==0:
            Y+=[h]
    pR=prod([h[1] for h in Y])
    if abs(pR)==abs(int((-a)^d*f(-b/a))):
        return true
    return false

#Predicts whether (ax+b) could be a square or not mod one of our
#extra prime ideals in O_K. Realize that O_K/(One of these Primes)
#is isomorphic to Z[x]/(x-h[0])Z[x] which is isomorphic to Z/pZ
#Let psi:O_K-->Z/pZ give this map. Note that x|->h[0].
#We compute kronecker(psi(ax+b)) where
#kronecker checks if something like w is a square in Z/pZ
#which is true if and only if w^((p-1)/2) is 1 mod p
def quadratic_residue(a,b):
    Y=[]
    v=vector(len(Q)*[0])
    for i in range(len(Q)):
        h=Q[i]
        if kronecker(a*h[0]+b,h[1])!=1:
            Y+=[h]
            v+=vector(makevector(i+1,len(Q)))
    return v

#To be a square in Z/nZ, we require phi(ax+b)>0.
def signof(a,b):
    if a*m+b>0:
        return [0]
    else:
        return [1]

```

```

#An auxiliary function:
def makevector(x,y):
    return (x-1)*[0]+[1]+(y-x)*[0]

#Turns factorization information of phi(ax+b) in Z
#into a vector of exponents corresponding to prime factors
def rational_vector(a,b):
    v=vector(len(R)*[0])
    t=a*m+b
    for i in range(len(R)):
        p=R[i]
        while t%p==0 and t!=0:
            t=t/p
            v+=vector(makevector(i+1,len(R)))
    return v

#Turns factorization information of (ax+b)O_K
#into a vector of exponents corresponding to prime ideal factors
def algebraic_vector(a,b):
    Y=[]
    v=vector(len(A)*[0])
    for i in range(len(A)):
        h=A[i]
        if (a*h[0]+b)%h[1]==0:
            Y+=[h]
            v+=vector(makevector(i+1,len(A)))
    return v

```

```

#Goes through a list of elements ax+b in O_K and performs the checks on each element
#to see if it is a good candidate for vector of exponents.
L=[]
for a in [1..41]:
    for b in [-400..400]:
        if check_rational(a,b) and check_algebraic(a,b):# and check_algebraic(a,b):
            L+=[(a,b)]

print("Elements ax+b that we can extract exponents from to find squares:")
print(L)

#For each of the elements ax+b that check out, form a vector of exponents:
ML=[]
for h in L:
    a=h[0]
    b=h[1]
    v1=rational_vector(a,b)
    v2=algebraic_vector(a,b)
    v3=quadratic_residue(a,b)
    row=signof(a,b)+list(v1)+list(v2)+list(v3)
    ML+=[row]

#We want sums of exponents to be even so we get a square integer
#and a square element in O_K. So we put these vectors of exponents
#as rows in a matrix with entries in Z/2Z=F_2.
M=matrix(GF(2),ML)
print("Row interpretation matrix of exponent data for selected ax+b")
print(M)

#Choose a vector in the kernel of the basis:
kv=list(M.kernel().basis()[0])
print("Vector in Kernel: \n", vector(kv))
print("Use this vector as exponents to find...")

#Use this kernel vector to determine which phi(ax+b) to multiply
#together to get our square integer rr.
rr=1
for i in range(len(L)):
    if kv[i]==1:
        rr*=L[i][0]*m+L[i][1]
print("Square in Z:", rr)

#Use this kernel vector again to determine which ax+b to multiply
#together to get our square element of O_K
RQ.<x> = PolynomialRing( QQ )
aa=1
for i in range(len(L)):
    if kv[i]==1:
        #Reduce mod g at each step!
        aa=aa*(L[i][0]*x+L[i][1])%g
#Now aa is the square.
print("Square in O_K:", aa)

```

```

#Set things up so we can do polynomial division in Q(t)[y] where t=x
FD.<t>= FunctionField(QQ)
RY.<y> = PolynomialRing( FD )

#Find the multiplication matrix for the element x of Q(x)
Mg=companion_matrix(g)
#Use this to find the multiplication matrix for aa and then
#the minimal polynomial of aa
tt=((derivative(aa,x,2)(x=0)/2)*Mg^2 +derivative(aa,x)(x=0)*Mg
                                         +aa(x=0)*matrix.identity(3)).minpoly()

#Compute the square root of aa. Since tt(x=x^2) factors nontrivially,
#aa will have a square root in the ring of integers.
F=factor(tt)
h=F[0][0]
zz=h(x=y)%(y^2-aa(x=t))

#The square root is -(constant term)/(y coefficient) of zz.
#We express dividing by the y coefficient as
#multiplying by a polynomial by finding its inverse u.
#The denominator dd occurring in u is a factor of the discriminant of the number field.
zzz0=zz(y=0).numerator()
zzz=derivative(zz,y)(y=0)
var('t')
q, u, v = zzz.numerator()(t=x).xgcd( g )
HH=[u(x=0),derivative(u,x)(x=0),derivative(u,x,2)(x=0)/2]
dd=lcm([h.denominator() for h in HH])

#Calculate the image of the square root from O_K
#to Z/NZ via phi with discriminant adjustment
try:
    onesqrt=mod(int(-zzz0(t=m)*(dd*u(x=m)))*inverse_mod(dd,N),N)
    othersqrt=mod(sqrt(rr),N)

    #Print Results:
    print("Square roots translated to Z/NZ:",onesqrt,othersqrt)
    print("Let's just see if either square root is +/- the other mod N")
    print(mod(onesqrt-othersqrt,N)==mod(0,N) or mod(onesqrt+othersqrt,N)==mod(0,N))
    print("Trying to find a factor:", gcd(onesqrt-othersqrt,N))
    print("Trying to find a factor:", gcd(onesqrt+othersqrt,N))
except:
    print("Found Factor:", gcd(dd,N))

```

Key Concepts from this Section

- **trace bilinear form:** (page 1119) Let K be a field extension of \mathbb{Q} of finite dimension. We define the trace form $T : K \times K \rightarrow \mathbb{Q}$ to be the map $(a, b) \mapsto \text{tr}(a \cdot b)$ where we take the trace of any matrix representing the multiplication action of (ab) thought of as a map $K \rightarrow K$.
- **changing the basis of a bilinear form:** (page 1120) Suppose that the matrix A represents a bilinear transformation T having a column input and a row input. Then suppose that U is the “unpretending

matrix" for a new basis. Then

$$U^T A U$$

represents the bilinear transformation with respect to this new basis.

- **discriminant of a basis:** (page 1120) Let K be a field extension of \mathbb{Q} of finite dimension and suppose that $\mathcal{B} = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is a basis for K over \mathbb{Q} . Then, we define the discriminant of \mathcal{B} to be the determinant of the trace bilinear form $(a, b) \mapsto \text{tr}(ab)$ written as a $n \times n$ bilinear matrix with respect to the basis \mathcal{B} in both inputs.
- **theorem 9.3.1 :** (page 1121) If $a \in \mathcal{O}_K$, the ring of integers of K , then $\text{tr}(a) \in \mathbb{Z}$.
- **theorem 9.3.2 :** (page 1122) We have a description of the ring of integers of $\mathbb{Q}(i)$:

$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z} + \mathbb{Z} \cdot i$$

- **gaussian integers:** (page 1122) We call the ring of integers of $\mathbb{Q}(i)$ the *Gaussian Integers*. It is the set $\mathbb{Z} + \mathbb{Z} \cdot i$.
- **theorem 9.3.3 :** (page 1123) Let \mathcal{B} be a basis for K (a field which is finite dimensional) over \mathbb{Q} such that \mathcal{B} is also a generating set over \mathbb{Z} for \mathcal{O}_K . Then if p is a prime which is not a factor of the discriminant of B , then p cannot have α^2 as a factor for any *nonunit* (explained below) $\alpha \in \mathcal{O}_K$. On the other hand, if p is a factor of the discriminant, then such a factorization of α^2 is possible.
- **unit in a ring:** (page 1123) An element u of a ring R is called a unit of R if u has a multiplicative inverse $u^{-1} \in R$.
- **prime gaussian integer:** (page 1123) Let $a + bi \in \mathcal{O}_{\mathbb{Q}(i)}$. Then $a + bi$ is a prime Gaussian integer if and only if its only factorizations can be expressed as units multiplied to $a + bi$. In particular, though not necessary, this happens when $a^2 + b^2$, the norm of $a + bi$ in the field extension $\mathbb{Q}(i)$ over \mathbb{Q} , is a prime number.
- **theorem 9.3.4 :** (page 1124) Every algebraic number is only a multiple of \mathbb{Z} away from an algebraic integer.
- **theorem 9.3.5 :** (page 1126) Let \mathcal{B} be a basis for K (a field which is finite dimensional) over \mathbb{Q} such that it has a discriminant which is square-free. Then, we know that \mathcal{B} generates \mathcal{O}_K over \mathbb{Z} .
- **theorem 9.3.6 :** (page 1127)

$$\mathcal{O}_{\mathbb{Q}(\sqrt{5})} \subset T^{-1}(\mathbb{Z}^2) \subset \frac{1}{d} \cdot (\mathbb{Z} \cdot \alpha + \mathbb{Z} \cdot \beta)$$

This can be generalized to any ring of integers \mathcal{O}_K where K is a field extension of dimension n over \mathbb{Q} , \mathbb{Z}^2 is replaced by \mathbb{Z}^n , and $\{\alpha, \beta\}$ is replaced by an appropriate basis. Notice that $\{\alpha, \beta\}$ do not have to generate \mathcal{O}_K over \mathbb{Z} .

- **theorem 9.3.7 :** (page 1128) The discriminant of a power basis $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ of a field K over \mathbb{Q} is *always* the square of the product of differences of distinct roots of the minimal polynomial of α . *Note: the generalization of matrix B in our discussion above is called a Vandermonde matrix.*
- **theorem 9.3.8 :** (page 1128) Any matrix describing T will have a nonzero determinant. In particular, the column interpretation map of the matrix will be injective.
- **$\mathbb{Z}[\alpha]$:** (page 1129) The set $\mathbb{Z}[\alpha]$ simply means $\mathbb{Z}[x]$ with x replaced by α . So this includes expressions like $2\alpha^3 - 5\alpha + 7$.
- **theorem 9.3.9 :** (page 1129) Let $\alpha \in \mathcal{O}_K$, then the ring $\mathbb{Z}[\alpha]$ is isomorphic to $\mathbb{Z}[x]/f(x)\mathbb{Z}[x]$ where $f(x)$ is the minimal polynomial for α .
- **index $[A : B]$:** (page 1130) We let $[A : B]$ denote the number of cosets of B in A . We call the number $[A : B]$ the *index* of B in A .
- **theorem 9.3.10 :** (page 1130) If $A \supset B \supset C$ are commutative additive groups, then:

$$[A : B] \cdot [B : C] = [A : C]$$

- **$a | b$:** (page 1131) This is read as “ a is a factor of b ” which can also be said as “ a divides b .
- **theorem 9.3.11 :** (page 1131)
$$[\mathcal{O}_K : p\mathcal{O}_K] = p^n$$
- **unmodding:** (page 1134) To *unmod* is to replace cosets by the elements in the coset. To *mod* is to replace elements in a coset chunk with the coset label itself. *We back out of a quotient when we unmod and go into a quotient when we mod.*
- **ideals:** (page 1134) The types of subsets that we have arrived at in \mathcal{O}_K are examples of what are called *ideals*. These are additive subgroups which are closed by any outside multiplication of elements in the ring \mathcal{O}_K . For instance, $3\mathbb{Z}$ is an ideal of \mathbb{Z} .
- **containment and factorization:** (page 1134) If an element is contained in an ideal, that ideal has a factor of that element.
- **factoring in \mathcal{O}_K :** (page 1135) When we talk about factoring in \mathcal{O}_K we usually mean in terms of *ideals* instead of elements. The multiplication is *set multiplication*. So we are really *factoring sets* instead of elements. Yet in reality we do this all of the time in \mathbb{Z} . For instance, $10 = 2 \cdot 5$ is the same thing as $10\mathbb{Z} = 2\mathbb{Z} \cdot 5\mathbb{Z}$.
- **theorem 9.3.12 :** (page 1135) Let A be an ideal of a ring R . Then R/A is a ring.
- **$a | b$:** (page 1136) This is read as “ a is a factor of b ” which can also be said as “ a divides b .

- **maximal ideal:** (page 1136) Let M be an ideal of a ring R such that there is no ideal A such that $M \subsetneq A \subsetneq R$. Then M is called a maximal ideal.
- **theorem 9.3.13 :** (page 1136) Let M be a maximal ideal of a ring R . Then the quotient ring R/M is a field. Conversely, if R/M is a field, then M is maximal.
- **prime ideal:** (page 1137) A prime ideal is an ideal P of R such that the zero coset is *not* a multiple of a nonzero element (i.e. coset) in the quotient R/P .
- **theorem 9.3.14 :** (page 1137) Maximal ideals are prime ideals.
- **zero divisor:** (page 1138) A zero divisor a in a ring R is a nonzero element such that some multiple of it like ab where $b \in R$ is equal to zero.
- **theorem 9.3.15 :** (page 1138) Each ideal in \mathcal{O}_K is a set. Every ideal of \mathcal{O}_K is a *set product* of prime ideals. This product is unique.
- **corollary 9.3.16 :** (page 1138) Let p be a prime number in \mathbb{Z} . Then we have the *unique* factorization:

$$p\mathcal{O}_K = P_1^{e_1} \cdots P_k^{e_k}$$

where P_1, \dots, P_k are the distinct prime ideals that contain p .

- **theorem 9.3.17 :** (page 1139) Suppose that K/\mathbb{Q} is a normal extension. Let ϕ be an element of the Galois group of this extension. If P is a prime ideal in \mathcal{O}_K that contains $p \in \mathbb{Z}$ (so could contain factors of p), then $\phi(P)$ is another prime ideal of \mathcal{O}_K that also contains p . Further, \mathcal{O}_K/P and $\mathcal{O}_K/\phi(P)$ are isomorphic.
- **corollary 9.3.18 :** (page 1139)

$$[\mathcal{O}_K : P] = [\mathcal{O}_K : \phi(P)]$$

- **corollary 9.3.19 :** (page 1139) There is a number e such that our factorization of the ideal $p\mathcal{O}_K$ becomes:

$$p\mathcal{O}_K = P_1^e \cdots P_k^e$$

- **theorem 9.3.20 :** (page 1139) All prime ideals in \mathcal{O}_K are maximal.
- **theorem 9.3.21 :** (page 1140) Let p be a prime element of \mathbb{Z} and suppose that $p \in P$ where P is a prime ideal of \mathcal{O}_K . Then, the field $\mathbb{Z}/p\mathbb{Z}$ sits injectively inside of \mathcal{O}_K/P . In particular, there is only one integer prime p which can live in P .
- **theorem 9.3.22 :** (page 1141) All finite dimensional field extensions of \mathbb{F}_p have Galois groups.
- **corollary 9.3.23 :** (page 1142) Irreducible polynomials over \mathbb{F}_p have no repeated roots.

- **theorem 9.3.24 :** (page 1142) The automorphisms of G that send roots $\alpha_j + P$ of $r(x)$ to other roots $\alpha_i + P$ of $r(x)$ make up a subgroup of G . We denote it as D_P . It is isomorphic to the Galois group of \mathcal{O}_K/P over \mathbb{F}_p . We are still assuming that $p \nmid d$.
- **theorem 9.3.25 :** (page 1143) Consider the field extension $\mathcal{O}_K/P = F(\alpha)$ of \mathbb{F}_p where $r(x)$ is the minimal polynomial of α . Then $P = p\mathcal{O}_K + r(\alpha)\mathcal{O}_K$.
- **corollary 9.3.26 :** (page 1143) The dimension of \mathcal{O}_K/P over $\mathbb{F}_p(\alpha)$ is the same as the degree of $r(x)$.
- **theorem 9.3.27 :** (page 1143) Suppose that $r_1(x)$ and $r_2(x)$ are two *distinct* irreducible factors of $f(x)$. Then, the two prime ideals $P_1 = p\mathcal{O}_K + r_1(\alpha)\mathcal{O}_K$ and $P_2 = p\mathcal{O}_K + r_2(\alpha)\mathcal{O}_K$ are also distinct.
- **chinese remainder theorem for ideals:** (page 1144)

$$\mathbb{F}_p^n = \mathbb{Z}^n/p\mathbb{Z}^n \cong \mathcal{O}_K/p\mathcal{O}_K = \mathcal{O}_K/P_1^e \cdots P_k^e \cong \mathcal{O}_K/P_1^e \times \cdots \times \mathcal{O}_K/P_k^e$$

- **corollary 9.3.28 :** (page 1145) In our case when $p \nmid d$, then $e = 1$. That is, there are no repeated factors in the ideal factorization of $p\mathcal{O}_K$.
- **discriminant of a basis of a vector space that is also a ring.:** (page 1146) Take a vector space V over a field F which is also a ring. Let a basis for V over F be $\{b_1, \dots, b_k\}$. Let $T : V \times V \rightarrow F$ be the bilinear map defined the same as we had before: $T(v, w) = \text{tr } M_{v \cdot w}$ where $M_{v \cdot w}$ is the matrix representing the linear transformation $V \rightarrow V$ given by multiplication by $(v \cdot w)$. No matter which basis or interpretation we choose in expressing the matrix $M_{v \cdot w}$, the trace is the same. Hence, this is a well defined map. Now the discriminant of the basis $\{b_1, \dots, b_k\}$ of V is the determinant of the matrix which describes the bilinear transformation T with respect to the basis $\{b_1, \dots, b_k\}$. *This is really what we had before!*
- **theorem 9.3.29 :** (page 1146) Take two rings R_1 and R_2 which are also vector spaces and consider their set product $R_1 \times R_2$ as a ring and a vector space with multiplication and addition being defined component-wise. Let \mathcal{B}_1 be a basis for R_1 and \mathcal{B}_2 be a basis for R_2 . Then let $\tilde{\mathcal{B}}_1$ be the elements $b \times 0_{R_2}$ for $b \in \mathcal{B}_1$. Similarly, we define $\tilde{\mathcal{B}}_2$. Then $\tilde{\mathcal{B}}_1 \cup \tilde{\mathcal{B}}_2$ is a basis for $R_1 \times R_2$. The discriminant of this basis is the product of the discriminants of \mathcal{B}_1 and \mathcal{B}_2 .
- **theorem 9.3.30 :** (page 1147) The quotient ring $\mathcal{O}_K/p\mathcal{O}_K$ though not a field is a \mathbb{F}_p vector space of dimension n over \mathbb{F}_p . It is the set product of the rings \mathcal{O}_K/P_i^e each of which in turn is a \mathbb{F}_p vector space.
- **theorem 9.3.31 :** (page 1147) Suppose that $\{b_1, \dots, b_n\}$ is a basis for K over \mathbb{Q} whose \mathbb{Z} -span is all of \mathcal{O}_K . Then, $\mathcal{B} = \{b_1 + p\mathcal{O}_K, \dots, b_n + p\mathcal{O}_K\}$ is a basis for $\mathcal{O}_K/p\mathcal{O}_K$ as a \mathbb{F}_p vector space.
- **theorem 9.3.32 :** (page 1148) The discriminant d of $\{b_1, \dots, b_n\}$ is $\equiv 0 \pmod{p}$ if and only if the discriminant of $\tilde{\mathcal{B}}$ is 0 in \mathbb{F}_p if and only if the part of $\tilde{\mathcal{B}}$ corresponding to \mathcal{O}_K/P_i^e for one of the i 's has a discriminant of 0 in \mathbb{F}_p .

- **theorem 9.3.33 :** (page 1148) Let d correspond to our basis $\{b_1, \dots, b_n\}$ whose \mathbb{Z} span is all of \mathcal{O}_K . Then, we have that $e = 1$ if and only if $p \nmid d$ and $e > 1$ if and only if $p \mid d$.
- **lemma 9.3.34 :** (page 1148) The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$.
- **lemma 9.3.35 :** (page 1149) Let m be a factor of $p-1$. Then there is a unique subgroup B of $A = \mathbb{Z}/(p-1)\mathbb{Z}$ such that $|A/B| = m$.
- **theorem 9.3.36 :** (page 1150) The discriminant of the basis $\{1, \zeta_p, \dots, \zeta_{p-2}\}$ of $\mathbb{Q}(\zeta_p)$ for $\mathbb{Q}(\zeta_p)$ over \mathbb{Q} if $p \neq 2$ is $(-1)^{\frac{p-1}{2}} p^{p-2}$
- **theorem 9.3.37 quadratic reciprocity:** (page 1151) Let p and q be two odd primes (i.e. not = 2). Then, q is a square mod p if and only if $(-1)^{\frac{p-1}{2}} p$ is a square mod q .
- **theorem 9.3.38 :** (page 1152)

$$(-1)^{\frac{p-1}{2}} = 1 \iff p \equiv 1 \pmod{4}$$

- **lemma 9.3.39 :** (page 1152) We can find gcd's in the Gaussian integers.
- **theorem 9.3.40 (fermat):** (page 1154) if $p \equiv 1 \pmod{4}$, then p is the sum of two squares.
- **method for writing p as a sum of two squares:** (page 1154) If $p \equiv 1 \pmod{4}$, we can do the following:
 - First factor $x^2 + 1$ mod p as $(x-r)(x+r)$.
 - Find the gcd $a+bi$ of $i+r$ and p in $\mathbb{Z}[i]$
 - We will have that $p = a^2 + b^2$.
- **comparison of proofs:** (page 1155) Notice that both in proving the sum of squares theorem and quadratic reciprocity there was a similar theme:
 - Relate our desired result to a factorization in a ring of integers.
 - Use a power basis for the ring of integers and have $p \nmid d$ so that we both know how to factor and that $e = 1$.
 - Go to finite fields when we mod out by our relevant prime and learn about the relevant Galois group by considering $x \mapsto x^{\text{prime}}$ which generates the Galois group to determine m .
 - Use the idea that $n = emk$ to find k and relate it to the factorization and make the statement we are interested in.
- **which fields in which proofs?:** (page 1156)
 - In the proof of quadratic reciprocity, we used the fields $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$.
 - In the proof of the sum of squares, we used $\mathbb{Q}(i)$.

- **norm of ideal:** (page 1162) Let the norm of an ideal A , denoted as $N(A)$ in \mathcal{O}_K be the index $[\mathcal{O}_K : A]$
- **norm of an element:** (page 1162) Let $N(w)$ denote the norm of the element w . This is given by the determinant of a matrix for the multiplication \mathbb{Q} -linear transformation $K \rightarrow K$ given by w —and equivalently this is given as the product of $\phi_i(w)$ where ϕ_i ranges through the ring homomorphisms $K \rightarrow \mathbb{C}$ which fix \mathbb{Q} .
- **theorem 9.3.41 :** (page 1163) Let $w \in \mathcal{O}_K$. Then:

$$N(w\mathcal{O}_K) = N(w)$$

- **theorem 9.3.42 :** (page 1163) Let P be the type of prime ideal of \mathcal{O}_K we mentioned above that we are considering. These are of the kind $p\mathcal{O}_K + (\alpha - r)\mathcal{O}_K$ where $p \nmid d$. Then, $N(P) = P$.
- **theorem 9.3.43 :** (page 1163) To check to see if we have a complete factorization of $(a\alpha + b)\mathcal{O}_K$ into prime ideals $p_i\mathcal{O}_K + (\alpha - r_i)\mathcal{O}_K$ of the kind we desire, we check to see if:

$$(-a)^d \cdot f\left(-\frac{b}{a}\right) = \underbrace{\prod}_{\text{product}} p_i$$

where d is the degree of $f(x)$.

- **general number field sieve:** (page 1164) This is the algorithm that steps through the above process to find two integers that represent the same square mod N . The gcd of the difference of these two integers with N hopefully reveals a factor of N .

Bibliography

- [1] Kevin Powell, *Discrete Perspectives in Mathematics: Mathematics without Limits*. Kindle Direct Publishing (2022)
- [2] Fan, Lianghuo (2003) A generalization of synthetic division and a general theorem of division of polynomials. Mathematical Medley, 30 (1)
- [3] John H. Hubbard / Barbara Burke Hubbard, *Vector Calculus, Linear Algebra, and Differential Forms: A Unified Approach*. Pearson, 2nd Edition, (2002)
- [4] Gerald B. Folland, *Real Analysis: Modern Techniques and Their Applications*, 2nd edition. John Wiley & Sons, Inc. Canada (1999)
- [5] Dunham Jackson The theory of Approximation, AMS Colloquium Publication Volume XI, New York (1930)
- [6] Thome, E. (2012). Square Root Algorithms for the Number Field Sieve. In: Ozbudak, F., Rodriguez-Henriquez, F. (eds) Arithmetic of Finite Fields. WAIFI 2012. Lecture Notes in Computer Science, vol 7369. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-31662-3_15
- [7] Harold Davenport *Multiplicative Number Theory*, 3rd Edition. Springer-Verlag New York, Inc. (2000)
- [8] Tom M. Apostol *Introduction to Analytic Number Theory* Springer-Verlag New York, Inc. (1976)
- [9] Henri Cohen *A Course in Computational Algebraic Number Theory* Springer-Verlag Berlin Heidelberg (1993)

- [10] Walter Rudin *Real and Complex Analysis*, 3rd Edition, McGraw-Hill, Inc. (1987)
- [11] Allen Hatcher, *Algebraic Topology* Cambridge University Press, New York (2001)

Index

- 0-cells, 414 \in “element of”, 39
1-cell, 414 \mathbb{C} , 38
2-cell, 415 \mathbb{N} , 38
 A^T , 461 $\mathbb{Q}(\alpha)$, 1078
 A^{-1} , 367 $\mathbb{Q}(\alpha, \beta)$, 1083
 $C[0, 1]$, 961 \mathbb{R} , 38
 $C^\omega[a, b]$, 1001 $\mathbb{R}[x]$ -module isomorphisms, 835
 C^n Functions, 1000 $\mathbb{R}[x]$ -span of a vector, 835
 D_8 , 808 \mathbb{R}^2 , 38
 H_L , 1088 \mathbb{R}^3 , 38
 K^H , 1089 \mathbb{Z} , 38
 L^2 norm, 964 \mathbb{Z} Row and Column Operations, 1037
 L^∞ -norm, 971 \mathbb{Z} -Rank of a \mathbb{Z} -module, 1033
 $P^n(R)$, 38 \mathbb{Z} -basis, 1036
 $R[x]$, 38 \mathbb{Z} -module, 1033
 $SO(n)$, 1018 \mathbb{Z} -module Homomorphism (Map), 1036
 S_A , 567 \mathbb{Z} -module Isomorphism, 1036
 V^* , 463 \mathbb{Z} -modules, 426
 \longmapsto , 43 $\mathbb{Z}/2\mathbb{Z}$, 431
 $\text{Hom}(D, C)$, 116 $\mathbb{Z}[\alpha]$, 1129
 $\text{Hom}_{\mathbb{R}}(V, \mathbb{R})$, 463 \otimes , 648
 f_x , 220 ∂ , 414
 f_y , 220 gcd: Greatest Common Factor, 844
 id_S , 69 \setminus , 41

\subset , 42	969
$\text{comp}_u(v)$, 465	Corollary 8.2.13 , 1019
$\text{comp}_v w$ Formula, 469	Corollary 8.2.5 , 1016
$\text{proj}_v w$ via Dot Product, 502	Corollary 9.1.10 , 1050
\times , 64	Corollary 9.1.11 , 1052
\emptyset , 42	Corollary 9.1.13 , 1059
\wedge , 663	Corollary 9.1.17 , 1061
dx , 662	Corollary 9.1.4 , 1039
f^* , 464	Corollary 9.2.15 , 1090
n -cycle, 568	Corollary 9.2.16 , 1090
n -form, 704	Corollary 9.2.19 , 1094
$v \bullet w$, 468	Corollary 9.2.21 , 1097
$v \perp w$, 470	Corollary 9.2.22 , 1097
v^* , 463	Corollary 9.2.7 , 1082
Corollary 2.2.4 Dimension of \mathbb{R}^n , 133	Corollary 9.3.17 , 1138
Corollary 2.2.5 Condition for Linear Independence by Counting, 133	Corollary 9.3.19 , 1139
Corollary 4.1.3 Isomorphisms Preserve Dimension, 277	Corollary 9.3.20 , 1139
Corollary 6.2.10 , 606	Corollary 9.3.24 , 1142
Corollary 6.2.3 Squares come from Diagonals, 584	Corollary 9.3.27 , 1143
Corollary 6.2.5 Determinant of Transpose, 587	Corollary 9.3.29 , 1145
Corollary 6.2.6 Column or Row Airdrops, 587	Lemma 5.3.11 , 532
Corollary 6.2.9 , 605	Lemma 5.3.12 , 532
Corollary 6.3.3 , 625	Lemma 7.4.16 , 885
Corollary 6.3.4 , 626	Lemma 7.4.17 , 885
Corollary 6.3.5 , 628	Lemma 7.5.4 , 914
Corollary 7.2.5 , 787	Lemma 8.2.11 , 1018
Corollary 7.2.7 Parallelograms in Three Dimensions, 789	Lemma 8.2.12 , 1019
Corollary 7.2.8 Parallelograms in n Dimensions, 791	Lemma 8.2.17 , 1024
Corollary 7.3.18 , 856	Lemma 9.1.7 , 1045
Corollary 7.3.8 , 839	Lemma 9.2.6 , 1081
Corollary 7.4.6 , 880	Lemma 9.3.35 , 1148
Corollary 7.4.9 , 881	Lemma 9.3.36 , 1149
Corollary 7.5.13 , 927	Lemma 9.3.40 , 1152
Corollary 7.5.6 , 915	Theorem 1.2.2 Fiber Partitions, 52
Corollary 7.5.8 , 916	Theorem 1.3.2 Surjectivity by Right Inverse, 70
Corollary 7.6.3 Parseval's Identity, 964	Theorem 1.3.3 Injectivity by Left Inverse, 72
Corollary 7.6.6 Parseval's Identity Infinite Version,	Theorem 1.3.4 Uniqueness of Inverses for Bijective Maps, 73
	Theorem 1.4.2 Cartesian Products of Additive Groups, 84

Theorem 1.4.3 Additive Functions Preserve Group Properties, 87	368
Theorem 1.4.4 Additive Group Fibers, 88	Theorem 4.5.2 , 411
Theorem 1.4.5 Zero Fiber Check for Injectivity, 89	Theorem 4.5.3 , 411
Theorem 2.1.2 Subspace Criteria, 108	Theorem 4.5.4 , 418
Theorem 2.1.3 Vector Span Description, 110	Theorem 5.1.2 Transposes and Inverses, 463
Theorem 2.2.2 Linear independence: Definition Equivalence, 130	Theorem 5.1.3 Symmetric Products, 465
Theorem 2.2.3 Basis Definition Equivalence, 132	Theorem 5.1.4 Projection Length is a Linear Transformation, 466
Theorem 2.2.6 Subspace Dimension, 135	Theorem 5.1.5 , 467
Theorem 2.2.7 Finitely Generated Vector Spaces have Bases, 136	Theorem 5.1.6 Orthogonality Condition, 470
Theorem 2.3.2 Linear Transformations Preserve Structure, 148	Theorem 5.1.7 Orthogonality by Bases, 470
Theorem 2.3.3 Linear Transformations and Linear Combinations, 149	Theorem 5.1.8 , 474
Theorem 2.3.4 Row and Column Interpretations Give Same Product, 161	Theorem 5.2.2 Domain Direct Sum, 489
Theorem 2.4.2 , 183	Theorem 5.2.3 Vector Decomposition, 492
Theorem 3.4.2 , 259	Theorem 5.3.10 , 526
Theorem 4.1.2 Isomorphisms Relabel Bases, 277	Theorem 5.3.13 , 532
Theorem 4.1.4 Range and Kernel are Vector Spaces, 278	Theorem 5.3.14 , 533
Theorem 4.1.5 Isomorphisms preserve the dimensions of the kernel and the range, 279	Theorem 5.3.2 Kernel Orthogonal to Row Space, 516
Theorem 4.1.6 Isomorphisms in Row and Column Interpretation, 284	Theorem 5.3.3 Orthogonal Right Inverse, 518
Theorem 4.1.7 Uniqueness and Existence of Smith Normal Form, 288	Theorem 5.3.4 Gram-Schmidt Iteration by Right Inverse, 519
Theorem 4.1.8 Duality of Injectivity and Surjectivity, 291	Theorem 5.3.5 Matrices for $g_n \circ f_n$, 521
Theorem 4.1.9 , 297	Theorem 5.3.6 Gram-Schmidt Matrix Iteration, 521
Theorem 4.2.2 Basis for the Range and Reduced Row Echelon Form, 327	Theorem 5.3.7 Gram-Schmidt Dot Product Iteration, 524
Theorem 4.2.3 Reduced Row Echelon Form is Unique, 327	Theorem 5.3.8 , 525
Theorem 4.3.2 , 360	Theorem 5.3.9 , 526
Theorem 4.3.3 A Unique Inverse, 367	Theorem 6.1.2 Decomposing Cycles into Transpositions, 572
Theorem 4.3.4 Taking Inverses Reverses Order, 367	Theorem 6.1.3 Constant Parity, 574
Theorem 4.3.5 Smith Normal Form of Isomorphism,	Theorem 6.1.4 Method for Determining if a Permutation is Odd or Even, 575
	Theorem 6.1.5 Number of Permutations, 576
	Theorem 6.2.11 , 607
	Theorem 6.2.12 , 609
	Theorem 6.2.2 Airdrop to Diagonal, 584
	Theorem 6.2.4 Permutations of Rows or Columns, 587
	Theorem 6.2.7 Determinants of Triangular Matrices, 588

Theorem 6.2.8 ,	604	Theorem 7.3.13 ,	842
Theorem 6.3.2 ,	625	Theorem 7.3.14 ,	843
Theorem 6.4.2 Product/Boxing Rule for Derivatives,		Theorem 7.3.15 ,	847
	655	Theorem 7.3.16 ,	848
Theorem 6.4.3 Multivariable Taylor Series (centered		Theorem 7.3.17 ,	856
at $(0, 0)$),	658	Theorem 7.3.19 ,	857
Theorem 6.4.4 ,	661	Theorem 7.3.2 ,	828
Theorem 6.4.5 ,	664	Theorem 7.3.3 ,	830
Theorem 6.4.6 ,	667	Theorem 7.3.4 ,	830
Theorem 6.5.2 ,	696	Theorem 7.3.5 ,	830
Theorem 6.5.3 Anticommutativity of The Cross Prod-		Theorem 7.3.6 ,	831
uct,	697	Theorem 7.3.7 ,	838
Theorem 6.5.4 ,	698	Theorem 7.3.9 ,	839
Theorem 6.5.5 Bilinear Properties of the Cross Prod-		Theorem 7.4.10 ,	882
uct,	698	Theorem 7.4.11 ,	882
Theorem 6.5.6 Zero Cross Product,	698	Theorem 7.4.12 ,	882
Theorem 6.5.7 ,	698	Theorem 7.4.13 ,	883
Theorem 6.5.8 ,	711	Theorem 7.4.14 ,	883
Theorem 7.1.2 ,	745	Theorem 7.4.15 ,	884
Theorem 7.1.3 ,	748	Theorem 7.4.18 ,	885
Theorem 7.1.4 ,	755	Theorem 7.4.2 ,	878
Theorem 7.1.5 ,	759	Theorem 7.4.3 ,	878
Theorem 7.2.10 ,	796	Theorem 7.4.4 ,	879
Theorem 7.2.11 ,	799	Theorem 7.4.5 ,	880
Theorem 7.2.12 ,	800	Theorem 7.4.7 ,	881
Theorem 7.2.13 ,	802	Theorem 7.4.8 ,	881
Theorem 7.2.14 ,	806	Theorem 7.5.10 ,	925
Theorem 7.2.15 ,	810	Theorem 7.5.11 ,	926
Theorem 7.2.16 ,	812	Theorem 7.5.12 ,	927
Theorem 7.2.17 ,	813	Theorem 7.5.14 ,	937
Theorem 7.2.18 Cycle Types and Conjugacy,	817	Theorem 7.5.15 ,	938
Theorem 7.2.2 ,	782	Theorem 7.5.2 ,	911
Theorem 7.2.3 ,	783	Theorem 7.5.3 ,	913
Theorem 7.2.4 ,	784	Theorem 7.5.5 ,	914
Theorem 7.2.6 Cauchy-Binet Formula (Special Case),		Theorem 7.5.7 ,	915
	789	Theorem 7.5.9 ,	924
Theorem 7.2.9 ,	795	Theorem 7.6.2 ,	961
Theorem 7.3.10 ,	839	Theorem 7.6.4 ,	967
Theorem 7.3.11 ,	841	Theorem 7.6.5 Fourier Series,	968
Theorem 7.3.12 ,	842	Theorem 7.6.7 Pointwise Convergence,	971

- Theorem 7.6.8** Uniform Convergence, 972
Theorem 8.1.2 , 1001
Theorem 8.2.10 , 1018
Theorem 8.2.14 , 1019
Theorem 8.2.15 , 1021
Theorem 8.2.16 Euler's Theorem, 1024
Theorem 8.2.2 , 1015
Theorem 8.2.3 , 1015
Theorem 8.2.4 , 1016
Theorem 8.2.6 , 1016
Theorem 8.2.7 , 1017
Theorem 8.2.8 , 1017
Theorem 8.2.9 , 1017
Theorem 9.1.12 Classification of Finitely Generated \mathbb{Z} -modules, 1058
Theorem 9.1.14 , 1060
Theorem 9.1.15 , 1060
Theorem 9.1.16 , 1061
Theorem 9.1.18 , 1061
Theorem 9.1.19 , 1062
Theorem 9.1.20 , 1062
Theorem 9.1.21 , 1062
Theorem 9.1.2 , 1037
Theorem 9.1.3 , 1037
Theorem 9.1.5 , 1044
Theorem 9.1.6 , 1044
Theorem 9.1.8 Chinese Remainder Theorem (\mathbb{Z} -module version), 1045
Theorem 9.1.9 Chinese Remainder Theorem (Ring Version), 1048
Theorem 9.2.10 , 1085
Theorem 9.2.11 , 1086
Theorem 9.2.12 , 1087
Theorem 9.2.13 , 1087
Theorem 9.2.14 Fundamental Theorem of Galois Theory, 1088
Theorem 9.2.17 , 1090
Theorem 9.2.18 , 1091
Theorem 9.2.20 , 1096
Theorem 9.2.23 , 1107
Theorem 9.2.24 , 1108
Theorem 9.2.2 , 1079
Theorem 9.2.3 , 1079
Theorem 9.2.4 , 1080
Theorem 9.2.5 , 1080
Theorem 9.2.8 , 1082
Theorem 9.2.9 Primitive Element Theorem, 1084
Theorem 9.3.10 , 1129
Theorem 9.3.11 , 1130
Theorem 9.3.12 , 1131
Theorem 9.3.13 , 1135
Theorem 9.3.14 , 1136
Theorem 9.3.15 , 1137
Theorem 9.3.16 , 1138
Theorem 9.3.18 , 1139
Theorem 9.3.21 , 1139
Theorem 9.3.22 , 1140
Theorem 9.3.23 , 1141
Theorem 9.3.25 , 1143
Theorem 9.3.26 , 1143
Theorem 9.3.28 , 1143
Theorem 9.3.2 , 1121
Theorem 9.3.30 , 1146
Theorem 9.3.31 , 1147
Theorem 9.3.32 , 1147
Theorem 9.3.33 , 1148
Theorem 9.3.34 , 1148
Theorem 9.3.37 , 1150
Theorem 9.3.38 Quadratic Reciprocity, 1151
Theorem 9.3.39 , 1152
Theorem 9.3.3 , 1122
Theorem 9.3.41 (Fermat), 1154
Theorem 9.3.42 , 1163
Theorem 9.3.43 , 1163
Theorem 9.3.44 , 1163
Theorem 9.3.4 , 1123
Theorem 9.3.5 , 1124
Theorem 9.3.6 , 1126
Theorem 9.3.7 , 1127
Theorem 9.3.8 , 1128

Theorem 9.3.9 , 1128

- Adding a Set and an Element, 81
- Additive Function, 85
- Additive Group, 82
- Additive Identity, 106
- Additive Questions via Matrices, 254
- Adjacency Matrix, 254
- Adjacency Matrix Powers, 255
- Adjugate Matrix, 621
- airdropping, 280
- Airdropping with Cofactor Strategy, 602
- Algebraic Field Extension, 1083
- Algebraic Integers \mathcal{O}_K , 1081
- Algebraic Number, 1080
- An m -form that evaluates like a $(m - 1)$ -form, 717
- An Infinite Orthonormal Set, 965
- Angled Projections in \mathbb{R}^2 , 499
- Area of a Parallelogram, 700
- Area of a Parallelogram in \mathbb{R}^4 , 700
- associativity, 82
- augmented matrix, 332
- Automorphism, 1088
- axiom of choice, 77
- Bar Notation for Quotients, 1041
- base case, 26
- Basis Definition 1, 113
- Basis Definition 2, 132
- Bijective, 52
- Bilinear Matrix Entries, 650
- Bilinear Transformation, 640
- Bilinear Transformations as Matrices, 641
- Block Diagonal Matrix, 183
- Boundary of an Edge, 414
- Bounded Variation, 970
- boxing rule, 553
- Cantor set, 968
- cartesian product arbitrary, 66
- Cartesian Product between Finitely Many Sets, 65
- Cartesian Product between Two Sets, 65
- Cauchy Riemann Equations, 677
- Cauchy sequence, 967
- Cauchy's Theorem Special Case, 1093
- Cell Complex, 415
- Central (or Principal) Submatrix, 598
- central submatrix, 778
- Chain Rule is Matrix Multiplication, 226
- Changing the Basis of a Bilinear form, 1120
- Characteristic Polynomial, 748
- Characteristic Polynomial of a 2×2 matrix, 782
- Checking if a Vector is in Subspace, 297
- Chinese Remainder Theorem for Ideals, 1144
- Choosing Eigenvectors, 891
- Chunking Principle, 53
- Class of Functions, 966
- codomain, 43
- Coefficient Sign Changes, 925
- Cofactor, 593
- Cofactor Expansion, 597
- Cofactor Function, 596
- Column Interpretation Convention, 462
- Column Interpretation of Matrix Input, 151
- Column Operations Matrix, 294
- Column Space, 151
- Column-Row Partition Multiplication, 176
- commutative, 105
- Commutative Diagrams, 67
- Comparison Between Orthogonal Methods, 504
- Comparison of Proofs, 1156
- complete, 967
- Complex Conjugate, 914
- complex linear, 677
- Complex Vector Space, 958
- Composition of Two Functions, 66
- Computing Multiplicative Inverses, 1063
- Conjugacy between Permutations, 816
- Conjugate Condition for Being Real Number, 914
- Conjugate Group Elements, 809
- Conjugate Linear, 959
- Conjugate Quaternion, 1014

- Conjugating by Unit Quaternions, 1019
Connected Component, 474
Connected Components, 410
Connected Components Strategy, 412
consistent, 28
Constants in Polynomials as Scalar Matrices, 747
Containment and Factorization, 1134
contradiction, 25
Converging to a Class of Functions, 966
Coordinates in Other Bases, 376
Coset Equations, Systems of Congruences, 1051
Cosets, 595, 1038
Cosets, Addition, and Scalar Multiplication, 1040
counterexample, 24
Counting Number of Paths, 757
Counting Spanning Trees, 806
covectors, 663
Cramer's Rule, 624
Cross Product, 695
Cross Product by Wedge Product, 697
Cycle Notation, 568
Cycle-Type, 817
Cyclotomic Polynomial, 1106
Defining Functions, 44
Definition matching, 23
Degree of Vertex, 473
Dependent System, 336
Derivative, 222
Derivative of a Function $\mathbb{R}^2 \rightarrow \mathbb{R}$, 219
Descartes' Rule of Signs, 926
Determinant by Cofactors:, 595
Determinant Matrix for 2×2 , 642
Determinant of a Matrix, 587
Determining Injectivity and Surjectivity from Smith Normal form, 291
Diagonal Change of Basis, 876
Diagonal Cofactors, 594
Diagonal Matrix, 583
Different Bases from Input to Output, 386
Different Complexes Yet the Same Homology, 432
Differential Equation Diagonalization, 1006
digraph, 252
Dihedral Group of order 8, 808
Dimension, 113
direct sum, 489
Directed Graph, 252
Discriminant of a Basis, 1120
Discriminant of a Basis of a Vector Space *That is Also a Ring.*, 1146
Disjoint cycle notation, 568
disjoint union, 42
Distance, 962
domain, 43
Dot Product, 468
Dual Space, 662
dual vector, 463
dual vectors, 663
Dual Vectors are Transposed Vectors, 463
duality, 291
Dualizing a vector, 666
Edge Boundary Matrix, 418
Eigenbasis, 917
Eigenspace, 842, 874
Eigenspaces are Invariant, 842, 874
Eigenvalue, 843, 874
Eigenvector, 843, 874
Eigenvectors for Diagonlization, 884
Element Chasing, 67
Elementary Column Operation, 282
Elementary Matrix, 603
Elementary Row Operation, 282
Equality in a \diamond sense, 968
Euclidean Algorithm, 830
Euler's Characteristic Formula, 442
Euler-phi Function, 1062
Evaluate a Trilinear Transformation Using Matrix Levels, 646
Even Permutation, 575
Examples of Three Basic Isomorphisms, 280
Extending a Transformation, 383

- Face Boundary Matrix, 417
- Face Orientations, 416
- faces, 414
- Factoring in \mathcal{O}_K , 1135
- Fast Matrix Squaring, 163
- Fiber, 47
 - fiber box diagram, 47
- Fiber Description of Range, 50
- Field, 105, 1077
- Field Extension, 1077
- Finding an Orthogonal Complement, 472
- Finding Approximate Surface Area, 708
- Finding the Minimal Polynomial—Method 1, 849
- Finding the Minimal Polynomial—Method 2, 852
- Finding the Rotation of an Ellipse Centered at Origin, 922
- Finite Fields \mathbb{F}_p , 106
- finitely generated, 136
- Finiteness Convention, 1078
- First 2-Sylow Theorem, 1094
- fixed point, 571
- Fixed Point of a Permutation, 568
- fixed points, 812
- Four Defining Properties of Determinants, 639
- Fourier Series and Closeness, 965
- Free \mathbb{Z} -module (finitely generated), 1033
- Free Rank, 136
- free variables, 336
- Full Rank, 367
- Function Definition Notation, 44
- Functions: Alternate Notation, 67
- Fundamental Parallelogram, 1034
- Fundamental Theorem of Algebra, 913, 1083
- Galois Group, 1088
- Gaussian Integers, 1122
- General Number Field Sieve, 1081, 1164
- Generalized Stoke's Theorem, 719
- Generators, 1034
- Gluing Diagram, 419
- graph, 217
- Greatest Common Factor, 829
- Hermitian Adjoint, 959
- Hermitian Inner Product, 959
- Hermitian Inner Products from Matrices, 960
- Hermitian Matrix, 959
- Hermitian Norm of a Vector, 960
- Homogeneous Linear Differential Equation, 1002
- Homology Groups, 432
- How to Change Coordinates in an n -form, 709
- How to Find Reduced Echelon Form, 328
- How to Find the Remainder without Dividing, 760
- How to Make a Unit Vector, 468
- Ideals, 1134
- Idempotent matrix, 856
- Identifying Multilinear Parts, 659
- identity, 82
- Identity Function, 69
- Identity Matrix, 285
- if and only if, 28
- image, 43
- Imaginary Part, 1013
- Imaginary Quaternion, 1014
- Important Note about Cofactors, 594
- In and Out Principles, 1057
- Incidence, 257
- Inconsistent System, 340
- Independent System, 339
- Index $[A : B]$, 1130
- induction hypothesis, 26
- Injective, 50
- Injective Matrix Function, 364
- Inner Product, 957
- Inner product on $C[0, 1]$, 961
- Inner Product Projection onto a Subspace, 964
- Inner Products from Matrices, 958
- Integral of a n -form over a n -dimensional region, 704
- Integral of a Constant n -form, 704
- Interpretation of Stochastic Multiplication, 260

- Invariant Subspace, 840
inverse, 82
Inverse by Cofactors, 622
Inverse of a 2×2 Matrix, 623
Inverse of a Function, 73
Invertible integers, 1036
irreducible polynomial, 848
Isometry, 1017
isomorphism, 430
Isomorphism of Vector Spaces, 277
Jacobian Matrix, 711
Kernel of a Linear Transformation, 278
Kernels are Orthogonal, 471
Kernels for Diagonalization, 892
Kitty-corner, 593
Klein Bottle, 424
Labeling Finite Dimensional Vector Spaces as \mathbb{R}^n , 378
Laplacian Matrix, 473
Least Common Multiple, 846
Least Squares, 549
Lebesgue Integral, 968
Lebesgue Measure 0 Set, 968
left cosets, 595
Left Function Inverse, 72
Left Stochastic Matrix, 259
Leibniz Formula for π , 973
Length of a Vector, 467
Length of Vector Formula, 469
Linear Combination, 112
Linear Operator, 1001
Linear Transformation, 148
Linearly Dependent, 130
Linearly Independent Definition 1, 129
Linearly Independent Definition 2, 129
Linearly Independent Definition 3, 129
Lines and Planes are Fibers, 217
Lines and Planes are Graphs of Shifts, 218
logical opposites, 25
logically equivalent, 28
Lower triangular matrices, 588
Lower triangular matrix, 534
LQ Decomposition, 534
LU Decomposition, 343
machine learning, 226
magnitude, 467
mapping, 43
mapping diagram, 43
Matching Column-Row Partition, 176
Matrices as Maps and Dual Maps, 464
Matrix Action Principle, 746
Matrix Block Multiplication, 179
Matrix for Orthogonal Projection proj_v , 503
Matrix Formation Principle, 205
Matrix Function Multiplication/Composition (Column Interpretation), 157
Matrix Function Multiplication/Composition (Row Interpretation), 159
Matrix in Skewed Coordinates, 379
Matrix in Standard Coordinates, 380
Matrix Labeling Notation, 152
matrix multiplication, 150
Matrix Partitioning Principle for Multiplication, 179
Maximal Ideal, 1136
Method for determining if a collection is linearly independent or dependent, 132
Method For Writing p as a Sum of Two Squares, 1154
Minimal Polynomial, 828, 1079
Minimal Polynomial of Element and Matrix, 1080
Minimal Polynomial on a Subspace, 836
Minimal Polynomial versus Characteristic polynomial, 848
Minimal Spanning Set, 113
Modules, 118
Monic Polynomial, 1079
Multilinear Function, 638
Multiplication for a Ring, 1048
Multiplicative Group, 83
Multiplicative group map, 810
Multiplicative Groups R^\times , 1060

- Multiplicative Inverse, 1077
 Multiplicative Inverses Notation, 1063
 Multiplying an Element to a Set, 81
 Multivariable Polynomial, 659
- Negative Definite, 923
 neural network, 226
 Nilpotent Matrix, 855
 Non-disjoint cycle notation, 568
 Non-uniqueness of Right Inverses, 364
 Nonhomogeneous Linear Differential Equation, 1003
 Nonorientable Surface, 424
 Nonsingular Square Matrix, 625
 Norm From an Inner Product, 958
 Norm in an Algebraic Field Extension, 1098
 Norm of an Element, 1163
 Norm of Ideal, 1162
 Normal Closure, 1087
 Normal Field Extension, 1086
 Normal Subgroup, 1091
 null space, 278
 Nullity of a Matrix, 288
- Odd Permutation, 575
 Oriented Incidence Matrix, 258
 Oriented Surface, 416
 Orthogonal Basis, 525
 Orthogonal Complement, 471
 Orthogonal Matrix, 1016
 orthogonal projection, 501
 Orthogonal Projection Length, 467
 orthogonal right inverse, 518
 Orthogonal Subspaces, 470
 Orthogonal Vectors, 470
 Orthogonality, 962
 Orthogonally Diagonalizable, 916
 Orthogonally Diagonalize a Symmetric Matrix, 917
 Orthonormal Basis, 525
- Pairwise Orthogonal, 518
 Parity, 573
 Parseval's Identity, 964
- Partial Derivatives, 222
 partition, 42
 Partitions by Cosets, 595
 Path Counting Question, 252
 Permutation, 566
 Permutation Groups as Matrices, 811
 Permuted Diagonal Product, 585
 Pivot, 326
 planar graph, 442
 Pointwise Convergence, 969
 Polynomial Span and Minimal Polynomial, 838
 Positive Definite, 923
 Positive Semi-definite Matrix, 925
 Possible Subspaces of \mathbb{R}^3 , 109
 Practical Interpretation of Bilinear part of a Multivariable Polynomial, 662
 Precise Definition of Smooth Function—Optional, 222
 preimage, 46
 Prime Gaussian Integer, 1123
 Prime Ideal, 1137
 Primitive Element, 1083
 Primitive Root of Unity, 1105
 principal submatrix, 597
 product rule, 553
 Projection onto a subspace, 963
 Proof by Induction, 26
 Properties of \wedge , 667
 Properties of the Dot product, 469
 Proving Equality of Sets, 29
 Proving Logical Equivalence, 28
 Proving that a set is or is not a basis, 134
 Proving the Equivalence of the Characteristic and Minimal Polynomials, 854
 Pseudo Inverse, 937
 Pseudo Inverse Properties, 934
- QR Decomposition, 530
 Quaternion, 1012
 Quaternion Ring, 1012
 quotient \mathbb{Z} -module, 430
 Quotient Module, 1039

- Quotient Vector Space, 115
- range, 43
- Range of a Linear Transformation, 278
- Ranges for Diagonalizing, 888
- Rank of a Matrix, 288
- Real Analytic Functions on an interval, 1000
- Real Hilbert Space, 967
- Real Part, 1014
- rearranging, 280
- Recursion to Matrix Powers via Columns, 245
- Recursion to Matrix Powers via Rows, 245
- recursive formula, 243
- Reduced Row Echelon Form, 327
- reducible, 848
- Relabeling Transformations, 385
- rescaling, 280
- Right Function Inverse, 70
- Right Inverse of a Linear Transformation, 360
- Right Stochastic Matrix, 259
- Ring, 117, 1077
- Ring Homomorphism, 1048
- Rotation, 1016
- Rotation Matrices are Orthogonal, 919
- Row Interpretation of Matrix Input, 155
- Row Operations Matrix, 294
- Row Space, 155, 516
- Row-Column Partition (non-matching), 179
- Scalable Function, 148
- Scalar Action on Eigenvectors, 874
- Scalar Matrix, 743
- scalars, 105
- Scalars to Make 1, 1054
- Second Derivative, 225
- Set Addition, 81
- Set builder notation, 40
- set image, 45
- Shadow Vector Function, 493
- Similarity, 783
- Simple Algebraic Field Extension, 1078
- Simpler at Every Step, 1058
- Simpler Representative Principle, 1057
- Singular Square Matrix, 625
- Singular Value Decomposition, 936
- Size of a Set Notation, 1061
- skewed, 375
- slide to a diagonal, 589
- Smith Normal Form (over a field), 287
- Smith Normal Form over $\mathbb{R}[x]$, 833
- Smooth Function, 221
- Solution to $f' = rf$, 1006
- Solving a System of Congruences, 1052
- Some Basic Examples of Linear Transformations, 205
- Span, 110
- Spanning Tree, 800
- Square Matrix, 163
- Stacking Principle, 643
- standard basis, 149
- Standard Basis Vectors, 149
- Standard Definition of Matrix Multiplication, 185
- Standard Hermitian Inner Product, 960
- Subfield, 1077
- Submodule, 1033
- subset, 42
- Subspace, 108
- Surjective, 51
- Surjective Matrix Function, 359
- Symmetric Group, 576
- Symmetric Groups, 811
- Symmetric Matrix, 464
- Symmetric Multilinear Form, 656
- Symmetry of a Square, 807
- synthetic division for any polynomial division, 755
- Systems of Congruences, 1050
- tensor product, 648
- The Equation of a Transformed Graph, 208
- The Inverse of an Orthogonal Matrix, 916
- The Pretending Matrix, 377
- The Sign of a Permutation, 813
- The size of Conjugacy Classes, 1093

The Unpretending Matrix, [376](#)

Topology, [426](#)

Total Degree, [659](#)

Trace, [778](#)

Trace Bilinear Form, [1119](#)

Trace in an Algebraic Field Extension, [1098](#)

Trace of a permutation matrix, [812](#)

Transpose of a Matrix, [461](#)

Transposes Reverse the Order of Multiplication, [462](#)

Transpositions, [572](#)

triangular matrix, [588](#)

trilinear transformation, [642](#)

Uniform Convergence, [971](#)

Unit in a Ring, [1123](#)

Unit Quaternion, [1017](#)

Unit Vector, [468](#)

Unitary Matrix, [961](#)

Unmodding, [1134](#)

Upper triangular matrix, [529](#)

upper triangular matrix, [588](#)

Using the Pretending Matrix, [382](#)

Variable Initialization Rule, [40](#)

Variations to Finding Scalars, [1056](#)

Vector Space, [106](#)

Vector Space of Faces, [415](#)

Vector Space of Functions, [116](#)

Vertex Touching Question, [257](#)

Wedge Product, [663](#)

Which Fields in Which Proofs?, [1156](#)

Zero Divisor, [1138](#)

Zero Divisor Matrix, [856](#)