Elementary Linear Algebra

Alex Nelson*

October 26, 2022

Contents

*This is a page from `https://pqnelson.github.io/notebk/`
Compiled: November 8, 2022 at 9:04am (PST)

Preface

These are notes about elementary linear algebra, roughly at the level of Math 22A at UC Davis. Our presentation is heavily inspired from Dr Andrew Waldron's 2007 Spring course. Later Dr Waldron and colleagues wrote their own textbook [1].

We try to keep discussion informal and conversational, we will delimit examples and definitions and theorems and whatnot. Towards this end, we will use "paragraph numbers" with some kind of label summarizing the paragraph chunk or mathematical register ["Theorem", "Definition", "Example", etc.]. Propositions are statements which are either true or false, and usually have a proof following their statement. Proofs end with the symbol "□" called the Halmos tombstone, we read them as "QED" [Latin *quod erat demonstrandum*, "that which was to be proven"]. These are all variations on a proposition:

Lemma refers to a "helper proposition" used to prove a tricky step in a later proposition, modern programmers might call lemmas "private propositions";

Theorem refers to an important proposition;

Corollary refers to a proposition which is an immediate consequence of a previous proposition;

Example is a proposition asserting an object is an instance of a gadget, or satisfies some property.

On the other hand, there are some registers which are not propositions:

Definition introduces a new property, a new gadget, or a new object [or function];

Remark clarifies or comments a certain aspect of a proposition or definition;

Problem statements which drive the conversation by explicitly providing motivation;

Puzzle statements which motivate future sections.

Examples and exercises are randomly generated using Lisp scripts, or from various cited sources. The reader is encouraged to work their way through the excercises found in, say, Kolman and Hill [2].

We rely on structured derivations to explain derivations involving chains of equations. It's explained a little in appendix A, but for the most part it looks like

$$\begin{array}{ll} & A \\ = & (\text{hint why } A = B) \\ & B \\ = & (\text{hint why } B = C) \\ & C \\ = & (\text{hint why } C = D) \\ & D \end{array}$$

From which we can conclude $A = B = C = D$ are all equal to each other. Usually we are trying to prove $A = D$.

Occasionally we may have discussions of difficult or subtle points. We reserve them in "dangerous bend" paragraphs, which begin with

The font is smaller for such discussions, and make be skipped on first reading.

Lastly, I have haphazardly added exercises and problems throughout. "Problems" are scattered wherever I think they might be fun or useful. "Exercises" are consolidated in their own subsection. NOTE: some of the exercises are redundant — in the sense that, some exercise in [say] §5 will ask you to prove something which was proven in [say] §3. This was originally accidental, but I realized this is useful to "spaced repetition" to reinforce your understanding of various proofs and concepts.

Part I
Problem Statement

1 Solving Systems of Equations

1·1. Example (Euler [4, Ch.IV §4 question 3 ¶612]). A mule and donkey carry a large load. The donkey complained of his load and said to the mule, "I need only 100 pounds of your load to make mine twice as heavy as yours would be." To which the mule answered, "But if you gave me 100 pounds of your load, I'd be carrying three times you would carry." How much did they carry?

Let d be the donkey's load, m be the mule's load. The donkey's statement could be presented in the equation,

$$d + 100 = 2(m - 100), \tag{1·1.1a}$$

whereas the mule's response,

$$m + 100 = 3(d - 100). \tag{1·1.1b}$$

From the first of these equations, we find

$$d = 2m - 300. \tag{1·1.2}$$

We plug this into the second equation to find

$$\begin{aligned} m + 100 &= 3(2m - 400) \\ &= 6m - 1200. \end{aligned} \tag{1·1.3}$$

Hence the mule carries,

$$m = \frac{1300}{5} = 260 \text{ pounds}, \tag{1·1.4a}$$

and this means the donkey carries,

$$d = 520 - 300 = 220 \text{ pounds}. \tag{1·1.4b}$$

1·2. Example (Sraffa [3]). One class of systems of linear equations occurs naturally in Neo-Ricardian economics. Consider a hypothetical economy consisting of two industry sectors, wheat and iron, whose production processes are described by the system of equations (where the left of the arrow refers to the inputs at the start of the production period, and the quantities to the right of the arrows are produced at the end of the period, and then an annual market takes place where iron is traded for wheat):

$$\begin{array}{rcl} \text{inputs} & \to & \text{outputs} \\ 280\text{ qr. wheat} + 12\text{ t. iron} & \to & 400\text{ qr. wheat} \\ 120\text{ qr. wheat} + 8\text{ t. iron} & \to & 20\text{ t. iron.} \end{array} \tag{1·2.1}$$

The question we want to know: what is the exchange rate between quarters[1] of wheat and tons of iron? We can create a system of equations by introducing two unknowns p_w for the price of 1 quarter of wheat, and p_i for the price of 1 ton of iron. We assume society is in a "self reproducing state", in the sense that the wheat sector exchanges enough wheat-for-iron to continue producing wheat (and the iron sector exchanges enough iron-for-wheat to continue producing iron):

$$\begin{array}{rcl} 280p_w + 12p_i & = & 400p_w \\ 120p_w + 8p_i & = & 20p_i. \end{array} \tag{1·2.2a}$$

[1] A "quarter" of wheat refers to an obscure measurement choice of 13th century England, because it can be found in the *Magna Carta*. By the 18th century, the measurement of 1 quarter of wheat in Britain varied port to port. It was finally standardized in 1824 to be 8 bushels (or 64 gallons).

We can rewrite the first equation (by subtracting both sides by $280p_w$):

$$\begin{aligned} 12p_i &= 120p_w \\ 120p_w + 8p_i &= 20p_i. \end{aligned} \tag{1·2.2b}$$

Then we rewrite the second equation (by subtracting both sides by $8p_i$):

$$\begin{aligned} 12p_i &= 120p_w \\ 120p_w &= 12p_i. \end{aligned} \tag{1·2.2c}$$

These are redundant equations! We end up with a class of solutions, described by

$$\boxed{10p_w = p_i,} \tag{1·2.2d}$$

that is to say, the price of 1 ton iron is equal to the price of 10 quarters of wheat.

1·2.1. *Remark.* This method of solving such equations in Neo-Ricardian economics works fine when there is no surplus; that is to say, when there is exactly as much produced (for each commodity) used as inputs in the economy. However, when there is surplus, we need more sophisticated techniques of linear algebra, because we will have an eigenvalue problem.

1·2.2. *Remark.* As of 28 October 2022, it appears the going rate is 1.18925 quarters of wheat exchanges for 1 ton of iron.

1·3. Example (Motivating Example)**.** Suppose we have two equations with two variables x and y given by:

$$-x - 2y = -2 \tag{1·3.1a}$$

$$5x + 6y = 1. \tag{1·3.1b}$$

Are there [real] values for x and y which makes this hold? We can add 5 times the first equation to the second equation, giving us:

$$-x - 2y = -2 \tag{1·3.2a}$$

$$0 - 4y = -9. \tag{1·3.2b}$$

The second equation may be solved for $y = 9/4$, then we may substitute this into the first equation giving us

$$-x - 2(9/4) = -2 \implies -x = 2(9/4) - 2 = \frac{9}{2} - \frac{4}{2} = \frac{5}{2}. \tag{1·3.3}$$

Hence we obtain the solutions

$$\boxed{x = \frac{5}{2}} \quad \text{and} \quad \boxed{y = \frac{9}{4}.} \tag{1·3.4}$$

1·4. Index Notation. We will rely heavily on index notation. Why? Well, there are 26 possible symbols (using lowercase Latin letters), which means we could not discuss anything beyond systems of 5 equations in 5 variables; if we also use the 26 uppercase Latin letters, then we cannot discuss anything beyond systems of 7 equations in 7 unknowns. Rather than struggle with new symbols, we will use indices: appending numbers as subscripts to letters to refer to distinct quantities. Thus we write x_1, x_2, x_3 instead of x, y, z.

We may use **"Dummy Variables"** to affix a variable as a subscript, writing x_i where i could be 1, 2, or 3. Here i is the dummy variable in the expression x_i. We often will write "x_i where $i = 1, 2, 3$" to indicate i is a dummy variable ranging over the values 1, 2, 3.

We can have several indices [plural of "index"] affixed to a symbol. We have seen this with coefficients, which had two indices separated by a comma. Some authors use a comma to separate indices, other authors do not.

Also we should note, some authors use superscripts indices. This will occur in some parts of mathematics, but we will avoid it in these notes whenever possible (because it's hard to tell if a superscript number is an exponent or an index).

1·5. Basic Terminology. A **"linear equation in one variable"** x looks like

$$b = ax \tag{1·5.1}$$

where a and b are real constants.

A single **"linear equation in two variables"** x and y looks like

$$ax + by = c \tag{1·5.2}$$

where a, b, and c are real constants.

A single linear equation in n variables $x_1, \ldots, x_n$ looks like

$$a_1x_1 + \cdots + a_nx_n = b \tag{1·5.3}$$

where $a_1, \ldots, a_n$, and b are real constants.

1·6. Terminology: Systems of equations. More generally, a **"System of m Linear Equations in n Unknowns"** $x_1, \ldots, x_n$ (where the subscripts are **"Indices"** to append to one symbol x a number or "dummy variable" [a variable ranging over the index values], giving us any number of variables for the price of one symbol) looks like:

$$\begin{array}{rcl} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n & = & b_2 \\ \vdots \qquad \vdots \qquad \ddots \qquad \vdots & \vdots & \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n & = & b_m \end{array} \tag{1·6.1}$$

where $b_1, \ldots, b_m$ are m real constants, and we have $a_{1,1}, a_{1,2}, \ldots, a_{m,n}$ be mn real constants called the **"Coefficients"**.

A **"Solution"** to a system of equations in n variables $x_1, \ldots, x_n$ is an assignment of n real values $s_1, \ldots, s_n$ to the variables (so $x_1 = s_1, \ldots, x_n = s_n$) which satisfies the system of equations.

1·7. Example (System of Nonlinear Equations)**.** We have to distinguish a system of linear equations from nonlinear equations. For example, the following is a nonlinear equation

$$3x^2 + x = 2, \tag{1·7.1}$$

because a polynomial of order $n > 1$ will be nonlinear. If you have a function $f(x)$ and you don't know if it's linear or not, check if $f(ax + by) = af(x) + bf(y)$ holds or not — this is the criteria of linearity.

The following equation is also nonlinear:

$$x + yz = 3. \tag{1·7.2}$$

We cannot multiply two [or more] unknowns together in a linear equation.

So the following equation is nonlinear:

$$x + y\cos(z) = 3, \tag{1·7.3}$$

on two counts: first, $\cos(z)$ is nonlinear; and second, $y\cos(z)$ is not allowed in a linear equation.

1·8. Method of Elimination. One method to find a solution, which has been taught to high school students for decades, is to take the first equation and use it to rewrite one variable in terms of the remaining. For example, in:

$$\begin{array}{rcrcrcr} 0 & + & 2x_2 & + & 3x_3 & = & 5 \\ 2x_1 & + & 0 & + & 3x_3 & = & -1 \\ x_1 & + & x_2 & + & x_3 & = & 1. \end{array} \tag{1·8.1}$$

We would use the first equation to substitute $x_2 = (5 - 3x_3)/2$ in the remaining equations, and discard the first equation, giving us:

$$\begin{array}{rcccccc} 2x_1 & + & 0 & + & 3x_3 & = & -1 \\ x_1 & + & \left(\dfrac{5-3x_3}{2}\right) & + & x_3 & = & 1. \end{array} \tag{1·8.2}$$

We do this again, to use the first equation to write $x_1 = (-1 - 3x_3)/2$, and plug this into the last equation, which gives us a value for x_3. We backsubstitute this into the second equation to obtain a value for x_1, then together these are backsubstituted into either the first or third equation of our original system to find the solution for x_2.

1·9. Issues with Method of Elimination. Doing this "method of elimination" is tedious. *I* [the author] does not want to do this, it's too much work. Is there a better way to find a solution to a system of linear equations?

A second issue with the method of elimination, it does not tell us when a solution exists. Or if there is a family of solutions, which we saw in Example 1·2 (the price of 1 ton of iron was 10 times the price of a quarter of wheat, whatever that is).

1·10. Roadmap: Enter the Matrix. Remember what a system of 1 linear equation in 1 variable looks like? We saw it was $ax = b$. We could solve this easily when $a \neq 0$, simply take $x = b/a$ or $x = a^{-1}b$. It would be lovely if all systems of linear equations could be so easy.

We will try to make it easy by generalizing the notion of a "number". Instead of writing a system of equations as

$$\begin{array}{rcl} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n & = & b_2 \\ \vdots \qquad \vdots \qquad \ddots \qquad \vdots & \vdots & \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n & = & b_m \end{array} \tag{1·10.1}$$

we will introduce a notion of a matrix $\mathbf{A}$ as an array of m rows and n columns, and vectors $\boldsymbol{x}$, $\boldsymbol{b}$, then rewrite our system as

$$\mathbf{A}\boldsymbol{x} = \boldsymbol{b}. \tag{1·10.2}$$

Just as with our simpler system with one equation in one unknown $ax = b$ where we multiplied both sides by the number a^{-1} (assuming a is invertible), we can imitate this and try "multiplying" both sides by a matrix $\mathbf{B}$ to transform our system to something like

$$\boldsymbol{x} = \mathbf{B}\boldsymbol{b}. \tag{1·10.3}$$

The problem: we will have to define a notion of matrix multiplication, and prove it satisfies the familiar properties which the multiplication of numbers enjoy.

Exercises

▸ **Exercise 1.1** (Sraffa [3, §2]). Find the exchange-values which ensure a self-reproducing state for the following economy:

$$\begin{array}{rcl} 240\text{ qr. wheat} + 12\text{ t. iron} + 18\text{ pigs} & \to & 450\text{ qr. wheat} \\ 90\text{ qr. wheat} + 6\text{ t. iron} + 12\text{ pigs} & \to & 21\text{ t. iron} \\ 120\text{ qr. wheat} + 3\text{ t. iron} + 30\text{ pigs} & \to & 60\text{ pigs.} \end{array} \tag{1·10.4}$$

Part II
Matrices

2 Matrix Zoo

We need to introduce the terminology first, before introducing notions of matrix addition (or matrix multiplication).

2·1. Definition. Let m, n be positive integers. We define an m-by-n **"Matrix"** A to be a rectangular array of mn real [or complex] numbers arranged in m horizontal **"Rows"** and n vertical **"Columns"**, written:

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mj} & \dots & a_{mn} \end{pmatrix} \leftarrow i^{\text{th}} \text{ row} \tag{2·1.1}$$

We have highlighted the i^{th} row, and the j^{th} column.

If further $m = n$ (so we have an n-by-n matrix), then we call it a **"Square Matrix"**. In this case, we can refer to the **"Main Diagonal"** as the components $a_{1,1}$, $a_{2,2}$, $\dots$, $a_{n,n}$.

2·1.1. *Remark.* We abbreviate "m-by-n matrix" as "$m \times n$ matrix". The pair of numbers (m, n) is called the **"Dimensions"** of the matrix.

Also note, some people use parentheses in writing matrices, other people use square brackets. Both are acceptable.

2·2. Matrix and Components. If we want to refer to a generic component of an m-by-n matrix $\mathbf{A}$, we write $\mathbf{A} = (a_{ij})$ to indicate we will use a_{ij} to refer to the component found in the i^{th} row and j^{th} column.

Also, very important, if we have some m-by-n matrix $\mathbf{A} = (a_{i,j})$ and we wanted to refer to its component in row r, column c, we may refer to that component by writing $(\mathbf{A})_{r,c}$. This is, of course, the same as $a_{r,c}$, but it will be useful [much later] to take a matrix and refer to certain components without introducing $(a_{i,j})$ first.

2·3. Example: Zero Matrix. For any positive integers m, n, we have the $m \times n$ **"Zero Matrix"** to be the matrix whose components are all zero. We denote this by $\mathbf{0}$ or 0 because it will play the analogous counterpart that $0 \in \mathbb{R}$ plays.

2·4. Example: Identity Matrix. For any positive integer n, we have the $n \times n$ **"Identity Matrix"** to be

$$\mathbf{I}_n = (\delta_{i,j}) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j \end{cases} \tag{2·4.1}$$

where the components $\delta_{i,j}$ are referred to as the **"Kronecker Delta"**. If n is clear from context, we may suppress the subscript and write $\mathbf{I}$ instead of $\mathbf{I}_n$. Some authors write $\mathbf{1}$ for the identity matrix, because (as we will see) it is analogous to the number $1 \in \mathbb{R}$.

2·5. Definition. A **"Column Vector"** refers to an $n \times 1$ matrix.

A **"Row Vector"** refers to a $1 \times m$ matrix.

A **"Vector"** may refer to either row vectors or column vectors; in these notes, we will reserve the word "vector" specifically for "column vector".

In vector calculus, we were quite cavalier about our notion of vectors. There a vector consisted of a BASE POINT and an "arrow" of some magnitude pointing in some direction from the base point. We could freely move the base point around willy-nilly. In linear algebra, we will be working with vectors, but they all share *the same* base point.

2·6. Definition. A square matrix $\mathbf{A} = (a_{i,j})$ for which $a_{i,j} = 0$ when $i \neq j$ is called a **"Diagonal Matrix"**. We may write $\mathbf{A} = \operatorname{diag}(a_{1,1}, a_{2,2}, \dots, a_{n,n})$ to indicate $\mathbf{A}$ is a diagonal matrix.

If further $a_{i,i} = c$ for all i, then we call $\mathbf{A}$ a **"Scalar Matrix"**.

2·6.1. *Remark* ("Scalars"). The word "scalar" means "number". We motivated our diversion into matrices by trying to create some gadget which resembles numbers. Scalar matrices are the "most number-like" among matrices.

2·7. Examples.

1. The following is a diagonal matrix which is not a scalar matrix
$$\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}. \tag{2·7.1a}$$
2. The following is not a diagonal matrix,
$$\mathbf{J} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{2·7.1b}$$
3. The following is a scalar matrix,
$$\mathbf{B} = \begin{pmatrix} -\pi & 0 \\ 0 & -\pi \end{pmatrix}. \tag{2·7.1c}$$
4. The identity matrix $\mathbf{I}_n$ is a scalar matrix.
5. The $n \times n$ zero matrix is a scalar matrix.

2·8. Definition. Let $\mathbf{A} = [a_{i,j}]$ and $\mathbf{B} = [b_{i,j}]$ be two $m \times n$ matrices. We say $\mathbf{A}$ and $\mathbf{B}$ are **"Equal"** if they have identical components in identical positions, i.e., if for each $i = 1, \dots, m$ and $j = 1, \dots, n$ we have $a_{i,j} = b_{i,j}$. We indicate the matrices are equal by writing $\mathbf{A} = \mathbf{B}$.

If $\mathbf{A}$ and $\mathbf{B}$ are not equal, then we write $\mathbf{A} \neq \mathbf{B}$.

2·8.1. *Remark.* We are technically introducing a new binary relation, **"Matrix Equality"**.

2·8.2. *Remark* (Same dimensions). If $\mathbf{A}$ and $\mathbf{B}$ do not have the same number of rows and columns, then they cannot possibly be equal. In this case (if they have different dimensions), we can still sensibly write $\mathbf{A} \neq \mathbf{B}$.

2·9. Definition. We call an $m \times n$ matrix $\mathbf{A} = (a_{i,j})$:

1. **"Upper Triangular"** if $a_{i,j} = 0$ for $i > j$, e.g., when $m = n$ it looks like:
$$\mathbf{A} = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \dots & a_{1,n} \\ 0 & a_{2,2} & a_{2,3} & \dots & a_{2,n} \\ 0 & 0 & a_{3,3} & \dots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_{n,n} \end{bmatrix}$$
2. **"Lower Triangular"** if $a_{i,j} = 0$ for $i < j$, e.g., when $m = n$ it looks like:
$$\mathbf{A} = \begin{bmatrix} a_{1,1} & 0 & 0 & \dots & 0 \\ a_{2,1} & a_{2,2} & 0 & \dots & 0 \\ a_{3,1} & a_{3,2} & a_{3,3} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \dots & a_{n,n} \end{bmatrix}$$

3. If $\mathbf{A}$ is upper-triangular and the diagonal entries are all zero, then we call $\mathbf{A}$ **"Strictly Upper Triangular"**.
4. Similarly, if $\mathbf{A}$ is lower-triangular and the diagonal entries are all zero, then we call $\mathbf{A}$ **"Strictly Lower Triangular"**.

2·10. Block matrix. It is useful to draw horizontal and vertical lines (either dashed or slid, it makes no difference except for typography), to partition a matrix into blocks, permitting us to write

$$\mathbf{A} = \left[\begin{array}{c:c} \mathbf{B} & \mathbf{C} \\ \hdashline \mathbf{D} & \mathbf{E} \end{array}\right] = \left[\begin{array}{c|c} \mathbf{B} & \mathbf{C} \\ \hline \mathbf{D} & \mathbf{E} \end{array}\right]. \tag{2·10.1}$$

We could partition a matrix however we want, and we call the blocks **"Submatrices"** of $\mathbf{A}$. Writing $\mathbf{A}$ in this manner is called a **"Block Decomposition"** of $\mathbf{A}$.

2·11. Example. Let us consider some 3×5 matrix $\mathbf{A}$ whose components are partitioned into block form:

$$\mathbf{A} = \left[\begin{array}{cc:ccc} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ \hdashline a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \end{array}\right] = \left[\begin{array}{c:c} \mathbf{B} & \mathbf{C} \\ \hdashline \mathbf{D} & \mathbf{E} \end{array}\right] \tag{2·11.1}$$

This partitions $\mathbf{A}$ into a 2×2 matrix $\mathbf{B}$, a 2×3 matrix $\mathbf{C}$, a 1×2 matrix $\mathbf{D}$, and a 1×3 matrix $\mathbf{E}$. We could also partition it in other ways, for example,

$$\mathbf{A} = \left[\begin{array}{c:ccc:c} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ \hdashline a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \end{array}\right]. \tag{2·11.2}$$

▸ **Exercise 2.1.** Can we have a (row or column) vector which is also a scalar matrix?

3 Matrix Algebra

3·1. Now, we want to define binary operators on matrices. But we don't want these definitions to be arbitrary. We want:
1. Matrix multiplication produce a system of linear equations,
2. Matrix addition of vectors recovers the familiar operation in vector calculus.

3·2. Definition. Let $\mathbf{A} = (a_{i,j})$ and $\mathbf{B} = (b_{i,j})$ be two $m \times n$ matrices. We define **"Matrix Addition"** of $\mathbf{A}$ and $\mathbf{B}$ to produce a third $m \times n$ matrix $\mathbf{C} = (c_{i,j})$ (called the *sum* of $\mathbf{A}$ and $\mathbf{B}$) whose components are defined by $c_{i,j} = a_{i,j} + b_{i,j}$.

We write $\mathbf{A} + \mathbf{B}$ for the sum of $\mathbf{A}$ and $\mathbf{B}$.

3·2.1. *Remark.* We should prove, for any $m \times n$ matrices $\mathbf{A}$ and $\mathbf{B}$, their sum exists and is unique. This is "obvious enough".

3·3. Example. Let

$$\mathbf{A} = \begin{bmatrix} -4 & -4 & 5 \\ 3 & -1 & 4 \end{bmatrix} \tag{3·3.1a}$$

and

$$\mathbf{B} = \begin{bmatrix} -3 & 1 & 2 \\ 6 & -3 & -5 \end{bmatrix}. \tag{3·3.1b}$$

Then

$$\mathbf{A} + \mathbf{B} = \begin{bmatrix} -4-3 & -4+1 & 5+2 \\ 3+6 & -1-3 & 4-5 \end{bmatrix} = \begin{bmatrix} -7 & -3 & 7 \\ 9 & -4 & -1 \end{bmatrix}. \tag{3·3.1c}$$

3·4. Proposition (Commutativity of Matrix Addition)**.** *For any two $m\times n$ matrices $\mathbf{A}=(a_{i,j})$ and $\mathbf{B}=(b_{i,j})$, we have $\mathbf{A}+\mathbf{B}=\mathbf{B}+\mathbf{A}$.*

Proof. We see $\mathbf{A}+\mathbf{B}=(a_{i,j}+b_{i,j})$ and for each component we have $a_{i,j}+b_{i,j}=b_{i,j}+a_{i,j}$ since componentwise we have addition of numbers (which is commutative). But the matrix with $(b_{i,j}+a_{i,j})=\mathbf{B}+\mathbf{A}$. Hence we find $\mathbf{A}+\mathbf{B}=\mathbf{B}+\mathbf{A}$. □

3·5. Proposition. *For any $m\times n$ matrix $\mathbf{A}=(a_{i,j})$, the sum of $\mathbf{A}$ with the $m\times n$ zero matrix 0 is $\mathbf{A}$.*

Proof. We see that the components of the zero matrix are all identically zero, $\mathbf{0}=[(0)_{i,j}]$. So

$\mathbf{A}+\mathbf{0}$

= (by definition of matrix addition)

(3·5.1a) $[a_{i,j}+(0)_{i,j}]$

= (since $(0)_{i,j}=0$ for all i, j)

(3·5.1b) $[a_{i,j}+0]$

= (arithmetic)

(3·5.1c) $[a_{i,j}]$

= (definition of $\mathbf{A}$)

(3·5.1d) $\mathbf{A}$.

Thus $\mathbf{A}+\mathbf{0}=\mathbf{A}$. □

3·6. Definition. Let $\mathbf{A}=(a_{i,j})$ be an $m\times n$ matrix, let r be a real [or complex] number. We define the **"Scalar Multiple"** of $\mathbf{A}$ by r to be the $m\times n$ matrix $r\mathbf{A}=(ra_{i,j})$ whose components are obtained by multiplying every component of $\mathbf{A}$ by r. We can also write this as $r\cdot\mathbf{A}=r\mathbf{A}$ to make the scalar multiplication explicit.

3·6.1. *Remark.* "Scalar multiplication" refers to the fact we are multiplying a matrix by a "scalar" [number], as opposed to multiplying by a vector or another matrix.

3·7. Example. Let r be a positive integer, let $\mathbf{A}$ be any matrix. Then

$$\underbrace{\mathbf{A}+\cdots+\mathbf{A}}_{r\text{ times}}=rA. \tag{3·7.1}$$

We can see this by induction on r.

Base case: $r=1$ means $\mathbf{A}=1\cdot\mathbf{A}$ which is trivially true.

Inductive Hypothesis: we now assume for any positive integer r that $\mathbf{A}+\cdots+\mathbf{A}=r\mathbf{A}$.

Inductive Case: we now prove that $r+1$ case. We want to prove

$$\underbrace{\mathbf{A}+\cdots+\mathbf{A}}_{r+1\text{ times}}=(r+1)\mathbf{A}. \tag{3·7.2}$$

We can use the inductive hypothesis to write:

$$\underbrace{\mathbf{A}+\cdots+\mathbf{A}}_{r\text{ times}}+\mathbf{A}=r\mathbf{A}+\mathbf{A}. \tag{3·7.3}$$

Then we observe $r\mathbf{A}+\mathbf{A}=(ra_{i,j})+(a_{i,j})=((r+1)a_{i,j})$ using the definition of matrix addition. Then by definition of scalar multiplication this is precisely $(r+1)\mathbf{A}$.

3·7.1. *Remark.* We have a sort of consistency result between scalar multiplication and adding a matrix to itself finitely many times. That's a good sign.

3·8. Example. Let $r = -2$ and

$$\mathbf{A} = \begin{bmatrix} -2 & 6 \\ 6 & -5 \end{bmatrix}. \tag{3·8.1a}$$

Then

$$r\mathbf{A} = \begin{bmatrix} -2\cdot(-2) & -2\cdot 6 \\ -2\cdot 6 & -2\cdot(-5) \end{bmatrix} = \begin{bmatrix} 4 & -12 \\ -12 & 10 \end{bmatrix}. \tag{3·8.1b}$$

3·9. Example. If $\mathbf{A} = (a_{i,j})$ is a scalar $n \times n$ matrix $\mathbf{A} = \operatorname{diag}(a, a, \dots, a)$, then $\mathbf{A} = a\mathbf{I}_n$.

3·10. Properties of the Scalar Product. Let r, s be numbers and $\mathbf{A}$, $\mathbf{B}$ be appropriately sized matrices. Then the following hold:

1. $r(s\mathbf{A}) = (rs)\mathbf{A}$
2. $(r+s)\mathbf{A} = r\mathbf{A} + s\mathbf{A}$ (distributivity)
3. $r(\mathbf{A}+\mathbf{B}) = r\mathbf{A} + r\mathbf{B}$

3·11. Definition. Let $\mathbf{A} = (a_{i,j})$, $\mathbf{B} = (b_{i,j})$ be two $m \times n$ matrices. We define their **"Difference"** to be the matrix $\mathbf{A} - \mathbf{B} = \mathbf{A} + -1\cdot\mathbf{B}$. Similarly, the **"Negation"** of $\mathbf{A}$ is the matrix $-\mathbf{A} = -1\cdot\mathbf{A}$.

3·12. Proposition. *For any matrix $\mathbf{A}$, we have $\mathbf{A} - \mathbf{A} = \mathbf{0}$.*

Exercises

▸ **Exercise 3.1.** Prove the sum of two diagonal matrices is another diagonal matrix. Is this true for scalar matrices (the sum of two scalar matrices is a scalar matrix)?

3.1 Matrix Transpose

3·13. Definition. Let $\mathbf{A} = (a_{i,j})$ be an $m \times n$ matrix. We define the **"Transpose"** of $\mathbf{A}$ to be the $n \times m$ matrix $\mathbf{A}^{\mathsf{T}} = (a^{\mathsf{T}}_{j,i})$ where $a^{\mathsf{T}}_{j,i} = a_{i,j}$.

3·14. Example. If we have

$$\mathbf{A} = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & a_{m,3} & \cdots & a_{m,n} \end{bmatrix}, \tag{3·14.1a}$$

(highlighting the first row to see where it goes, along with several select entries), then we find

$$\mathbf{A}^{\mathsf{T}} = \begin{bmatrix} a_{1,1} & a_{2,1} & a_{3,1} & \cdots & a_{m,1} \\ a_{1,2} & a_{2,2} & a_{3,2} & \cdots & a_{m,2} \\ a_{1,3} & a_{2,3} & a_{3,3} & \cdots & a_{m,3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{1,n} & a_{2,n} & a_{3,n} & \cdots & a_{m,n} \end{bmatrix}. \tag{3·14.1b}$$

3·15. Proposition (Transpose is idempotent)**.** *For any matrix $\mathbf{A}$, we have $(\mathbf{A}^{\mathsf{T}})^{\mathsf{T}} = \mathbf{A}$.*

Proof. Let $\mathbf{B} = \mathbf{A}^{\mathsf{T}}$ Then $(\mathbf{B}^{\mathsf{T}})_{i,j} = (\mathbf{B})_{j,i}$ by definition of the transpose, and $(\mathbf{B})_{j,i} = (\mathbf{A}^{\mathsf{T}})_{j,i} = (\mathbf{A})_{i,j}$. Hence $\big((\mathbf{A}^{\mathsf{T}})^{\mathsf{T}}\big)_{i,j} = (\mathbf{A})_{i,j}$, as desired. □

3·16. Definition. Let $\mathbf{A}$ be an $n \times n$ matrix. We call $\mathbf{A}$ **"Symmetric"** if it is equal to its transpose: $\mathbf{A} = \mathbf{A}^{\mathsf{T}}$. Similarly, we call $\mathbf{A}$ **"Antisymmetric"** if it is the negation of its transpose $\mathbf{A} = -\mathbf{A}^{\mathsf{T}}$.

3·17. Example. Let $\mathbf{A}$ be an anti-symmetric 3×3 matrix. Then it must look like

$$\mathbf{A} = \begin{pmatrix} 0 & a_{1,2} & a_{2,3} \\ -a_{1,2} & 0 & -a_{3,1} \\ a_{3,1} & -a_{2,3}0 & \end{pmatrix}. \tag{3·17.1}$$

In particular, the diagonal of an antisymmetric matrix consists of zero entries.

Exercises

- **Exercise 3.2.** If $\mathbf{U}$ is an upper triangular matrix, then is $\mathbf{U}^{\mathsf{T}}$ upper triangular or lower triangular?
- **Exercise 3.3.** If $\mathbf{L}$ is an lower triangular matrix, then is $\mathbf{L}^{\mathsf{T}}$ upper triangular or lower triangular?
- **Exercise 3.4.** Prove or find a counter-example: if $\mathbf{M}$ is an arbitrary $n\times n$ matrix, then $\mathbf{A} = (\mathbf{M}-\mathbf{M}^{\mathsf{T}})/2$ is an antisymmetric matrix and $\mathbf{S} = (\mathbf{M}+\mathbf{M}^{\mathsf{T}})/2$ is a symmetric matrix.
- **Exercise 3.5.** Let $\mathbf{M}$ be an arbitrary $n\times n$ matrix. Prove or find a counter-example: there exists a unique symmetric matrix $\mathbf{S}=\mathbf{S}^{\mathsf{T}}$ and a unique antisymmetric matrix $\mathbf{A} = -\mathbf{A}^{\mathsf{T}}$ such that $\mathbf{M} = \mathbf{S}+\mathbf{A}$.
- **Exercise 3.6.** If $\mathbf{S}$ is a symmetric $n\times n$ matrix, is $\mathbf{S}\mathbf{S}^{\mathsf{T}}$ symmetric? What about $\mathbf{S}+\mathbf{S}^{\mathsf{T}}$?

3.2 Dot Product and Matrix Multiplication

3·18. Definition. Recall, if we have two n-vectors $\boldsymbol{a} = (a_1,\dots,a_n)$ and $\boldsymbol{b} = (b_1,\dots,b_n)$, we define their **"Dot Product"** to be the scalar [number]

$$\boldsymbol{a}\cdot\boldsymbol{b} = a_1b_1 + a_2b_2 + \dots + a_nb_n = \sum_{j=1}^{n} a_jb_j. \tag{3·18.1}$$

3·19. Example. Let

$$\boldsymbol{a} = \begin{bmatrix} -1 \\ 4 \\ -5 \end{bmatrix}, \quad\text{and}\quad \boldsymbol{b} = \begin{bmatrix} -6 \\ 2 \\ 4 \end{bmatrix}. \tag{3·19.1}$$

Then

$$\begin{aligned} \boldsymbol{a}\cdot\boldsymbol{b} &= (-1)\cdot(-6) + 4\cdot 2 + (-5)\cdot 4 \\ &= 6 + 8 - 20 = -6. \end{aligned} \tag{3·19.2}$$

3·20. Proposition. *The dot product is symmetric,* $\boldsymbol{a}\cdot\boldsymbol{b} = \boldsymbol{b}\cdot\boldsymbol{a}$.

3·21. Definition. Let $\mathbf{A} = (a_{i,j})$ be an $m\times p$ matrix, let $\mathbf{B} = (b_{j,k})$ be an $p\times n$ matrix. We define the **"Matrix Multiplication"** of $\mathbf{A}$ and $\mathbf{B}$ to be an $m\times n$ matrix $\mathbf{C} = (c_{i,k})$ whose components are defined by the equation

$$c_{i,k} = \sum_{j=1}^{p} a_{i,j}b_{j,k}. \tag{3·21.1}$$

That is to say, it is formed by taking the dot product of the i^{th} row of $\mathbf{A}$ with the j^{th} column of $\mathbf{B}$,

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,p} \\ a_{2,1} & a_{2,2} & \dots & a_{2,p} \\ \vdots & \vdots & & \vdots \\ a_{i,1} & a_{i,2} & \dots & a_{i,p} \\ \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,p} \end{bmatrix} \begin{bmatrix} b_{1,1} & b_{1,2} & \dots & b_{1,j} & \dots & b_{1,n} \\ b_{2,1} & b_{2,2} & \dots & b_{2,j} & \dots & b_{2,n} \\ \vdots & \vdots & & \vdots & & \vdots \\ b_{p,1} & b_{p,2} & \dots & b_{p,j} & \dots & b_{p,n} \end{bmatrix} = \begin{bmatrix} c_{1,1} & c_{1,2} & \dots & c_{1,j} & \dots & c_{1,n} \\ c_{2,1} & c_{2,2} & \dots & c_{2,j} & \dots & c_{2,n} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{i,1} & c_{i,2} & \dots & c_{i,j} & \dots & c_{i,n} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{m,1} & c_{m,2} & \dots & c_{m,j} & \dots & c_{m,n} \end{bmatrix}$$

We denote the matrix multiplication of $\mathbf{A}$ and $\mathbf{B}$ by $\mathbf{AB}$.

3·22. Example. Let us consider an example just to show the "mechanics" of matrix multiplication. Let

$$\mathbf{A} = \begin{bmatrix} 3 & 1 & 6 \\ 2 & 1 & 3 \end{bmatrix} \tag{3·22.1a}$$

and

$$\mathbf{B} = \begin{bmatrix} 2 & 1 & 7 \\ 6 & 1 & 0 \\ 1 & -1 & 5 \end{bmatrix}. \tag{3·22.1b}$$

Then we find the component in the first column, first row, of the product is:

$$\begin{aligned} \mathbf{AB} &= \begin{bmatrix} 3 & 1 & 6 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 2 & 1 & 7 \\ 6 & 1 & 0 \\ 1 & -1 & 5 \end{bmatrix} = \begin{bmatrix} 3\cdot 2 + 1\cdot 6 + 6\cdot 1 & ? & ? \\ ? & ? & ? \end{bmatrix} \\ &= \begin{bmatrix} 18 & ? & ? \\ ? & ? & ? \end{bmatrix} \end{aligned} \tag{3·22.1c}$$

The next entry in the first row is:

$$\begin{aligned} \mathbf{AB} &= \begin{bmatrix} 3 & 1 & 6 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 2 & 1 & 7 \\ 6 & 1 & 0 \\ 1 & -1 & 5 \end{bmatrix} = \begin{bmatrix} 18 & 3\cdot 1 + 1\cdot 1 + 6\cdot -1 & ? \\ ? & ? & ? \end{bmatrix} \\ &= \begin{bmatrix} 18 & -2 & ? \\ ? & ? & ? \end{bmatrix} \end{aligned} \tag{3·22.1d}$$

The last entry on the first row:

$$\begin{aligned} \mathbf{AB} &= \begin{bmatrix} 3 & 1 & 6 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 2 & 1 & 7 \\ 6 & 1 & 0 \\ 1 & -1 & 5 \end{bmatrix} = \begin{bmatrix} 18 & -2 & 3\cdot 7 + 1\cdot 0 + 6\cdot 5 \\ ? & ? & ? \end{bmatrix} \\ &= \begin{bmatrix} 18 & -2 & 51 \\ ? & ? & ? \end{bmatrix} \end{aligned} \tag{3·22.1e}$$

We can continue to the second row:

$$\begin{aligned} \mathbf{AB} &= \begin{bmatrix} 3 & 1 & 6 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 2 & 1 & 7 \\ 6 & 1 & 0 \\ 1 & -1 & 5 \end{bmatrix} = \begin{bmatrix} 18 & -2 & 51 \\ 2\cdot 2 + 1\cdot 6 + 3\cdot 1 & ? & ? \end{bmatrix} \\ &= \begin{bmatrix} 18 & -2 & 51 \\ 13 & ? & ? \end{bmatrix} \end{aligned} \tag{3·22.1f}$$

The next column in the second row:

$$\begin{aligned} \mathbf{AB} &= \begin{bmatrix} 3 & 1 & 6 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 2 & 1 & 7 \\ 6 & 1 & 0 \\ 1 & -1 & 5 \end{bmatrix} = \begin{bmatrix} 18 & -2 & 51 \\ 13 & 2\cdot 1 + 1\cdot 1 + 3\cdot -1 & ? \end{bmatrix} \\ &= \begin{bmatrix} 18 & -2 & 51 \\ 13 & 0 & ? \end{bmatrix} \end{aligned} \tag{3·22.1g}$$

Finally, the remaining entry:

$$\begin{aligned} \mathbf{AB} &= \begin{bmatrix} 3 & 1 & 6 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 2 & 1 & 7 \\ 6 & 1 & 0 \\ 1 & -1 & 5 \end{bmatrix} = \begin{bmatrix} 18 & -2 & 51 \\ 13 & 0 & 2\cdot 7 + 1\cdot 0 + 3\cdot 5 \end{bmatrix} \\ &= \begin{bmatrix} 18 & -2 & 51 \\ 13 & 0 & 29 \end{bmatrix} \end{aligned} \tag{3·22.1h}$$

3·23. Recovering System of Linear Equations. This is pretty random, why on Earth should we accept it? Well, the biggest reason is because we recover a system of linear equations by multiplying an $m \times n$ matrix by an $n \times 1$ column vector. If we write our $m \times n$ matrix $\mathbf{A}$ as m row vectors

$$\mathbf{A} = \begin{bmatrix} \boldsymbol{a}_1^{\mathsf{T}} \\ \boldsymbol{a}_2^{\mathsf{T}} \\ \vdots \\ \boldsymbol{a}_m^{\mathsf{T}} \end{bmatrix}$$

then we see that multiplying it by our column vector $\boldsymbol{x}$ produces

$$\mathbf{A}\boldsymbol{x} = \begin{bmatrix} \boldsymbol{a}_1 \cdot \boldsymbol{x} \\ \boldsymbol{a}_2 \cdot \boldsymbol{x} \\ \vdots \\ \boldsymbol{a}_m \cdot \boldsymbol{x} \end{bmatrix}. \tag{3·23.1}$$

If we have an m-vector of constants $\boldsymbol{b}$, and $\boldsymbol{x}$ were a vector of unknowns, then

$$\mathbf{A}\boldsymbol{x} = \boldsymbol{b} \tag{3·23.2}$$

is precisely a system of m linear equations in n unknowns. This is wonderful: it's what we were trying to do all along!

3·24. Example. Let $\mathbf{A} = (a_{j,k})$ be an $m \times n$ matrix, consider the matrix multiplication of the $m \times m$ identity matrix $\mathbf{I}_m$ with $\mathbf{A}$. We find

$(\mathbf{I}_m \mathbf{A})_{i,k}$

= (definition of matrix multiplication)

(3·24.1) $\displaystyle\sum_{j=1}^{m} \delta_{i,j} a_{j,k}$

= (breaking up the sum)

(3·24.2) $\displaystyle\left(\sum_{j=1}^{i-1} \delta_{i,j} a_{j,k}\right) + \delta_{i,i} a_{i,k} + \left(\sum_{j=i+1}^{m} \delta_{i,j} a_{j,k}\right)$

= (since $\delta_{i,j} = 0$ if $i \neq j$)

(3·24.3) $0 + \delta_{i,i} a_{i,k} + 0$

= (since $\delta_{i,i} = 1$)

(3·24.4) $a_{i,k}$

= (folding back $\mathbf{A}$ into the result)

(3·24.5) $(\mathbf{A})_{i,k}$.

Hence $\mathbf{I}_m \mathbf{A} = \mathbf{A}$.

3·25. Example. Let

$$\mathbf{A} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \tag{3·25.1a}$$

and $\mathbf{I}_2$ be the 2-by-2 identity matrix. Then

$$\mathbf{A}\mathbf{I}_2 = \mathbf{A}. \tag{3·25.1b}$$

3·26. Example. Let $\mathbf{A}$ be a $1 \times n$ matrix (i.e., a row n-vector) and $\mathbf{B}$ be a $n \times 1$ matrix (i.e., a column n vector). Let us write $\mathbf{A} = (a_1, \dots, a_n)$ and $\mathbf{B} = (b_1, \dots, b_n)^{\mathsf{T}}$. Then

$$\mathbf{AB} = \sum_{j=1}^{n} a_j b_j = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n. \tag{3·26.1}$$

Does this look familiar? It's the dot product of two vectors $\boldsymbol{a}$, $\boldsymbol{b}$. We specifically have, if $\boldsymbol{a}$ and $\boldsymbol{b}$ are both column n-vectors, then

$$\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{a}^{\mathsf{T}} \boldsymbol{b}. \tag{3·26.2}$$

This relates matrix multiplication to the transpose and dot product.

3·27. Rephrasing the definition. If we have an $m \times n$ matrix $\mathbf{A}$ and an $n \times 2$ matrix $\mathbf{B}$, we could view $\mathbf{B}$ as a pair of column n-vectors

$$\mathbf{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2). \tag{3·27.1}$$

In this case, we see that matrix multiplication amounts to,

$$\mathbf{AB} = (\mathbf{A}\boldsymbol{b}_1, \mathbf{A}\boldsymbol{b}_2). \tag{3·27.2}$$

We can continue in this manner, for an arbitrary $n \times p$ matrix $\mathbf{C}$ thinking of it as p column n-vectors $\mathbf{C} = (\boldsymbol{c}_1, \dots, \boldsymbol{c}_p)$. Then matrix multiplication amounts to

$$\mathbf{AC} = (\mathbf{A}\boldsymbol{c}_1, \dots, \mathbf{A}\boldsymbol{c}_p). \tag{3·27.3}$$

This is just rephrasing the definition more vividly.

3·28. Concerns about the definition. We should not get too ahead of ourselves here, we want to check matrix multiplication has nice properties. Presumably not all the properties of multiplying numbers, but hopefully enough of them. We should check for associativity (very important property), commutativity (nice but inessential), and distributivity over [matrix] addition.

3·29. Theorem (Associativity)**.** *Let $\mathbf{A}$ be an $m \times n$ matrix, $\mathbf{B}$ be an $n \times p$ matrix, and $\mathbf{C}$ a $p \times q$ matrix. Then matrix multiplication is associative, i.e.,*

$$\mathbf{A}(\mathbf{BC}) = (\mathbf{AB})\mathbf{C}. \tag{3·29.1}$$

There are two ways to prove this. The first is to define $\mathbf{R} = \mathbf{BC}$ and $\mathbf{L} = \mathbf{AB}$, then unfold the definitions to show $\mathbf{A}(\mathbf{BC}) = \mathbf{AR}$ (by definition of $\mathbf{R}$) and $(\mathbf{AB})\mathbf{C} = \mathbf{LC}$, and then unfolding the definition of matrix multiplication we would prove $\mathbf{AR} = \mathbf{LC}$. This involves rather nasty nested sums.

The second approach is by induction on q. When $q = 1$, we have $\mathbf{C}$ be a column p-vector $\mathbf{C} = \boldsymbol{c}_1$. Matrix multiplication becomes far more intuitive in this case. Proving $\mathbf{A}(\mathbf{B}\boldsymbol{c}_1) = (\mathbf{AB})\boldsymbol{c}_1$ is the base case of induction. Then we assume the inductive hypothesis (i.e., this works for arbitrary q, that $(\mathbf{AB})\mathbf{C}_q = \mathbf{A}(\mathbf{BC}_q)$). Then we have to prove the inductive case, when $\mathbf{C} = (\mathbf{C}_q, \boldsymbol{c}_{q+1})$ is the block structure of $\mathbf{C}$. Intuitively this describes the process of "adding another column to $\mathbf{C}$, and proving associativity still holds". When combined with the base case, it suffices to prove this works for any q.

3·29.1. *Remark.* One intuition of vectors is that they describe a certain state or configuration, where each component refers to a different degree-of-freedom. In Neo-Ricardian economics, this would be one possible stock of goods (each component referring to a different commodity). In physics, the components would be the coordinates for the positions of various bodies.

Matrices then are used to transform states $\mathbf{A}\boldsymbol{x}_{\text{old}} = \boldsymbol{x}_{\text{new}}$. In Neo-Ricardian economics, this is precisely the production process. In physics, this could be the effect of rotation about an axis by a certain angle, or time-evolution forward a certain amount of time.

Matrix multiplication describes composing these transformations (from right to left), if $\mathbf{A}_1\boldsymbol{x}_0 = \boldsymbol{x}_1$ describes how $\mathbf{A}_1$ transforms $\boldsymbol{x}_0$, then $\mathbf{A}_2\mathbf{A}_1\boldsymbol{x}_0 = \mathbf{A}_2\boldsymbol{x}_1$. We could use associativity to create a composite process $\mathbf{A}_{\text{composite}} = \mathbf{A}_2\mathbf{A}_1$. But what's more, we could create a composite process from any (finite number) of intermediate processes, by matrix multiplication!

3·30. Example (Matrix Multiplication is NOT commutative). Lets compute

$$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}=\begin{bmatrix}2 & 1\\1 & 1\end{bmatrix} \tag{3·30.1a}$$

But at the same time, if we try commuting these two matrices, we get

$$\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}=\begin{bmatrix}1 & 1\\1 & 2\end{bmatrix}. \tag{3·30.1b}$$

Hence we conclude matrix multiplication is noncommutative, because we have found a counter-example. And one counter-example is all we need to disprove the hypothesis "Matrix multiplication is commutative".

3·31. Proposition. *Let r be a number, let $\mathbf{A}$ be an $m\times n$ matrix, let $\mathbf{B}$ be an $n\times p$ matrix. Then $\mathbf{A}(r\mathbf{B})=r(\mathbf{AB})=(r\mathbf{A})\mathbf{B}$.*

3·32. Proposition. *Let $\mathbf{A}$ be an $m\times n$ matrix, let $\mathbf{B}$ be an $n\times p$ matrix. Then the transpose of matrix product is the matrix multiplication of the transposes, $(\mathbf{AB})^{\mathsf{T}}=\mathbf{B}^{\mathsf{T}}\mathbf{A}^{\mathsf{T}}$.*

The proof will involve two steps: (1) expanding out $((\mathbf{AB})^{\mathsf{T}})_{k,i}$, and (2) expanding out $(\mathbf{B}^{\mathsf{T}}\mathbf{A}^{\mathsf{T}})_{k,i}$. Then we will find they are identical for every i, k.

Proof. First we find

$$(\mathbf{B}^{\mathsf{T}}\mathbf{A}^{\mathsf{T}})_{k,i}$$

= (definition of matrix multiplication)

$$\sum_{j=1}^{n}(\mathbf{B}^{\mathsf{T}})_{k,j}(\mathbf{A}^{\mathsf{T}})_{j,i}$$

= (definition of transpose)

$$\sum_{j=1}^{n}(\mathbf{B})_{j,k}(\mathbf{A})_{i,j}$$

= (commutativity of multiplying components)

$$\sum_{j=1}^{n}(\mathbf{A})_{i,j}(\mathbf{B})_{j,k}. \tag{3·32.1a}$$

We similarly find, starting "from the other end" of the desired result,

$$\big((\mathbf{AB})^{\mathsf{T}}\big)_{k,i}$$

= (definition of transpose)

$$(\mathbf{AB})_{i,k}$$

= (definition of matrix multiplication)

$$\sum_{j=1}^{n}(\mathbf{A})_{i,j}(\mathbf{B})_{j,k}. \tag{3·32.1b}$$

But by comparing these two results, we find them identical, and since it's true for every component of the product, we are forced to conclude

$$(\mathbf{AB})^{\mathsf{T}}=\mathbf{B}^{\mathsf{T}}\mathbf{A}^{\mathsf{T}} \tag{3·32.1c}$$

Hence the result. □

▸ **Problem 1.** Is it true that $(\mathbf{ABC})^{\mathsf{T}}=\mathbf{C}^{\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{A}^{\mathsf{T}}$? What if we had n factors, is it true that $(\mathbf{A}_1\dots\mathbf{A}_n)^{\mathsf{T}}=\mathbf{A}_n^{\mathsf{T}}\dots\mathbf{A}_1^{\mathsf{T}}$?

3·33. Example (Plane geometry)**.** We can look at 2×2 matrices as acting on points $(x, y) \in \mathbb{R}^2$ on the plane. We turn (x, y) into a column vector.

We have rotation anticlockwise by an angle θ given by

$$\mathbf{A}_\theta = \begin{bmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{bmatrix}. \tag{3·33.1}$$

Reflection about the x-axis is

$$\mathbf{R} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}. \tag{3·33.2}$$

Dilation by a positive real number $\lambda > 0$ is a diagonal matrix

$$\mathbf{D}_\lambda = \begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}. \tag{3·33.3}$$

Observe for $0 < \lambda < 1$, $\mathbf{D}_\lambda$ is a contraction.

3·34. Definition. Let n be a non-negative integer, let $\mathbf{A}$ be a square matrix. We define the **"Matrix Power"** of $\mathbf{A}$ raised to the n^{th} power as the matrix $\mathbf{A}^n$ inductively defined by:

1. $\mathbf{A}^0 = \mathbf{I}$, and
2. $\mathbf{A}^{n+1} = \mathbf{A}^n\mathbf{A}$ (and in particular $\mathbf{A}^1 = \mathbf{A}$).

So we have

$$\underbrace{\mathbf{A}\cdots\mathbf{A}}_{n\text{ times}} = \prod_{j=1}^{n}\mathbf{A} = \mathbf{A}^n. \tag{3·34.1}$$

3·35. Example. Consider

$$\mathbf{J} = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}. \tag{3·35.1}$$

Then

$$\mathbf{J}^2 = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix} = -\mathbf{I}_2. \tag{3·35.2}$$

Thus we have discovered some matrix which "acts like" $\sqrt{-1}$. There is something profound here, if we examine Example 3·33, we will find J amounts to a rotation in $\mathbb{R}^2$ anticlockwise by $90°$. This is precisely what happens if we multiply numbers in the complex plane by $\mathrm{i} = \sqrt{-1}$.

3·36. Example. The Fibonacci sequence is defined by $F_0 = 0$, $F_1 = 1$, and

$$F_{n+1} = F_n + F_{n-1}. \tag{3·36.1}$$

We see that

$$F_{n+2} = F_{n+1} + F_n = (F_n + F_{n-1}) = 2F_n + F_{n-1}. \tag{3·36.2}$$

Then we can describe it using a system of equations

$$\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}F_{n-1}\\ F_n\end{pmatrix} = \begin{pmatrix}F_{n+1}\\ F_{n+2}\end{pmatrix}. \tag{3·36.3}$$

We can use matrix power to simplify calculations to

$$\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}^n\begin{pmatrix}0\\ 1\end{pmatrix} = \begin{pmatrix}F_n\\ F_{n+1}\end{pmatrix}. \tag{3·36.4}$$

We will later find a really slick way to compute the powers of a matrix quickly, because right now all we've done is rephrased the recurrence relation in new notation.

▸ **Problem 2.** For any square matrix $\mathbf{A}$ and non-negative integers p and q, prove $(\mathbf{A}^p)^q = \mathbf{A}^{pq}$ and $\mathbf{A}^p\mathbf{A}^q = \mathbf{A}^{p+q}$.

▸ **Problem 3.** Let $\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Compute $\mathbf{A}^n$. Start with $n = 2$, 3, 4, then try to generalize the results.

3·37. Puzzle. Suppose we have an $m \times n$ matrix $\mathbf{A}$. When will there be an $n \times m$ matrix $\mathbf{B}$ such that $\mathbf{BA} = \mathbf{I}_n$? Or $\mathbf{AB} = \mathbf{I}_m$?

Exercises

▸ **Exercise 3.7.** If you've never proven the geometric series formally, compute

$$(1-x)\left(\sum_{n=0}^{\infty} x^n\right)$$

formally (i.e., without worrying about convergence, just manipulate things algebraically, assuming the usual rules of arithmetic apply to variables).

▸ **Exercise 3.8.** What is the computational complexity of matrix multiplication? That is to say, if $\mathbf{A}$ is an $m \times n$ matrix and $\mathbf{B}$ is an $n \times p$ matrix, how many addition and multiplication operations [of numbers] are needed to compute $\mathbf{AB}$? [Hint: do this for the dot product of vectors, then do this for every entry in the result of the matrix multiplication.]

▸ **Exercise 3.9** (Discussion question)**.** If we recall the Taylor series expansion for $\exp(x)$ from basic calculus,

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!},$$

could we pretend this works when x is a square matrix? Why or why not? Would this correspond to the limit definition of the exponential function

$$\exp(x) = \lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n$$

if we could replace x with a square matrix?

▸ **Exercise 3.10** (Left distributivity over addition)**.** Prove or find a counter-example: for any matrices [of suitable dimensions] $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$, we have $\mathbf{A}(\mathbf{B} + \mathbf{C} = \mathbf{AB} + \mathbf{AC}$.

▸ **Exercise 3.11** (Right distributivity over addition)**.** Prove or find a counter-example: for any matrices [of suitable dimensions] $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$, we have $(\mathbf{A} + \mathbf{B})\mathbf{C} = \mathbf{AC} + \mathbf{BC}$.

3.3 Matrix Inverse

3·38. Definition. Let $\mathbf{A}$ be an $n \times n$ matrix. We call an $n \times n$ matrix $\mathbf{B}$ an **"Inverse"** of $\mathbf{A}$ if

$$\mathbf{AB} = \mathbf{BA} = \mathbf{I}_n. \tag{3·38.1}$$

In this case, we call $\mathbf{A}$ **"Invertible"** (or **"Nonsingular"**).

Otherwise, if no such $\mathbf{B}$ exists, then $\mathbf{A}$ is called a **"Noninvertible"** (or **"Singular"**) matrix.

3·39. Example. The identity matrix is its own inverse. The zero matrix has no inverse.

3·40. Theorem (Uniqueness of inverse matrix)**.** *Let* $\mathbf{A}$ *be an* $n \times n$ *matrix. Assume* $\mathbf{B}$ *is the inverse matrix for* $\mathbf{A}$*. Then* $\mathbf{B}$ *is unique.*

By "unique", we mean if we happen to come across another inverse of $\mathbf{A}$, then it will be equal (by matrix equality) to $\mathbf{B}$.

Proof. Let $\mathbf{B}_1$ and $\mathbf{B}_2$ be inverse matrices for $\mathbf{A}$. We will prove $\mathbf{B}_1 = \mathbf{B}_2$.

Consider the following calculation:

$\mathbf{B}_1$

= (defining property of identity matrix)

(3·40.1a) $\mathbf{B}_1\mathbf{I}_n$

= (definition of inverse matrix)

(3·40.1b) $\mathbf{B}_1(\mathbf{A}\mathbf{B}_2)$

= (associativity of matrix multiplication)

(3·40.1c) $(\mathbf{B}_1\mathbf{A})\mathbf{B}_2$

= (definition of matrix inverse)

(3·40.1d) $\mathbf{I}_n\mathbf{B}_2$

= (defining property of identity matrix)

(3·40.1e) $\mathbf{B}_2$.

Hence we conclude $\mathbf{B}_1 = \mathbf{B}_2$, as desired. □

3·41. Notation for Inverse Matrix. Since the inverse matrix is unique (if it exists), we will denote the matrix inverse of $\mathbf{A}$ by $\mathbf{A}^{-1}$.

3·42. Example. Consider the matrix

$$\varepsilon = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}. \tag{3·42.1}$$

This is noninvertible. How can we see it? Well, we observe

$$\varepsilon^2 = \mathbf{0}. \tag{3·42.2}$$

If ε had an inverse matrix $\mathbf{A}$, then

ε

= (defining property of identity matrix)

(3·42.3a) $\mathbf{I}_2\varepsilon$

= (using the fact $\mathbf{A}$ is an inverse matrix)

(3·42.3b) $(\mathbf{A}\varepsilon)\varepsilon$

= (associativity of matrix multiplication)

(3·42.3c) $\mathbf{A}(\varepsilon^2)$

= (by Eq (3·42.2))

(3·42.3d) $\mathbf{A}(\mathbf{0})$

= (defining property of zero matrix)

(3·42.3e) $\mathbf{0}$.

Hence if ε were invertible, we would have $\varepsilon = \mathbf{0}$. But this contradicts the definition of ε, which is a nonzero matrix. Thus we are forced to conclude ε is noninvertible.

3·43. Solving Systems of Linear Equations. Returning to our original motivation for this diversion into matrix algebra, we can now use matrix inversion to solve systems of linear equations. We do it thus:[2]

$\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$

$\equiv$ (multiply both sides by $\mathbf{A}^{-1}$)

(3·43.1a) $\mathbf{A}^{-1}(\mathbf{A}\boldsymbol{x}) = \mathbf{A}^{-1}\boldsymbol{b}$

$\equiv$ (associativity of matrix multiplication)

(3·43.1b) $(\mathbf{A}^{-1}\mathbf{A})\boldsymbol{x} = \mathbf{A}^{-1}\boldsymbol{b}$

$\equiv$ (definition of matrix inverse)

(3·43.1c) $\mathbf{I}_n\boldsymbol{x} = \mathbf{A}^{-1}\boldsymbol{b}$

$\equiv$ (defining property of identity matrix)

(3·43.1d) $\boldsymbol{x} = \mathbf{A}^{-1}\boldsymbol{b}$

But we have just traded notation for notation: we currently have no algorithm to compute the inverse of a matrix! While this is true, we can still meaningfully prove properties about the matrix inverse (a useful skill for mathematicians to know, how to prove things despite lacking an algorithm for computing it). But we will address this problem in the next couple sections.

3·44. Theorem (Inverse of products). *Let* $\mathbf{A}$*,* $\mathbf{B}$ *be invertible [square] matrices. Then* $(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$*.*

Proof. We compute directly

$(\mathbf{AB})^{-1}\mathbf{AB} = \mathbf{I}$

$\equiv$ (multiply on right by $\mathbf{B}^{-1}$)

(3·44.1a) $(\mathbf{AB})^{-1}\mathbf{ABB}^{-1} = \mathbf{IB}^{-1}$

$\equiv$ (associativity of matrix multiplication, defining property of $\mathbf{I}$)

(3·44.1b) $(\mathbf{AB})^{-1}\mathbf{A}(\mathbf{BB}^{-1}) = \mathbf{B}^{-1}$

$\equiv$ (definition of matrix inverse of $\mathbf{B}$)

(3·44.1c) $(\mathbf{AB})^{-1}\mathbf{AI} = \mathbf{B}^{-1}$

$\equiv$ (defining property of identity matrix)

(3·44.1d) $(\mathbf{AB})^{-1}\mathbf{A} = \mathbf{B}^{-1}$

$\equiv$ (multiply both sides on right by $\mathbf{A}^{-1}$)

(3·44.1e) $(\mathbf{AB})^{-1}\mathbf{AA}^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$

$\equiv$ (associativity of matrix multiplication)

(3·44.1f) $(\mathbf{AB})^{-1}(\mathbf{AA}^{-1}) = \mathbf{B}^{-1}\mathbf{A}^{-1}$

$\equiv$ (definition of matrix inverse)

(3·44.1g) $(\mathbf{AB})^{-1}\mathbf{I} = \mathbf{B}^{-1}\mathbf{A}^{-1}$

$\equiv$ (defining property of identity matrix)

(3·44.1h) $(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$

Hence we obtain the desired result. $\square$

3·45. Proposition (Inverse commutes with transpose). *Let* $\mathbf{A}$ *be an invertible matrix. Then* $(\mathbf{A}^{-1})^{\mathsf{T}} = (\mathbf{A}^{\mathsf{T}})^{-1}$*.*

[2] Since we are proving equations are logically equivalent to each other, we write $(A = B) \equiv (A' = B')$ for "$(A = B)$ is logically equivalent to $(A' = B')$, in the sense that one implies the other *and* vice-versa".

Proof. Recall Proposition 3·32 which established the product of the transpose is the product-in-reverse-order of transposes $(\mathbf{AB})^{\top} = \mathbf{B}^{\top}\mathbf{A}^{\top}$. Set $\mathbf{B} = \mathbf{A}^{-1}$. We find the left hand side becomes,

$$(\mathbf{AB})^{\top} = (\mathbf{A}\mathbf{A}^{-1})^{\top} = \mathbf{I}^{\top} = \mathbf{I}; \tag{3·45.1}$$

the right-hand side becomes

$$\mathbf{B}^{\top}\mathbf{A}^{\top} = (\mathbf{A}^{-1})^{\top}\mathbf{A}^{\top}. \tag{3·45.2}$$

Setting these equal yields

$(\mathbf{A}^{-1})^{\top}\mathbf{A}^{\top} = \mathbf{I}$

$\equiv$ (multiply both sides on the right by $(\mathbf{A}^{\top})^{-1}$)

(3·45.3a) $(\mathbf{A}^{-1})^{\top}\mathbf{A}^{\top}(\mathbf{A}^{\top})^{-1} = \mathbf{I}(\mathbf{A}^{\top})^{-1}$

$\equiv$ (associativity of matrix multiplication, defining property of identity matrix)

(3·45.3b) $(\mathbf{A}^{-1})^{\top}(\mathbf{A}^{\top}(\mathbf{A}^{\top})^{-1}) = (\mathbf{A}^{\top})^{-1}$

$\equiv$ (definition of matrix inverse)

(3·45.3c) $(\mathbf{A}^{-1})^{\top}\mathbf{I} = (\mathbf{A}^{\top})^{-1}$

$\equiv$ (defining property of identity matrix)

(3·45.3d) $(\mathbf{A}^{-1})^{\top} = (\mathbf{A}^{\top})^{-1}$

Hence we obtain the desired result. □

3·46. Proposition (Matrix inversion is idempotent)**.** *Let* $\mathbf{A}$ *be an invertible matrix. Then* $(\mathbf{A}^{-1})^{-1} = \mathbf{A}$

Proof. Let $\mathbf{B} = \mathbf{A}^{-1}$. Then $\mathbf{AB} = \mathbf{BA} = \mathbf{I}$. But this implies $\mathbf{A} = \mathbf{B}^{-1} = (\mathbf{A}^{-1})^{-1}$, as desired. □

3·47. Definition. Let $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ be a system of equations. We call a solution **"Trivial"** if $\boldsymbol{x} = \mathbf{0}$ it is the zero vector. If a solution is not the zero vector, then we call it a **"Nontrivial"** solution.

3·48. Theorem. *Let* $\mathbf{A}$ *be an* $n \times n$ *matrix. The system of equations* $\mathbf{A}\boldsymbol{x} = \mathbf{0}$ *has a nontrivial solution if and only if* $\mathbf{A}$ *is singular [i.e., noninvertible].*

This statement is of the form "p if and only if q", so there are two claims being made: (1) "if p, then q", and (2) "if q, then p". We will need to prove both claims.

Proof. ($\implies$) We want to prove the claim "if $\mathbf{A}\boldsymbol{x} = \mathbf{0}$ has a nontrivial solution, then $\mathbf{A}$ is noninvertible." We can prove the contrapositive — that is, we recognize "if p, then q" is logically equivalent to "if not-q, then not-p". We assume that $\mathbf{A}$ is invertible, and we will show $\mathbf{A}\boldsymbol{x} = \mathbf{0}$ has only trivial solutions. We can see this by multiplying both sides on the left by $\mathbf{A}^{-1}$, which gives us the system $\mathbf{A}^{-1}\mathbf{A}\boldsymbol{x} = \mathbf{A}^{-1}\mathbf{0}$. The right-hand side is still the zero vector. The left-hand side is just $\boldsymbol{x}$. Hence we deduce $\boldsymbol{x} = \mathbf{0}$ — only the trivial solutions satisfy the system.

($\impliedby$) We need to prove if $\mathbf{A}$ is singular, then $\mathbf{A}\boldsymbol{x} = \mathbf{0}$ has a nontrivial solution. Logically, this looks like "$p \implies q$", which is logically equivalent to "$(\neg p) \vee q$" [either not-p, or q, or both] and "$\neg(p \wedge \neg q)$" [not (p and not-q)]. We will prove this by contradiction: we will prove "$p \wedge \neg q$ implies a contradiction".

So assume that $\mathbf{A}$ is invertible *and* $\mathbf{A}\boldsymbol{x} = \mathbf{0}$ has a nontrivial solution. But then we just proved $\mathbf{A}\boldsymbol{x} = \mathbf{0}$ implies $\mathbf{A}$ is noninvertible. We therefore conclude that $\mathbf{A}$ is both invertible and noninvertible, a contradiction. □

3·48.1. *Remark.* Proofs by contradiction always feel lackluster. Did we, you know, *do anything*? This feeling is normal.

3·49. Logically equivalent conditions to invertibility. Let $\mathbf{A}$ be an $n \times n$ matrix. The following are logically equivalent to each other:

1. $\mathbf{A}$ is invertible
2. $\boldsymbol{x} = \mathbf{0}$ is the only solution to $\mathbf{A}\boldsymbol{x} = \mathbf{0}$
3. $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ has a unique solution for every column n-vector $\boldsymbol{b}$.

Exercises

▸ **Exercise 3.12.** Prove or find a counter-example: if $\mathbf{P}$ is an invertible $n\times n$ matrix and $\mathbf{A}$ is an $n\times n$ matrix, then for any $k\in\mathbb{N}$ we have $(\mathbf{PAP}^{-1})^k = \mathbf{PA}^k\mathbf{P}^{-1}$.

▸ **Exercise 3.13.** Let $\mathbf{U}$ be a strictly upper-triangular $n\times n$ matrix (i.e., $\mathbf{U}$ is upper-triangular and its diagonal entries are zero).

1. Prove $\mathbf{U}^n = 0$
2. Prove $(\mathbf{I}+\mathbf{U})^{-1} = \sum_{k=0}^{n}\mathbf{U}^k$

▸ **Exercise 3.14.** Let $\mathbf{A}$ be an invertible $n\times n$ matrix, let $\mathbf{B}$ be an arbitrary $n\times n$ matrix, and let $0<\varepsilon\ll 1$. Prove or find a counter-example: $(\mathbf{A}+\varepsilon\mathbf{B})^{-1} = \mathbf{A}^{-1}(1+\varepsilon\mathbf{A}^{-1}\mathbf{B})^{-1}$.

▸ **Exercise 3.15.** We call a square matrix $\mathbf{A}$ **"Orthogonal"** if its transpose is its inverse $\mathbf{A}^{-1}=\mathbf{A}^{\mathsf{T}}$.

1. Is the identity matrix orthogonal?
2. If $\mathbf{A}$ is an orthogonal $n\times n$ matrix, then [letting $0<\varepsilon\ll 1$ be "infinitesimal", i.e., we ignore all terms of order ε^2 but keep terms of first-order in ε] when will $\mathbf{A}+\varepsilon\mathbf{B}$ be an orthogonal matrix?

4 Solving Linear Equations with Augmented Matrices

4·1. Recall (§3·43) we found a way to encode a system of linear equations using matrix notation as

$$\mathbf{A}\boldsymbol{x} = \boldsymbol{b}. \tag{4·1.1}$$

But we got no farther than that. Now we will begin to solve such a system in an algorithmic manner.

Our first step will be to work with an **"Augmented Matrix"**, which has block form

$$(\mathbf{A}\mid\boldsymbol{b}). \tag{4·1.2}$$

Since the unknowns (encoded in the vector $\boldsymbol{x}$) are not known, we omit them from the augmented matrix. For a concrete example:

$$\begin{pmatrix}4&3&3\\-4&-1&1\\-1&-1&-1\\0&2&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}-5\\1\\-2\\-1\end{pmatrix}\mapsto\left[\begin{array}{ccc|c}4&3&3&-5\\-4&-1&1&1\\-1&-1&-1&-2\\0&2&1&-1\end{array}\right] \tag{4·1.3}$$

This is our first step, now what?

We will apply certain elementary row operations to repeatedly modify our augmented matrix until it's in a form suitable for solving. Let us define our elementary row operations, then lay out the criteria for an augmented matrix being "suitably nice".

4·2. Definition. Let $\mathbf{A}$ be a matrix. We define an **"Elementary Row Operation"** to be one of the following:

1. Multiply row i by a nonzero scalar r,
2. Add a multiple of row i to row j,
3. Swap rows i and j.

4·2.1. *Remark.* These elementary row operations correspond to (respectively):

1. Multiply both sides of equation i by a nonzero number r,
2. Add a multiple of equation i to equation j,
3. Swap equations i and j.

We see this is permitted by elementary algebra.

4·3. Definition. Let $\mathbf{A}$ be a matrix. We say it is in **"Reduced Row Echelon Form"**

1. All rows consisting of zeroes are at the bottom of the matrix, and
2. The leading coefficient of a nonzero row is strictly "to the right" of the leading coefficient of the row above it, and
3. The leading coefficient is 1.

4·3.1. *Remark.* Some authors do not require "the leading coefficient is 1" to the criteria, but we require it.

4·4. Example. A generic reduced row echelon form matrix looks like

$$\begin{bmatrix}
1 & a_{1,2} & a_{1,3} & \dots & a_{1,j} & a_{1,j+1} & a_{1,j+2} & a_{1,j+3} & \dots & a_{1,n} \\
0 & 1 & a_{2,3} & \dots & a_{2,j} & a_{2,j+1} & a_{2,j+2} & a_{2,j+3} & \dots & a_{2,n} \\
0 & 0 & 1 & \dots & a_{3,j} & a_{3,j+1} & a_{3,j+2} & a_{3,j+3} & \dots & a_{3,n} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \dots & 0 & 1 & a_{i,j+2} & a_{i,j+3} & \dots & a_{i,n} \\
0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & \dots & a_{i+1,n} \\
0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0
\end{bmatrix} \tag{4·4.1}$$

4·5. Example. For an augmented matrix in reduced row echelon form, we have

$$\left[\begin{array}{ccc|c} 1 & 2 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{array}\right] \tag{4·5.1}$$

This would correspond to the system of equations

$$\begin{aligned} 1x_1 + 2x_2 + 0x_3 &= 1 \\ 0x_1 + 1x_2 + 0x_3 &= 1 \\ 0x_1 + 0x_2 + 1x_3 &= 2 \end{aligned}$$

We can solve this immediately, finding $x_3 = 2$, $x_2 = 1$, and $x_1 = -1$.

4.1 Gauss–Jordan Elimination

4·6. The idea is to use elementary row operations to transform our augmented matrix $(\mathbf{A} \mid \boldsymbol{b})$ to reduced row echelon form $(\mathbf{B} \mid \boldsymbol{c})$, then solve the system of equations $\mathbf{B}\boldsymbol{x} = \boldsymbol{c}$ which will also be a solution to $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$.

We see that the two augmented matrices $(\mathbf{A} \mid \boldsymbol{b})$ and $(\mathbf{B} \mid \boldsymbol{c})$ are "the same", very analogous to how the fractions 1/2 and 2/4 are "the same" despite having different numerators and denominators. Before demonstrating Gaussian elimination, let us formalize this notion of "sameness".

4·7. Definition. We call two augmented matrices $(\mathbf{A} \mid \boldsymbol{b})$ and $(\mathbf{B} \mid \boldsymbol{c})$ **"Equivalent"** if they have the same solutions, and denote this by $(\mathbf{A} \mid \boldsymbol{b}) \sim (\mathbf{B} \mid \boldsymbol{c})$.

More generally, any two $m \times n$ matrices $\mathbf{A}$, $\mathbf{B}$ are **"Equivalent"** if there is a finite sequence of elementary row operations that transforms $\mathbf{A}$ into $\mathbf{B}$. (Further, "equivalence of augmented matrices" coincides with "equivalence of matrices", so we will use the same symbol $\sim$ for both of them.)

4·8. Proposition. *Matrix equivalence satisfies the following properties:*

1. *Reflexivity: for any matrix* $\mathbf{A}$*, we have* $\mathbf{A} \sim \mathbf{A}$
2. *Symmetry: for any* $m \times n$ *matrices* $\mathbf{A}$ *and* $\mathbf{B}$*, we have* $\mathbf{A} \sim \mathbf{B}$ *implies* $\mathbf{B} \sim \mathbf{A}$
3. *Transitivity: for any* $m \times n$ *matrices* $\mathbf{A}$*,* $\mathbf{B}$*,* $\mathbf{C}$*, we have* $\mathbf{A} \sim \mathbf{B}$ *and* $\mathbf{B} \sim \mathbf{C}$ *implies* $\mathbf{A} \sim \mathbf{C}$*.*

4·9. Gauss–Jordan Elimination. Consider the augmented matrix

$$\left[\begin{array}{ccc:c} 0 & 0 & 1 & 6\\ 2 & 4 & 6 & 8\\ 2 & 3 & 4 & 5 \end{array}\right] \tag{4·9.1a}$$

The algorithm for transforming it to reduced row echelon form consists of the following steps.

Step 1: Locate nonzero column. Look for the first column that is not all zeroes. We can see this is the first column (highlighted):

$$\left[\begin{array}{ccc:c} 0 & 0 & 1 & 6\\ 2 & 4 & 6 & 8\\ 2 & 3 & 4 & 5 \end{array}\right] \tag{4·9.1b}$$

If, for some reason, the first column is a zero column vector, move to the next column to the right (and keep moving until you find the first column vector which is not a zero column vector); we will ignore the zero columns, and refer to the first nonzero column vector as "the first column" or "the leading column".

Step 2: Pivot. If the first row has a zero entry in the leading column, swap a row with a nonzero entry in the leading column. We could pick *any* such row with a nonzero entry in the leading column, we will swap the second row

$$\left[\begin{array}{ccc:c} 0 & 0 & 1 & 6\\ 2 & 4 & 6 & 8\\ 2 & 3 & 4 & 5 \end{array}\right] \sim \left[\begin{array}{ccc:c} 2 & 4 & 6 & 8\\ 0 & 0 & 1 & 6\\ 2 & 3 & 4 & 5 \end{array}\right]. \tag{4·9.1c}$$

Step 3: Normalize. We now normalize the top row by diving through by the nonzero pivot (or, equivalent, multiplying by $1/(\text{pivot})$). For us, this is dividing the first row by 2:

$$\left[\begin{array}{ccc:c} 2 & 4 & 6 & 8\\ 0 & 0 & 1 & 6\\ 2 & 3 & 4 & 5 \end{array}\right] \sim \left[\begin{array}{ccc:c} 1 & 2 & 3 & 4\\ 0 & 0 & 1 & 6\\ 2 & 3 & 4 & 5 \end{array}\right] \tag{4·9.1d}$$

Step 4: Transform lower rows. For each row *below the first row* with a nonzero leading component, we will subtract a multiple of the first row from it. The idea is to transform each row *below the first row* to have a zero entry in the leading column. For us, we see there is one row [beneath the first row] with a nonzero entry in the leading column, highlighted in blue:

$$\left[\begin{array}{ccc:c} 1 & 2 & 3 & 4\\ 0 & 0 & 1 & 6\\ 2 & 3 & 4 & 5 \end{array}\right] \tag{4·9.1e}$$

We then add -2 times the first row to the third row, giving us

$$\left[\begin{array}{ccc:c} 1 & 2 & 3 & 4\\ 0 & 0 & 1 & 6\\ 2 & 3 & 4 & 5 \end{array}\right] \sim \left[\begin{array}{ccc:c} 1 & 2 & 3 & 4\\ 0 & 0 & 1 & 6\\ 0 & -1 & -2 & -3 \end{array}\right] \tag{4·9.1f}$$

At this point, the first column with a nonzero entry will have its general form look like $(1, 0, 0, \dots, 0)$ (i.e., it leads with 1 and all entries below it are zero).

Step 5: Repeat on the submatrix. We take the submatrix for the remaining rows and remaining columns, then return to step 1, and transform the submatrix to reduced row echelon form.

$$\left[\begin{array}{c|cc:c} 1 & 2 & 3 & 4\\ \cline{2-4} 0 & 0 & 1 & 6\\ 0 & -1 & -2 & -3 \end{array}\right] \tag{4·9.1g}$$

We will find, for our particular example, the matrix has reduced row echelon form

$$\cdots \sim \left[\begin{array}{ccc:c} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 6 \end{array}\right]. \tag{4·9.1h}$$

4·9.1. *Remark.* We should prove that Gauss-Jordan elimination produces a unique augmented matrix, in some sense. It's obviously not true the results will be identical, since we had some choice in swapping rows. But the solutions produced from the resulting augmented matrices *will* be identical. After a few examples, we will prove this.

4·10. Gaussian Elimination. We may optionally skip normalizing the "pivot" (step 3), but continue to transform the lower rows so everything below the pivot is zero. The slightly modified algorithm is referred to as **"Gaussian Elimination"**, *not* to be confused with Gauss–Jordan elimination.

Gaussian elimination produces a matrix in **"Row Echelon Form"**. The matrix is no longer "reduced", because the pivots are not necessarily 1.

Is there a reason to prefer one or the other? Well, with Gaussian elimination, we could do it with a number system without division (like, the integers). But with Gauss–Jordan elimination, when solving the system of equations, step 3 avoids a division operation later on (which can be convenient). One method is not "better" than the other, but they are *different* "siblings".

4·11. Example. Suppose we have a 2×2 matrix $\mathbf{A}$ with generic entries

$$\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}. \tag{4·11.1}$$

Suppose $\mathbf{A}$ is invertible. What are the components of $\mathbf{A}^{-1}$?

Right now, they are unknowns

$$\mathbf{A}^{-1} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}. \tag{4·11.2a}$$

Matrix multiplication gives us

$$\mathbf{A}\mathbf{A}^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{bmatrix}. \tag{4·11.2b}$$

Which. . . does not really seem to improve the situation. Or does it? We expect this to be equal to the identity matrix, and really this is a system of 4 linear equations

$$\left.\begin{array}{ccccccc} ax & & +bz & & = & 1 \\ & ay & & +bw & = & 0 \\ cx & & +dz & & = & 0 \\ & cy & & +dw & = & 1 \end{array}\right\} \equiv \left(\begin{array}{cccc:c} a & & b & & 1 \\ & a & & b & 0 \\ c & & d & & 0 \\ & c & & d & 1 \end{array}\right) \tag{4·11.2c}$$

We can now transform this augmented matrix to row echelon form (not reduced, but still row echelon form).

$$\begin{aligned} &\left(\begin{array}{cccc:c} a & 0 & b & 0 & 1 \\ 0 & a & 0 & b & 0 \\ c & 0 & d & 0 & 0 \\ 0 & c & 0 & d & 1 \end{array}\right) \\ \sim\quad & \text{(add } (-c/a)\text{(row 1) to row 3)} \\ & \left(\begin{array}{cccc:c} a & 0 & b & 0 & 1 \\ 0 & a & 0 & b & 0 \\ 0 & 0 & d-\dfrac{bc}{a} & 0 & \dfrac{-c}{a} \\ 0 & c & 0 & d & 1 \end{array}\right) \end{aligned} \tag{4·11.3a}$$

$\sim$ (add $(-c/a)$(row 2) to row 4)

$$\left(\begin{array}{cccc:c} a & 0 & b & 0 & 1 \\ 0 & a & 0 & b & 0 \\ 0 & 0 & d - \dfrac{bc}{a} & 0 & \dfrac{-c}{a} \\ 0 & 0 & 0 & d - \dfrac{bc}{a} & 1 \end{array}\right) \tag{4·11.3b}$$

$\sim$ (since $d - (bc/a) = (ad - bc)/a$)

$$\left(\begin{array}{cccc:c} a & 0 & b & 0 & 1 \\ 0 & a & 0 & b & 0 \\ 0 & 0 & \dfrac{ad-bc}{a} & 0 & \dfrac{-c}{a} \\ 0 & 0 & 0 & \dfrac{ad-bc}{a} & 1 \end{array}\right) \tag{4·11.3c}$$

This has solution

$$w = \frac{a}{ad - bc} \tag{4·11.4a}$$

$$z = \frac{-c}{ad - bc} \tag{4·11.4b}$$

$$y = \frac{-b}{ad - bc} \tag{4·11.4c}$$

$$\begin{aligned} ax - \frac{bc}{ad - bc} &= 1 \\ \implies ax &= \frac{bc}{ad - bc} + 1 = \frac{ad}{ad - bc} \\ \implies x &= \frac{d}{ad - bc}. \end{aligned} \tag{4·11.4d}$$

Hence

$$\boxed{\mathbf{A}^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.} \tag{4·11.5}$$

4·12. Algorithm to determine inverse matrix. From the previous example, we see that we could rephrase our process as considering the $n \times 2n$ augmented matrix $(\mathbf{A} \mid \mathbf{I})$, then "applying Gauss–Jordan elimination and backsubstituting" (i.e., applying elementary row operations until) we obtain

$$(\mathbf{A} \mid \mathbf{I}) \sim (\mathbf{I} \mid \mathbf{A}^{-1}). \tag{4·12.1}$$

If elementary row operations cannot transform $\mathbf{A}$ to the identity matrix $\mathbf{A} \not\sim \mathbf{I}$, then $\mathbf{A}$ is singular.

4.2 LU-Decomposition

4·13. Some matrices are easier to work with than others. Scalar matrices are particular easy to invert, for example. We will consider what perhaps could be called the "silver bullet of linear algebra": factorizing a given matrix into a product of nicer matrices (i.e., writing $\mathbf{A} = \mathbf{M}_1 \cdots \mathbf{M}_n$).

4·14. Definition. Let $\mathbf{A}$ be an $n \times n$ matrix. Recall Definition 2·9 where we defined upper triangular and lower triangular matrices. We define the **"LU-Decomposition"** of $\mathbf{A}$ to consist of

1. a lower-triangular $n \times n$ matrix $\mathbf{L}$
2. an upper-triangular $n \times n$ matrix $\mathbf{U}$

such that

1. $\mathbf{A} = \mathbf{LU}$

4·14.1. *Remark.* Some texts add the condition that the diagonals of the lower-triangular matrix are either 1 or 0. Other texts change that condition to be imposed on the upper-triangular matrix instead. The reason for this is because there is a unique LU decomposition in those situations. Without either condition, there are many different possible LU decompositions. The reader should be aware that not one of these definitions is "better" than another — one is not "the correct definition" and the others are "wrong definitions" — but under certain circumstances, it is preferable to *adopt the convention* that we are working with the lower-triangular matrix with 1 or 0 on the diagonal (or whatever).

4·15. Why on Earth is this an improvement? Well, recall Gauss–Jordan elimination transformed $\mathbf{A}$ into an upper triangular matrix $\mathbf{U}$, and that was how we could algorithmically solve systems of equations. More explicitly, if $\mathbf{U}$ is upper triangular, we can solve the system of equations

$$\mathbf{U}\boldsymbol{x} = \boldsymbol{b} \tag{4·15.1a}$$

or, written explicitly with components,

$$\begin{pmatrix} u_{1,1} & u_{1,2} & u_{1,3} & \dots & u_{1,n} \\ 0 & u_{2,2} & u_{2,3} & \dots & u_{2,n} \\ 0 & 0 & u_{3,3} & \dots & u_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & u_{n,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_n \end{pmatrix} \tag{4·15.1b}$$

The solution looks like, starting with the last equation in row n,

$$x_n = \frac{b_n}{u_{n,n}} \tag{4·15.2a}$$

then we plug this into the $n-1$ row to get,

$$x_{n-1} = \frac{1}{u_{n-1,n-1}}(b_{n-1} - u_{n-1,n}x_n) \tag{4·15.2b}$$

$$\vdots$$

and continuing until we get to row j, which has the generic solution:

$$x_j = \frac{1}{u_{j,j}}\left(b_j - \sum_{k=j+1}^{n} u_{j,k}x_k\right). \tag{4·15.2c}$$

This procedure is known as **"Backsubstitution"**.

4·16. We have a completely analogous way to handle lower-triangular matrices $\mathbf{L}$ in systems of equations

$$\begin{pmatrix} \ell_{1,1} & 0 & 0 & \dots & 0 \\ \ell_{2,1} & \ell_{2,2} & 0 & \dots & 0 \\ \ell_{3,1} & \ell_{3,2} & \ell_{3,3} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \ell_{n,1} & \ell_{n,2} & \ell_{n,3} & \dots & \ell_{n,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_n \end{pmatrix} \tag{4·16.1}$$

This time, we start with the first row, to find its solution,

$$x_1 = \frac{1}{\ell_{1,1}}(b_1) \tag{4·16.2a}$$

then plugging this into the second row gives the solution,

$$x_2 = \frac{1}{\ell_{2,2}}(b_2 - \ell_{2,1}x_1) \tag{4·16.2b}$$

and continuing to the generic row j

$$x_j = \frac{1}{\ell_{j,j}}\left(b_j - \sum_{k=1}^{j-1}\ell_{j,k}x_k\right). \tag{4·16.2c}$$

This is called **"Forward Substitution"**.

4·17. Algorithm: LU Factorization. The generic algorithm for LU decomposition is best illustrated by example. Given an $n \times n$ matrix $\mathbf{A}$. We will generate a sequence of matrices $\mathbf{L}_1$, $\mathbf{U}_1$, $\mathbf{L}_2$, $\mathbf{U}_2$, …, $\mathbf{L}_n$, $\mathbf{U}_n$ which progressively get "more triangular" until we reach the end result. Then we will call $\mathbf{U} := \mathbf{U}_n$ and $\mathbf{L} := \mathbf{L}_n$. Consider the matrix

$$\mathbf{A} = \begin{bmatrix} -2 & 1 & 3 & 4 \\ 1 & 2 & -5 & -2 \\ -1 & 1 & 25 & 3 \\ 4 & -4 & 20 & 2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{r}_1^{\mathsf{T}} \\ \boldsymbol{r}_2^{\mathsf{T}} \\ \boldsymbol{r}_3^{\mathsf{T}} \\ \boldsymbol{r}_4^{\mathsf{T}} \end{bmatrix} \tag{4·17.1}$$

where $\boldsymbol{r}_1^{\mathsf{T}}$ is the first row, $\boldsymbol{r}_2^{\mathsf{T}}$ is the second row, and so on.

Step 1. We form $\mathbf{U}_1$ by a process similar to Gauss-Jordan elimination, we will "zero out" the first column beneath the first row. We take subtract $a_{2,1}/a_{1,1} = (-1/2)$ times the first row to the second row, subtract $a_{3,1}/a_{1,1} = (1/2)$ times the first row to the third row, and subtract $a_{4,1}/a_{1,1} = (-4/2) = -2$ times the first row to the fourth row, to obtain $\mathbf{U}_1$:

$$\mathbf{U}_1 = \begin{pmatrix} \boldsymbol{r}_1^{\mathsf{T}} \\ \boldsymbol{r}_2^{\mathsf{T}} - (-1/2)\boldsymbol{r}_1^{\mathsf{T}} \\ \boldsymbol{r}_3^{\mathsf{T}} - (1/2)\boldsymbol{r}_1^{\mathsf{T}} \\ \boldsymbol{r}_4^{\mathsf{T}} - (-2)\boldsymbol{r}_1^{\mathsf{T}} \end{pmatrix} = \begin{pmatrix} -2 & 1 & 3 & 4 \\ 0 & 5/2 & -7/2 & 0 \\ 0 & 1/2 & 47/2 & 1 \\ 0 & -2 & 26 & 10 \end{pmatrix} = \begin{pmatrix} (\boldsymbol{u}_1^{(1)})^{\mathsf{T}} \\ (\boldsymbol{u}_2^{(1)})^{\mathsf{T}} \\ (\boldsymbol{u}_3^{(1)})^{\mathsf{T}} \\ (\boldsymbol{u}_4^{(1)})^{\mathsf{T}} \end{pmatrix} \tag{4·17.2}$$

We denote the rows of $\mathbf{U}_1$ using $(\boldsymbol{u}_j^{(1)})^{\mathsf{T}}$.

We construct $\mathbf{L}_1$ by taking 1 along the diagonal, and in the first column setting $\ell_{j,1}$ equal to the these multipliers, i.e., $\ell_{j,1} = a_{j,1}/a_{1,1}$:

$$\mathbf{L}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a_{2,1}/a_{1,1} & 1 & 0 & 0 \\ a_{3,1}/a_{1,1} & ? & 1 & 0 \\ a_{4,1}/a_{1,1} & ? & ? & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1/2 & 1 & 0 & 0 \\ 1/2 & ? & 1 & 0 \\ -2 & ? & ? & 1 \end{pmatrix} \tag{4·17.3}$$

Why does this work? Well, when we examine the resulting first column from the product $\mathbf{L}_1\mathbf{U}_1$ we see we recover the first column of our original matrix $\mathbf{A}$.

Step 2. Now we assemble $\mathbf{U}_2$ from $\mathbf{U}_1$. We take $\mathbf{U}_1$ and "zero out" the entries in the second column beneath the second row. We do this by subtracting $(u_{3,2}^{(1)}/u_{2,2}^{(1)}) = 1/5$ times the second row from the third row, and subtracting $(u_{4,2}^{(1)}/u_{2,2}^{(1)}) = -4/5$ time the second row from the fourth row:

$$\mathbf{U}_2 = \begin{pmatrix} (\boldsymbol{u}_1^{(1)})^{\mathsf{T}} \\ (\boldsymbol{u}_2^{(1)})^{\mathsf{T}} \\ (\boldsymbol{u}_3^{(1)})^{\mathsf{T}} - (1/5)(\boldsymbol{u}_2^{(1)})^{\mathsf{T}} \\ (\boldsymbol{u}_4^{(1)})^{\mathsf{T}} - (-4/5)(\boldsymbol{u}_2^{(1)})^{\mathsf{T}} \end{pmatrix} = \begin{pmatrix} -2 & 1 & 3 & 4 \\ 0 & 5/2 & -7/2 & 0 \\ 0 & 0 & 121/5 & 1 \\ 0 & 0 & 116/5 & 10 \end{pmatrix} = \begin{pmatrix} (\boldsymbol{u}_1^{(2)})^{\mathsf{T}} \\ (\boldsymbol{u}_2^{(2)})^{\mathsf{T}} \\ (\boldsymbol{u}_3^{(2)})^{\mathsf{T}} \\ (\boldsymbol{u}_4^{(2)})^{\mathsf{T}} \end{pmatrix}. \tag{4·17.4}$$

We denote the rows of $\mathbf{U}_2$ using $(\boldsymbol{u}_j^{(2)})^{\mathsf{T}}$.

Now we enter the multiples in the second column beneath the diagonal of $\mathbf{L}_1$ to obtain $\mathbf{L}_2$:

$$\mathbf{L}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1/2 & 1 & 0 & 0 \\ 1/2 & (u_{3,2}^{(1)}/u_{2,2}^{(1)}) & 1 & 0 \\ -2 & (u_{4,2}^{(1)}/u_{2,2}^{(1)}) & ? & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1/2 & 1 & 0 & 0 \\ 1/2 & 1/5 & 1 & 0 \\ -2 & -4/5 & ? & 1 \end{pmatrix}. \tag{4·17.5}$$

The reader can verify that the product of $\mathbf{L}_2$ and the second column of $\mathbf{U}_2$ gives the second column of $\mathbf{A}$.

Step 3. The last step for us, we need to subtract 116/121 times the third row of $\mathbf{U}_2$ from the last row of $\mathbf{U}_2$ to construct $\mathbf{U}_3$:

$$\mathbf{U}_3 = \begin{pmatrix} (\boldsymbol{u}_1^{(2)})^{\mathsf{T}} \\ (\boldsymbol{u}_2^{(2)})^{\mathsf{T}} \\ (\boldsymbol{u}_3^{(2)})^{\mathsf{T}} \\ (\boldsymbol{u}_4^{(2)})^{\mathsf{T}} - (116/121)(\boldsymbol{u}_3^{(2)})^{\mathsf{T}} \end{pmatrix} = \begin{pmatrix} -2 & 1 & 3 & 4 \\ 0 & 5/2 & -7/2 & 0 \\ 0 & 0 & 121/5 & 1 \\ 0 & 0 & 0 & 1094/121. \end{pmatrix} \tag{4·17.6}$$

We see this is upper-triangular.

Now, the last entry in the lower-triangular matrix, we set it equal to

$$\mathbf{L}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1/2 & 1 & 0 & 0 \\ 1/2 & 1/5 & 1 & 0 \\ -2 & -4/5 & (u_{4,3}^{(2)}/u_{3,3}^{(2)}) & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1/2 & 1 & 0 & 0 \\ 1/2 & 1/5 & 1 & 0 \\ -2 & -4/5 & 116/121 & 1 \end{pmatrix}. \tag{4·17.7}$$

The reader can verify that $\mathbf{L}_3$ times the third column of $\mathbf{U}_3$ produces the third column of $\mathbf{A}$, *and* that $\mathbf{L}_3$ times the last column of $\mathbf{U}_3$ produces the last column of $\mathbf{A}$.

Step 4. We then call $\mathbf{L} := \mathbf{L}_3$ and $\mathbf{U} := \mathbf{U}_3$, then return this as the LU-decomposition of $\mathbf{A}$.

4·17.1. *Remark.* The basic pattern is revealed, we are constructing $\mathbf{L}_{j+1}$ and $\mathbf{U}_{j+1}$ by modifying the $j+1$ columns of $\mathbf{L}_j$ and $\mathbf{U}_j$ such that the matrix multiplication of $\mathbf{L}_{j+1}$ times the $(j+1)^{\text{th}}$ column of $\mathbf{U}_{j+1}$ equals the $(j+1)^{\text{th}}$ column of $\mathbf{A}$. Programmers call this "property which holds after every step of the loop" an "invariant property" of the algorithm.

4·17.2. *Remark.* This LU decomposition algorithm is analogous to "long division" of numbers we learn in elementary school: we construct the quotient one digit at a time, multiplying the latest digit by the divisor, then subtracting from the residue of the dividend this product.

4·18. LU Decomposition works on any matrix. There is no reason why we need $\mathbf{A}$ to be a square matrix. We could have let it be an $m\times n$ matrix. Then $\mathbf{L}$ would be an $m\times m$ matrix and $\mathbf{U}$ would be an $m\times n$ matrix. Or $\mathbf{L}$ could be an $m\times n$ matrix, and $\mathbf{U}$ would be an $n\times n$ matrix. The algorithm works the same, regardless.

4·19. Block LU Decomposition. Suppose we have a 2×2 matrix

$$\mathbf{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{4·19.1}$$

The reader can verify

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c/a & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d-(c/a)b \end{pmatrix}. \tag{4·19.2}$$

We can go farther, and observe:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c/a & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d-(cb/a) \end{pmatrix}\begin{pmatrix} 1 & b/a \\ 0 & 1 \end{pmatrix}. \tag{4·19.3}$$

What if we have a block matrix

$$\mathbf{M} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{pmatrix}, \tag{4·19.4}$$

where $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, and $\mathbf{D}$ are all square matrices of the same dimension — say, they are all $n \times n$ matrices. could we factorize it similarly? Let us try!

We, first of all, see that we will need to find the inverse of $\mathbf{A}$ (since this is the analog to dividing by a). So before we can do anything, we *must* have $\mathbf{A}$ be an invertible matrix. If it is singular, then there is no hope of an analogous decomposition.

There is some ambiguity in trying to figure out the analog to c/a — should it be $\mathbf{A}^{-1}\mathbf{C}$ or $\mathbf{C}\mathbf{A}^{-1}$? For us to answer this question, we should ask ourselves, "What are the dimensions of $\mathbf{A}^{-1}$ and $\mathbf{C}$?" We assumed they are both $n \times n$, so either would work ostensibly. The L matrix would be multiplied by a diagonal matrix

$$L \begin{pmatrix} \mathbf{A} & 0 \\ 0 & \mathbf{D} - \text{“}cb/a\text{”} \end{pmatrix} \tag{4·19.5}$$

For this to make sense, we would have the "c/a" block multiplied on the right by $\mathbf{A}$. This means $\mathbf{C}\mathbf{A}^{-1}$ is the analogous quantity, and we find

$$L = \begin{pmatrix} \mathbf{I} & 0 \\ \mathbf{C}\mathbf{A}^{-1} & \mathbf{I} \end{pmatrix}. \tag{4·19.6}$$

Similar reasoning suggests the upper triangular matrix should be

$$U = \begin{pmatrix} \mathbf{I} & \mathbf{A}^{-1}\mathbf{B} \\ 0 & \mathbf{I} \end{pmatrix}. \tag{4·19.7}$$

Now, the diagonal matrix is the thorn in our side. If we multiply it out with the U matrix, we find

$$\begin{pmatrix} \mathbf{A} & 0 \\ 0 & \mathbf{D} - \text{“}cb/a\text{”} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{A}^{-1}\mathbf{B} \\ 0 & \mathbf{I} \end{pmatrix} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ 0 & (\mathbf{D} - \text{“}cb/a\text{”})\mathbf{I} \end{pmatrix} \tag{4·19.8}$$

Multiplying this on the left by the L matrix,

$$\begin{pmatrix} \mathbf{I} & 0 \\ \mathbf{C}\mathbf{A}^{-1} & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ 0 & \mathbf{D} - \text{“}cb/a\text{”} \end{pmatrix} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{C}\mathbf{A}^{-1}\mathbf{B} + (\mathbf{D} - \text{“}cb/a\text{”}) \end{pmatrix} \tag{4·19.9}$$

For this to equal our original matrix, we need

$$\mathbf{C}\mathbf{A}^{-1}\mathbf{B} - \text{“}cb/a\text{”} = 0 \tag{4·19.10}$$

that is to say,

$$\text{“}cb/a\text{”} = \mathbf{C}\mathbf{A}^{-1}\mathbf{B}. \tag{4·19.11}$$

This gives us the block LU decomposition of $\mathbf{M}$:

$$\boxed{\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{pmatrix} = \begin{pmatrix} \mathbf{I} & 0 \\ \mathbf{C}\mathbf{A}^{-1} & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{A} & 0 \\ 0 & \mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{A}^{-1}\mathbf{B} \\ 0 & \mathbf{I} \end{pmatrix}.} \tag{4·19.12}$$

Exercises

▸ **Exercise 4.1.** What happens if $\mathbf{A}$ is $m \times q$, $\mathbf{B}$ is $m \times p$, $\mathbf{C}$ is $n \times q$, and $\mathbf{C}$ is $n \times p$? For what values of m, n, p, and q would the block LU decomposition work? [Hint: $\mathbf{A}$ must be invertible, what constraints does that place on its dimension?][3]

[3]We could make this needlessly complicated, working with the three cases $m < q$, $m = q$, and $m > q$. For the sake of discussion, consider the two separate subcases of $m \neq q$ [for a total of 4 cases — 2 subcases of $m < q$ and 2 subcases of $m > q$]

▸ **Exercise 4.2.** Let $\mathbf{A}$ be an $m \times n$ matrix and $\mathbf{U}$ be an upper-triangular matrix. Will $\mathbf{AU}$ be [upper or lower] triangular?

▸ **Exercise 4.3.** Let

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Compute $\mathbf{A}^n$ by induction on $n \in \mathbb{N}$.

---

when there exists:

1. a matrix $\mathbf{A}_L$ is a $q \times m$ matrix such that it acts like an inverse from the left $\mathbf{A}_L\mathbf{A} = \mathbf{I}_q$ (but not necessarily from the right), and separately
2. a matrix $\mathbf{A}_R$ is an $q \times m$ matrix which acts like an inverse from the right $\mathbf{A}\mathbf{A}_R = \mathbf{I}_m$ (but not necessarily from the left).

What happens if you try computing $\mathbf{A}_R\mathbf{A}$ (and $\mathbf{A}\mathbf{A}_L$) is — at best! — you end up with a block matrix of the form $(\mathbf{I}|0)$ or its transpose. You can work this out, if you want, but we will develop more tools later that will help you answer this pathological variant problem.

4·20. STOP!!! And take a break, go out for a walk, drink a glass of water. We've covered a lot in this section, introducing a general algorithm to solve systems of linear equations, and we introduced for the first time(!) a notion of "factorization" of matrices. That's a lot of new stuff.

5 Determinant

5·1. Remember when we figured out the inverse of a 2×2 matrix, in Eq (4·11.5) there was a funny common factor of $ad-bc$. That was odd.

But if we try the same thing with a 3×3 matrix, we end up with

$$\mathbf{A}^{-1} = \begin{pmatrix} a & b & c\\ d & e & f\\ g & h & i\end{pmatrix}^{-1} = \frac{1}{a(ei-fh)-b(di-fg)+c(dh-eg)}\begin{pmatrix} A & B & C\\ D & E & F\\ G & H & I\end{pmatrix} \tag{5·1.1}$$

where A, B, C, etc., are all some mess. We're focused on the scalar factor out in front: if $b=c$ or $d=g=0$, then we recover a similar formula as in the 2×2 case. Similarly, if $a=b=0$, we recover a similar factor.

There is a recurring pattern here where, for a general $n\times n$ matrix $\mathbf{A}$, there is a common factor when computing its inverse

$$\mathbf{A}^{-1} = \frac{1}{(\text{suspicious factor})}\mathbf{B}. \tag{5·1.2}$$

If we set $(n-1)$ entries in the first row to zero, we recover the suspicious factor from the $(n-1)\times(n-1)$ matrix inverse.

This suspicious factor turns out to be extremely important.

5·2. Geometric Intuition. Think about 2-dimensional space $\mathbb{R}^2$. We could begin by examining the unit square:

$$C^2 = \{(x_1,x_2)\in\mathbb{R}^2 \mid 0\leq x_j\leq 1, j=1,2\}. \tag{5·2.1}$$

We read the right-hand side as the set (demarcated by squiggle brackets $\{\dots\}$) consisting of points in the plane $(x_1,x_2)\in\mathbb{R}^2$ ("$\in$" takes an object to its left and a set to its right) such that ("$|$" encodes "such that") $0\leq x_j\leq 1, j=1,2$ the components x_1 and x_2 lie between 0 and 1 inclusive. This notation is known as "set-builder notation". If the reader is unfamiliar with it, then they should consult Appendix [**?**].

What is its area? This is very silly, everyone learns in High School it is the product of the lengths of its sides,

$$\mathrm{Area}(C^2) = 1\times 1 = 1. \tag{5·2.2}$$

But now suppose we "deform" the square to form a parallelogram with one vertex fixed at the origin. Then we have the two sides described by endpoints located at $\boldsymbol{a}=(a_1,a_2)$ and $\boldsymbol{b}=(b_1,b_2)$.

What is its area? We can recall from vector calculus that it is the magnitude of the their cross product $|\boldsymbol{a}\times\boldsymbol{b}| = |a_1b_2-a_2b_1|$.

Does it look familiar? It should: it's precisely the suspicious factor in Eq (4·11.5).

5·3. What about the case in $\mathbb{R}^3$? What if we start with the unit cube

$$C^3 = \{(x_1,x_2,x_3)\in\mathbb{R}^3 \mid 0\leq x_j\leq 1, j=1,2,3\}. \tag{5·3.1}$$

The analogous quantity of interest is now its *volume*. What is the volume of the cube with side length equal to 1? We recall

$$\mathrm{Vol}(C^3) = 1\times 1\times 1 = 1. \tag{5·3.2}$$

Very simple.

What if we deform the (x_1,x_2) cross sections to be a parallelogram with sides at endpoints (a_1,a_2,x_3) and (b_1,b_2,x_3), like we did in the $\mathbb{R}^2$ case? Intuitively, this is "dragging" a parallelogram in the (x_1,x_2)-plane "up" the x_3-axis for a ways of 1 unit of length. What is the volume of this? It turns out to be the area of the parallelogram multiplied by the distance we drag it. Its volume would be

$$\mathrm{Vol}(P) = (a_1 b_2 - a_2 b_1) \times 1. \tag{5·3·3}$$

This is not terribly surprising, so let us deform further.

Specifically, we deform the unit cube to be a parallelepiped P with a corner fixed at the origin. The endpoints for our parallelepepiped P along its length, width, and height would be $\boldsymbol{a} = (a_1, a_2, a_3)$, $\boldsymbol{b} = (b_1, b_2, b_3)$ and $\boldsymbol{c} = (c_1, c_2, c_3)$. What is its volume? The trick is to cheat and rotate axes until $\boldsymbol{a}$ and $\boldsymbol{b}$ live in the (x_1, x_2) plane.

But if we don't know that, then we can form the unit normal to the face formed by edges $\boldsymbol{a}$ and $\boldsymbol{b}$ by taking their cross-product,

$$\widehat{\boldsymbol{n}} = \frac{\boldsymbol{a} \times \boldsymbol{b}}{|\boldsymbol{a} \times \boldsymbol{b}|}. \tag{5·3·4}$$

We find the height to be the projection of $\boldsymbol{c}$ onto this normal vector

$$h = \boldsymbol{c} \cdot \widehat{\boldsymbol{n}}. \tag{5·3·5}$$

We can find the base area B of the parallelogram formed by $\boldsymbol{a}$ and $\boldsymbol{b}$ by

$$B = |\boldsymbol{a} \times \boldsymbol{b}|, \tag{5·3·6}$$

and, as always, base times height yields volume:

$$\mathrm{Vol}(P) = Bh = |\boldsymbol{a} \times \boldsymbol{b}|\ \boldsymbol{c} \cdot \widehat{\boldsymbol{n}}. \tag{5·3·7}$$

Great, but this doesn't seem to help much. We just unfold the definition of the unit normal, and we find

$$\mathrm{Vol}(P) = |\boldsymbol{a} \times \boldsymbol{b}| \frac{\boldsymbol{c} \cdot (\boldsymbol{a} \times \boldsymbol{b})}{|\boldsymbol{a} \times \boldsymbol{b}|} = \boldsymbol{c} \cdot (\boldsymbol{a} \times \boldsymbol{b}). \tag{5·3·8}$$

What is this explicitly? Let's write it out:

$$\mathrm{Vol}(P) = c_1(a_2 b_3 - a_3 b_2) - c_2(a_1 b_3 - a_3 b_1) + c_3(a_1 b_2 - a_2 b_1). \tag{5·3·9}$$

Does it look familiar? It should: it's the suspicious factor in the case of finding the inverse for a 3×3 matrix.

5·4. In short, this suspicious factor — the exact same quantity — appears in the volume of n-dimensional parallelograms, and when computing the inverse for an $n \times n$ matrix. This is strange, because one situation is geometry whereas the other situation is algebra. "Strange" is not the correct word for it: "Profound" should be employed.

5·5. Problem: How to compute this "suspicious factor"? Now that we've established the profundity of this "suspicious factor", how exactly do we compute it? What properties does it have? Why does it matter in linear algebra? And what should we call it?

5·6. Definition. Let $\mathbf{A} = (a_{i,j})$ be an $n \times n$ matrix. We recursively define its **"Determinant"** to be a scalar, defined by:

1. if $n = 1$, we just take $\det(\mathbf{A}) = a_{1,1}$;
2. if $n = 2$, we simply take

$$\det(\mathbf{A}) = \det\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} = a_{1,1}a_{2,2} - a_{2,1}a_{1,2}; \tag{5·6.1}$$

3. for $n > 2$, we recursively define it using the formula

$$\det(\mathbf{A}) = \sum_{j=1}^{n}(-1)^{j+1}a_{1,j}\det(\mathbf{M}_{1,j}) \tag{5·6.2}$$

where $\mathbf{M}_{1,j}$ is called a *minor* of $\mathbf{A}$, obtained from $\mathbf{A}$ by deleting its first row and its j^{th} column — more generally $\mathbf{M}_{i,j}$ is obtained by deleting row i and column j from $\mathbf{A}$.

5·7. Lemma. *Let $\mathbf{A}$ be an $n\times n$ matrix with a column or row consisting of zeros. Then $\det(\mathbf{A}) = 0$.*

5·8. Theorem. *Let $\mathbf{T} = (t_{i,j})$ be a triangular $n\times n$ matrix (either upper-triangular, or lower-triangular, it doesn't matter). Then its determinant is just the product of diagonal entries $\det(\mathbf{T}) = \prod_{j=1}^{n} t_{j,j}$.*

Proof. We do this by induction on n.

Base Case: $n = 2$, for upper-triangular matrices we find

$$\det\begin{pmatrix} t_{1,1} & t_{1,2}\\ 0 & t_{2,2}\end{pmatrix} = t_{1,1}t_{2,2} - t_{1,2}0 = t_{1,1}t_{2,2}. \tag{5·8.1}$$

For lower-triangular matrices

$$\det\begin{pmatrix} t_{1,1} & 0\\ t_{2,1} & t_{2,2}\end{pmatrix} = t_{1,1}t_{2,2} - 0t_{2,1} = t_{1,1}t_{2,2}. \tag{5·8.2}$$

Hence we establish the base case.

Inductive Hypothesis: We assume this is true for general n.

Inductive Case: For the $n \to n+1$ case, we will examine two subcases. Subcase 1 is when $\mathbf{T}$ is upper-triangular, where we write the block components out:

$$\mathbf{T} = \begin{pmatrix} t_{1,1} & \boldsymbol{t}^{\mathsf{T}}\\ \mathbf{0} & \mathbf{T}^{(n)}\end{pmatrix} \tag{5·8.3}$$

The inductive hypothesis assumed $\det(\mathbf{T}^{(n)}$ is the product of diagonal components. We see that the minors $\mathbf{M}_{1,i}$ has a zero column for $i > 1$. Hence only the $i = 1$ minor contributes to the determinant, giving us

$\det(\mathbf{T})$

= (definition of determinant)

(5·8.4a) $\displaystyle\sum_{i=1}^{n+1}(-1)^{i+1}t_{1,i}\det(\mathbf{M}_{1,i})$

= (pulling out the first term from the sum)

(5·8.4b) $\displaystyle t_{1,1}\det(\mathbf{M}_{1,1}) + \sum_{i=2}^{n+1}(-1)^{i+1}t_{1,i}\det(\mathbf{M}_{1,i})$

= (but $\det(\mathbf{M}_{1,i}) = 0$ for $i > 1$)

(5·8.4c) $\displaystyle t_{1,1}\det(\mathbf{M}_{1,1}) + \sum_{i=2}^{n+1}(-1)^{i+1}t_{1,i}\cdot 0$

= (the sum of zeros is zero)

(5·8.4d) $t_{1,1}\det(\mathbf{M}_{1,1}) + 0$

= (arithmetic)

(5·8.4e) $t_{1,1}\det(\mathbf{M}_{1,1})$

= (the minor $\mathbf{M}_{1,1} = \mathbf{T}^{(n)}$)

(5·8.4f) $t_{1,1}\det(\mathbf{T}^{(n)})$
= (inductive hypothesis)
(5·8.4g) $t_{1,1}\prod_{j=2}^{n+1} t_{j,j}$
= (associativity of multiplication)
(5·8.4h) $\prod_{j=1}^{n+1} t_{j,j}.$

Hence we conclude for upper-triangular matrices, its determinant is just the product of diagonal components.

SUBCASE 2: LOWER-TRIANGULAR MATRIX. The reasoning for lower-triangular matrices is similar. Its block components would look like

$$\mathbf{T} = \begin{pmatrix} t_{1,1} & \mathbf{0}^{\mathsf{T}} \\ \boldsymbol{t} & \mathbf{T}^{(n)} \end{pmatrix} \tag{5·8.5}$$

The steps would be exactly the same, but this time because $t_{1,j} = 0$ for $j > 1$. □

5·9. Levi-Civita Symbol. It is an unfortunate fact that the definition we have given for the determinant, while useful for *performing calculations*, cannot easily be used to prove properties concerning the determinant. Consequently, we introduce an equivalent definition using a terrifying quantity known as the Levi–Civita symbol. Its terror stems from having multiple indices, but do not worry: it is used for book-keeping.

Let us define the Levi–Civita symbol for three-dimensions as $\epsilon_{i,j,k}$ such that

1. $\epsilon_{1,2,3} = +1$, and
2. swapping two adjacent indices costs us a sign: $\epsilon_{j,i,k} = -\epsilon_{i,j,k} = \epsilon_{i,k,j}$; $\epsilon_{k,i,j} = \epsilon_{i,j,k} = \epsilon j,k,i$.

As a consequence of the second property, any repeated index will correspond to a zero entry: $\epsilon_{i,i,k} = 0$, $\epsilon_{i,j,j} = 0$, and so on. The Levi–Civita symbol in n indices has analogous properties:

1. $\epsilon_{1,2,3,\dots,n-1,n} = +1$, and
2. swapping two adjacent indices costs us a sign: $\epsilon_{i_1,\dots,i_j,i_{j+1},\dots,i_n} = -\epsilon_{i_1,\dots,i_{j+1},i_j,\dots,i_n}$.

Yes, we have subscripts *on our subscripts* — we've indexed the indexing variables!

The determinant in three-dimensions for matrix $\mathbf{A} = (a_{i,j})$ is then

$$\boxed{\det(\mathbf{A}) = \sum_{i=1}^{3}\sum_{j=1}^{3}\sum_{k=1}^{3} \epsilon_{i,j,k} a_{1,i} a_{2,j} a_{3,k}.} \tag{5·9.1}$$

We can see this by performing the sums when $i = 1$, we get

$$\sum_{j=1}^{3}\sum_{k=1}^{3} \epsilon_{1,j,k} a_{1,1} a_{2,j} a_{3,k} = a_{1,1}\left(\sum_{k=1}^{3} \epsilon_{1,2,k} a_{2,2} a_{3,k} + \epsilon_{1,3,k} a_{2,3} a_{3,k}\right) \tag{5·9.2}$$

But the antisymmetry property forces us to have $k = 3$ in the first term and $k = 2$ in the second term as the only nonzero contribution in the right-hand side:

$$\sum_{j=1}^{3}\sum_{k=1}^{3} \epsilon_{1,j,k} a_{1,1} a_{2,j} a_{3,k} = a_{1,1}\left(\epsilon_{1,2,3} a_{2,2} a_{3,3} + \epsilon_{1,3,2} a_{2,3} a_{3,2}\right) \tag{5·9.3}$$

Invoking antisymmetry to rearrange indices:

$$\sum_{j=1}^{3}\sum_{k=1}^{3} \epsilon_{1,j,k} a_{1,1} a_{2,j} a_{3,k} = a_{1,1}\left(\epsilon_{1,2,3} a_{2,2} a_{3,3} - \epsilon_{1,2,3} a_{2,3} a_{3,2}\right) \tag{5·9.4}$$

then invoking the first property simplifies the right-hand side:

$$\sum_{j=1}^{3}\sum_{k=1}^{3}\epsilon_{1,j,k}a_{1,1}a_{2,j}a_{3,k} = a_{1,1}\left(a_{2,2}a_{3,3} - a_{2,3}a_{3,2}\right). \tag{5·9.5}$$

This is precisely what we had as the coefficient to $a_{1,1}$ in the familiar definition of the determinant. If we continue along, we will find our new definition coincides with our old definition.

If we had a 4×4 matrix $\mathbf{A} = (a_{i,j})$, then we would have

$$\det(\mathbf{A}) = \sum_{i=1}^{4} a_{1,i}\det(M_{1,i}) \tag{5·9.6}$$

using our familiar definition. But we can rewrite $\det(M_{1,i})$ using the Levi–Civita symbol as (remembering the minors are 3×3 matrices):

$$\det(\mathbf{A}) = \sum_{i=1}^{4}(-1)^{i+1}a_{1,i}\left(\sum_{j=1}^{3}\sum_{k=1}^{3}\sum_{\ell=1}^{3}\epsilon_{j,k,\ell}(M_{1,j})_{2,j}(M_{1,k})_{3,k}(M_{1,\ell})_{4,\ell}\right), \tag{5·9.7}$$

or by suppressing the column i explicitly and reindexing accordingly:

$$\det(\mathbf{A}) = \sum_{i=1}^{4}(-1)^{i+1}a_{1,i}\left(\sum_{\substack{j=1\\ j\neq i}}^{4}\sum_{\substack{k=1\\ k\neq i}}^{4}\sum_{\substack{\ell=1\\ \ell\neq i}}^{4}\epsilon_{j,k,\ell}a_{2,j}a_{3,k}a_{4,\ell}\right), \tag{5·9.8}$$

We observe the factor of $(-1)^{i+1}\epsilon_{j,k,\ell}$ could be replaced by $\epsilon_{i,j,k,\ell}$ (which will also enforce the conditions $i\neq j$ and $k\neq i$ and so on). Thus we find:

$$\det(\mathbf{A}) = \sum_{i=1}^{4}\epsilon_{i,j,k,\ell}a_{1,i}\sum_{j=1}^{4}\sum_{k=1}^{4}\sum_{\ell=1}^{4}a_{2,j}a_{3,k}a_{4,\ell}. \tag{5·9.9}$$

We invoke distributivity to tidy up the right-hand side as:

$$\boxed{\det(\mathbf{A}) = \sum_{i=1}^{4}\sum_{j=1}^{4}\sum_{k=1}^{4}\sum_{\ell=1}^{4}\epsilon_{i,j,k,\ell}a_{1,i}a_{2,j}a_{3,k}a_{4,\ell}.} \tag{5·9.10}$$

There seems to be a pattern emerging, when we examing the three-dimensional case in Eq (5·9.1) and compare it to the four-dimensional case: we have a Levi–Civita symbol with n indices, and n factors of $a_{1,i_1}a_{2,i_2}(\cdots)a_{n,i_n}$.

Thus we could argue, for any $n\times n$ matrix $\mathbf{A} = (a_{i,j})$, we have:

$$\boxed{\det(\mathbf{A}) = \sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_n=1}^{n}\epsilon_{i_1,i_2,\dots,i_n}a_{1,i_1}a_{2,i_2}(\cdots)a_{n,i_n}.} \tag{5·9.11}$$

We've shown this is true for $n=3$ and $n=4$, and we've shown how $n=4$ boils down to $n=3$. The general argument is similar, we would argue by induction — our base case has been established, we just need to prove the inductive case $n+1$ in terms of the "arbitrary n" inductive hypothesis. But this is precisely what we've done when moving from $n=3$ to $n=4$. The only difference will be slight, writing

$$\begin{aligned}\det\mathbf{A} &= \sum_{i_1=1}^{n+1}(-1)^{i_1+1}a_{1,i_1}\det(\mathbf{M}_{1,i_1}) \qquad (5·9.12)\\ &= \sum_{i_1=1}^{n+1}(-1)^{i_1+1}a_{1,i_1}\left(\sum_{i_2=1}^{n}(\cdots)\sum_{i_{n+1}=1}^{n}\epsilon_{i_2,\dots,i_n,i_{n+1}}(\mathbf{M}_{i_1,i_2})_{2,i_2}(\cdots)(\mathbf{M}_{i_1,i_n})_{n,i_n}(\mathbf{M}_{i_1,i_{n+1}})_{n+1,i_{n+1}}\right).\end{aligned}$$

The argument is exactly the same: rewrite the minors by components and explicitly enforce $i_j \neq i_1$ in the sums, then we would replace the $(-1)^{i_1+1}\epsilon_{i_2,\dots,i_{n+1}}$ by $\epsilon_{i_1,i_2,\dots,i_{n+1}}$, and find the $i_j \neq i_1$ conditions redundant (so we'd remove them), then invoking distributivity to obtain Eq (5·9.11). We will therefore take Eq (5·9.11) to be proven.

5·10. Lemma. *The $n \times n$ identity matrix $\mathbf{I}$ has determinant 1.*

Proof. We find

$$\det(\mathbf{I})$$

= (using Eq (5·9.11))

$$\sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} \epsilon_{i_1,\dots,i_n}\delta_{1,i_1}\dots\delta_{n,i_n} \tag{5·10.1}$$

= (summing over i_n)

$$\sum_{i_1=1}^{n} \cdots \sum_{i_{n-1}=1}^{n} \epsilon_{i_1,\dots,i_{n-1},n}\delta_{1,i_1}\dots\delta_{n-1,i_{n-1}} \tag{5·10.2}$$

= (induction)

$$\sum_{i_1=1}^{n} \epsilon_{i_1,2,\dots,n-1,n}\delta_{1,i_1} \tag{5·10.3}$$

= (defining property of the Kronecker–delta)

$$\epsilon_{1,2,\dots,n} \tag{5·10.4}$$

= (defining property of Levi–Civita)

$$+1 \tag{5·10.5}$$

Hence we conclude, for any n, the $n \times n$ identity matrix has determinant $\det(\mathbf{I}) = 1$. □

5·11. Theorem. *If $\mathbf{D}$ is a diagonal $n \times n$ matrix $\mathbf{D} = \mathrm{diag}(d_1, \dots, d_n)$, then its determinant is the product of the diagonal entries*

$$\det(\mathbf{D}) = \prod_{j=1}^{n} d_j. \tag{5·11.1}$$

This theorem is important, its proof is lengthy and involved. There are no tricks to learn from it, so its importance is just to ensure the result is true.

Proof. We find

$$\det(\mathbf{D})$$

= (Eq (5·9.11))

$$\sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} \epsilon_{i_1,\dots,i_n} d_{1,i_1}\dots d_{n,i_n} \tag{5·11.2}$$

= (since $d_{1,i} = d_1\delta_{1,i}$, etc.)

$$\sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} \epsilon_{i_1,\dots,i_n} \prod_{j=1}^{n} d_j\delta_{j,i_j} \tag{5·11.3}$$

= (defining property of Kronecker-delta applied in each summation)

$$\epsilon_{1,2,\dots,n} \prod_{j=1}^{n} d_j \tag{5·11.4}$$

$=$ (by definition of the Levi–Civita symbol)

$$(+1)\prod_{j=1}^{n} d_j. \tag{5·11.5}$$

This concludes the proof. $\square$

5·12. Theorem. *For any $n \times n$ matrices $\mathbf{A}$, $\mathbf{B}$, the determinant of their product is the product of their determinants*

$$\det(\mathbf{AB}) = \det(\mathbf{A})\det(\mathbf{B}). \tag{5·12.1}$$

Proof. Let $\mathbf{C} = (c_{i,k}) = \mathbf{AB}$, $\mathbf{A} = (a_{i,j})$ and $\mathbf{B} = (b_{i,j})$. We know from the definition of matrix multiplication

$$c_{i,k} = \sum_{j=1}^{n} a_{i,j} b_{j,k}. \tag{5·12.2}$$

We find

$\det(\mathbf{C})$

$=$ (using Eq (5·9.11))

$$\sum_{j_1=1}^{n} \cdots \sum_{j_n=1}^{n} \epsilon_{j_1,\ldots,j_n} c_{1,j_1}(\cdots) c_{n,j_n} \tag{5·12.3a}$$

$=$ (using the formula for $c_{i,k}$ from Eq (5·12.2))

$$\sum_{j_1=1}^{n} \cdots \sum_{j_n=1}^{n} \epsilon_{j_1,\ldots,j_n} \left(\sum_{k=1}^{n} a_{1,k} b_{k,j_1}\right) \left(\sum_{k=1}^{n} a_{2,k} b_{k,j_2}\right) (\cdots) \left(\sum_{k=1}^{n} a_{n,k} b_{k,j_n}\right) \tag{5·12.3b}$$

$=$ (collapsing sums)

$$\sum_{\substack{j_1=1\\ \vdots \\ j_n=1}}^{n} \epsilon_{j_1,\ldots,j_n} \left(\sum_{k=1}^{n} a_{1,k} b_{k,j_1}\right) \left(\sum_{k=1}^{n} a_{2,k} b_{k,j_2}\right) (\cdots) \left(\sum_{k=1}^{n} a_{n,k} b_{k,j_n}\right) \tag{5·12.3c}$$

$=$ (reindexing)

$$\sum_{\substack{j_1=1\\ \vdots \\ j_n=1}}^{n} \epsilon_{j_1,\ldots,j_n} \left(\sum_{i_1=1}^{n} a_{1,i_1} b_{i_1,j_1}\right) \left(\sum_{i_2=1}^{n} a_{2,i_2} b_{i_2,j_2}\right) (\cdots) \left(\sum_{i_n=1}^{n} a_{n,i_n} b_{i_n,j_n}\right) \tag{5·12.3d}$$

$=$ (distributivity)

$$\sum_{\substack{i_1=1\\ \vdots \\ i_n=1}}^{n} \sum_{\substack{j_1=1\\ \vdots \\ j_n=1}}^{n} \epsilon_{j_1,\ldots,j_n} a_{1,i_1} b_{i_1,j_1} a_{2,i_2} b_{i_2,j_2} (\cdots) a_{n,i_n} b_{i_n,j_n} \tag{5·12.3e}$$

If we start at the other end, we find

$\det(\mathbf{A})\det(\mathbf{B})$

$=$ (using Eq (5·9.11))

$$\left(\sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} \epsilon_{i_1,\ldots,i_n} a_{1,i_1}(\cdots) a_{n,i_n}\right) \left(\sum_{j_1=1}^{n} \cdots \sum_{j_n=1}^{n} \epsilon_{j_1,\ldots,j_n} b_{1,j_1}(\cdots) b_{n,j_n}\right) \tag{5·12.4a}$$

$=$ (collapsing indices into a single summation symbol)

$$\text{(5·12.4b)}\qquad \left(\sum_{\substack{i_1=1\\ \vdots\\ i_n=1}}^{n}\epsilon_{i_1,\dots,i_n}a_{1,i_1}(\cdots)a_{n,i_n}\right)\left(\sum_{\substack{j_1=1\\ \vdots\\ j_n=1}}^{n}\epsilon_{j_1,\dots,j_n}b_{1,j_1}(\cdots)b_{n,j_n}\right)$$

$=$ (using distributivity)

$$\text{(5·12.4c)}\qquad \sum_{\substack{i_1=1\\ \vdots\\ i_n=1}}^{n}\sum_{\substack{j_1=1\\ \vdots\\ j_n=1}}^{n}(\epsilon_{i_1,\dots,i_n}a_{1,i_1}(\cdots)a_{n,i_n}\epsilon_{j_1,\dots,j_n}b_{1,j_1}(\cdots)b_{n,j_n})$$

$=$ (reindexing the j indices)

$$\text{(5·12.4d)}\qquad \sum_{\substack{i_1=1\\ \vdots\\ i_n=1}}^{n}\sum_{\substack{j_{i_1}=1\\ \vdots\\ j_{i_n}=1}}^{n}(\epsilon_{i_1,\dots,i_n}a_{1,i_1}(\cdots)a_{n,i_n}\epsilon_{j_{i_1},\dots,j_{i_n}}b_{i_1,j_{i_1}}(\cdots)b_{i_n,j_{i_n}})$$

We want to show that reindexing the j_{i_k} indices as j_k will cost us a factor of the Levi–Civita symbol. Well, we would be applying a permutation π to the j indices, which *would* cost us a Levi–Civita symbol.

$$\sum_{\substack{i_1=1\\ \vdots\\ i_n=1}}^{n}\sum_{\substack{j_{i_1}=1\\ \vdots\\ j_{i_n}=1}}^{n}(\epsilon_{i_1,\dots,i_n}a_{1,i_1}(\cdots)a_{n,i_n}\epsilon_{j_{i_1},\dots,j_{i_n}}b_{i_1,j_{i_1}}(\cdots)b_{i_n,j_{i_n}})$$

$=$ (permuting j_{i_k} with j_k costs us a Levi–Civita symbol)

$$\text{(5·12.4e)}\qquad \sum_{\substack{i_1=1\\ \vdots\\ i_n=1}}^{n}\sum_{\substack{j_1=1\\ \vdots\\ j_n=1}}^{n}(\epsilon_{i_1,\dots,i_n}a_{1,i_1}(\cdots)a_{n,i_n}\epsilon_{i_1,\dots,i_n}\epsilon_{j_1,\dots,j_n}b_{i_1,j_1}(\cdots)b_{i_n,j_n})$$

$=$ (the $\epsilon_{j_1,\dots,j_n}(\epsilon_{i_1,\dots,i_n})^2$ is just $\epsilon_{j_1,\dots,j_n}$)

$$\text{(5·12.4f)}\qquad \sum_{\substack{i_1=1\\ \vdots\\ i_n=1}}^{n}\sum_{\substack{j_1=1\\ \vdots\\ j_n=1}}^{n}(a_{1,i_1}(\cdots)a_{n,i_n}\epsilon_{j_1,\dots,j_n}b_{i_1,j_1}(\cdots)b_{i_n,j_n})$$

$=$ (associativity)

$$\text{(5·12.4g)}\qquad \sum_{\substack{i_1=1\\ \vdots\\ i_n=1}}^{n}\sum_{\substack{j_1=1\\ \vdots\\ j_n=1}}^{n}\epsilon_{j_1,\dots,j_n}a_{1,i_1}(\cdots)a_{n,i_n}b_{i_1,j_1}(\cdots)b_{i_n,j_n}$$

The fact we could replace $\epsilon_{i_1,\dots,i_n}\epsilon_{i_1,\dots,i_n}\epsilon_{j_1,\dots,j_n}$ with $\epsilon_{j_1,\dots,j_n}$ stems from the fact that we require the $i_1 \neq i_2 \neq \dots \neq i_n$ to be distinct in the sum, but this is also equivalent to demanding the $j_1 \neq j_2 \neq \dots \neq j_n$ be distinct; however, the $\epsilon_{j_1,\dots,j_n}$ factor guarantees this is always the case. So the $\epsilon^2_{i_1,\dots,i_n}$ would contribute only its magnitude (i.e., a factor of +1), hence we can drop it. But we see, this is precisely what we worked out for $\det(\mathbf{AB})$. Hence the result follows. □

5·13. Lemma. *Let* $\mathbf{A} = (a_{i,j})$ *be an* $n\times n$ *matrix, let* $r\in\mathbb{R}$ *be some number, and let* $\mathbf{B} = (b_{i,j})$ *be obtained from* $\mathbf{A}$ *by adding* r *times row* μ *to row* ν $b_{i,j} = a_{i,j} + ra_{\mu,j}\delta_{i,\nu}$. *Then* $\det(\mathbf{A}) = \det(\mathbf{B})$.

Proof. We see that $\mathbf{B} = (\mathbf{I} + r\mathbf{E}_{\mu,\nu})\mathbf{A}$, where $\mathbf{E}_{\mu\nu}$ has a single nonzero entry located at row μ, column ν, which is equal to 1. Then $\det(\mathbf{B}) = \det(\mathbf{I} + r\mathbf{E}_{\mu,\nu})\det(\mathbf{A})$ since the determinant of products is the product of determinants. But $\mathbf{I} + r\mathbf{E}_{\mu,\nu}$ is either upper-triangular (when $\mu < \nu$) or lower-triangular (when $\mu > \nu$), and in both cases the determinant would be just the product of the diagonal $\det(\mathbf{I} + r\mathbf{E}_{\mu,\nu}) = \det(\mathbf{I})$ and we determined this is 1. Hence $\det(\mathbf{B}) = (1)\det(\mathbf{A})$. □

5·14. Theorem. *Let* $\mathbf{A}$ *be an* $n \times n$ *matrix such that row* i *is a multiple of row* j*. Then* $\det(\mathbf{A}) = 0$*.*

Let $\mathbf{B}$ *be an* $n \times n$ *matrix such that column* i *is a multiple of column* j*. Then* $\det(\mathbf{B}) = 0$*.*

Proof. Since we can add multiples of rows (or columns) to other rows without affecting the determinant, we see if we subtract a multiple of row i from row j in $\mathbf{A}$ we will have a row consisting of zeroes. This obviously has determinant 0 (it was the first thing we proved after the definition of determinant).

Similar reasoning holds for $\mathbf{B}$. □

5·15. Lemma. *Let* $\mathbf{S}(i,j)$ *be the* $n \times n$ *matrix obtained from the identity matrix, swapping row* i *and row* j*. Then* $\det(\mathbf{S}(i,j)) = (-1)^{i-j}$*.*

Proof. Let us prove this for the case when $j = i+1$. The general case follows by applying this particular case repeatedly. In this case, our matrix would look, in block form, like

$$\det(\mathbf{S}(i,i+1)) = \left(\begin{array}{c|cc|c} \mathbf{I} & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & \mathbf{I} \end{array}\right) \tag{5·15.1}$$

We then add row $i+1$ to row i

$$(\mathbf{I} + \mathbf{E}_{i+1,i})(\mathbf{S}(i,i+1)) = \left(\begin{array}{c|cc|c} \mathbf{I} & 0 & 0 & 0 \\ \hline 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & \mathbf{I} \end{array}\right) \tag{5·15.2}$$

Then we subtract row i from row $i+1$:

$$(\mathbf{I} - \mathbf{E}_{i,i+1})(\mathbf{I} + \mathbf{E}_{i+1,i})(\mathbf{S}(i,i+1)) = \left(\begin{array}{c|cc|c} \mathbf{I} & 0 & 0 & 0 \\ \hline 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 \\ \hline 0 & 0 & 0 & \mathbf{I} \end{array}\right) \tag{5·15.3}$$

Since this is upper-triangular,its determinant is just the product of diagonal entries:

$$\det\left((\mathbf{I} - \mathbf{E}_{i,i+1})(\mathbf{I} + \mathbf{E}_{i+1,i})(\mathbf{S}(i,i+1))\right) = -1. \tag{5·15.4}$$

However, since adding a multiple of one row to another does not affect the determinant, we find

$$\det\left((\mathbf{I} - \mathbf{E}_{i+1,i})(\mathbf{I} + \mathbf{E}_{i,i+1})\mathbf{S}(i,i+1)\right) = \det(\mathbf{S}(i,i+1)). \tag{5·15.5}$$

Hence we establish the case when $j = i+1$.

This general reasoning holds when we restore j, namely that

$$\det\left((\mathbf{I} - \mathbf{E}_{i,j})(\mathbf{I} + \mathbf{E}_{j,i})(\mathbf{S}(i,j))\right) = -1, \tag{5·15.6}$$

hence

$$\det(\mathbf{S}(i,j)) = -1. \tag{5·15.7}$$

Precisely as desired. □

5·16. Proposition. *Let* $\mathbf{A}$ *be an* $n \times n$ *matrix, let* $\mathbf{B}$ *be obtained by swapping rows* i *and* j *in* $\mathbf{A}$*. Then* $\det(\mathbf{B}) = (-1)^{i-j}\det(\mathbf{A})$*.*

Proof. We see that $\mathbf{B} = \mathbf{S}(i,j)\mathbf{A}$. Then by the determinant of products is the product of determinants, we find

$$\det(\mathbf{B}) = \det(\mathbf{S}(i,j))\det(\mathbf{A}). \tag{5·16.1}$$

We just proved $\det(\mathbf{S}(i,j)) = (-1)^{i-j}$, so substituting this in yields the result. □

5·17. Theorem. *Let* $\mathbf{A}$ *be an invertible* $n \times n$ *matrix. If* $\det(\mathbf{A}) \neq 0$*, then* $\det(\mathbf{A}^{-1}) = (\det(\mathbf{A}))^{-1}$.

Proof. We know $\mathbf{A}\mathbf{A}^{-1} = \mathbf{I}$, and then taking the determinant of both sides yields

$$\det(\mathbf{A}\mathbf{A}^{-1}) = 1. \tag{5·17.1}$$

We know the determinant of products is the product of determinants

$$\det(\mathbf{A}\mathbf{A}^{-1}) = \det(\mathbf{A})\det(\mathbf{A}^{-1}) = 1. \tag{5·17.2}$$

Dividing both sides by $\det(\mathbf{A})$ yields the result. □

5·18. Theorem. *Let* $\mathbf{A}$ *be an* $n \times n$ *matrix. The determinant is zero if and only if* $\mathbf{A}$ *is singular; equivalently, the determinant is nonzero if and only if* $\mathbf{A}$ *is invertible.*

Proof. Suppose $\mathbf{A}$ is invertible. Then $\det(\mathbf{A}\mathbf{A}^{-1}) = \det(\mathbf{I}) = 1 \neq 0$. In particular, this means $\det(\mathbf{A}) \neq 0$.

The other direction is just the contrapositive: "if p, then q" is logically equivalent to its contrapositive "if not-q, then not-p". Here q is "$\det(\mathbf{A}) \neq 0$", and p is "$\mathbf{A}$ is invertible". Hence the contrapositive is "If $\det(\mathbf{A}) = 0$, then $\mathbf{A}$ is not invertible". And that's what we wanted to prove! So, we're done. □

5·19. Theorem. *Let* $\mathbf{A}$ *be an* $n \times n$ *matrix. The determinant of the transpose is the determinant of the original matrix:*

$$\det(\mathbf{A}^{\mathsf{T}}) = \det(\mathbf{A}).$$

Proof. Either $\mathbf{A}$ is invertible or not. If not, then it is singular and has zero determinant. Its transpose will be singular, and have zero determinant. Hence the result holds for singular matrices.

For nonsingular matrices, we recall the LU-factorization $\mathbf{A} = \mathbf{L}\mathbf{U}$ where $\mathbf{U}$ has nonzero diagonal entries (because $\mathbf{A}$ is nonsingular) and $\mathbf{L}$ has 1 along its diagonal (hence $\det(\mathbf{L}) = 1$. Hence

$\det(\mathbf{A}^{\mathsf{T}})$

= (LU decomposition)

(5·19.1a) $\det((\mathbf{L}\mathbf{U})^{\mathsf{T}})$

= (transpose of products is reverse product of transposes)

(5·19.1b) $\det(\mathbf{U}^{\mathsf{T}}\mathbf{L}^{\mathsf{T}})$

= (determinant of product is product of determinants)

(5·19.1c) $\det(\mathbf{U}^{\mathsf{T}})\det(\mathbf{L}^{\mathsf{T}})$

= ($\mathbf{L}^{\mathsf{T}}$ is triangular with 1 on diagonal)

(5·19.1d) $\det(\mathbf{U}^{\mathsf{T}})1 = \det(\mathbf{U}^{\mathsf{T}})$

= ($\mathbf{U}^{\mathsf{T}}$ is triangular with the same diagonal entries as $\mathbf{U}$)

(5·19.1e) $\det(\mathbf{U})$

= ($\mathbf{L}$ is triangular with 1 on diagonal)

(5·19.1f) $1\det(\mathbf{U}) = \det(\mathbf{L})\det(\mathbf{U})$

= (product of determinants is determinant of products)

(5·19.1g) $\det(\mathbf{L}\mathbf{U})$

= (by LU decomposition of $\mathbf{A}$)

(5·19.1h) $\det(\mathbf{A})$.

Hence the result. □

5·19.1. *Remark.* This proof is important, because it shows the basic gambit in linear algebra: we take a matrix, and try factorizing it into a product of nice matrices. Then we use this factorization to prove the desired result.

Exercises

▸ **Exercise 5.1.** Let $\mathbf{M}$ be an $n \times n$ matrix. We call $\mathbf{M}$ **"Antisymmetric"** if $\mathbf{M}^{\mathsf{T}} = -\mathbf{M}$.

1. What would the diagonal values be for an antisymmetric matrix?
2. Write down a 3×3 antisymmetric matrix.
3. What would the determinant of a 3×3 antisymmetric matrix be? What about a 4×4 antisymmetric matrix?

▸ **Exercise 5.2.** Let $\mathbf{A}$ be an $n \times n$ matrix, let $c \neq 0$ be a nonzero number. Is $\det(c\mathbf{A})$ a multiple of $\det(\mathbf{A})$? If so, what is that multiple? If not, what is the determinant of a scalar matrix?

▸ **Exercise 5.3.** Prove or find a counter-example: if $\boldsymbol{a} = (a_j)$ and $\boldsymbol{b} = (b_k)$ are vectors in $\mathbb{R}^3$, then their cross product has components $\boldsymbol{a} \times \boldsymbol{b} = (\sum_j \sum_k \epsilon_{i,j,k} a_j b_k)$.

(This gives one generalization of the cross-product to other dimensions using the Levi–Civita symbol. We see the difficulty generalizing it to higher dimensions: the Levi–Civita symbol in n dimensions has n indices. In other words, for $n \geq 3$ dimensions, we need $n-1$ vectors to form a cross-product.)

▸ **Exercise 5.4.** We call an $n \times n$ matrix $\mathbf{N}$ **"Nilpotent"** if there is a positive integer m such that $\mathbf{N}^m = 0$. If $\mathbf{N}$ is nilpotent, then what is its determinant?

▸ **Exercise 5.5.** We call an $n \times n$ matrix $\mathbf{A}$ **"Idempotent"** if $\mathbf{A}^2 = \mathbf{A}$. What constraints does this impose on $\det(\mathbf{A})$?

▸ **Exercise 5.6.** Suppose $\mathbf{B}$ is an $n \times n$ matrix obtained from $\mathbf{A}$ by multiplying row i in $\mathbf{A}$ by a nonzero number γ. What is $\det(\mathbf{B})$ in terms of $\det(\mathbf{A})$ and γ?

[Hint: they are not equal to each other in general, only for $\gamma = 1$ are the determinants equal.]

▸ **Exercise 5.7.** Let D be a function which eats in an $n \times n$ matrix $\mathbf{A}$ treated as n column vectors $\mathbf{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n)$; so $D(\mathbf{A}) = D(\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n)$ such that

1. $D(\mathbf{I}) = 1$ for the identity matrix
2. it is linear in every slot: for any $\boldsymbol{u}$, $\boldsymbol{v} \in \mathbb{R}^n$, and every $a, b \in \mathbb{R}$, we have $D(\boldsymbol{a}_1, \dots, a\boldsymbol{u} + b\boldsymbol{v}, \dots, \boldsymbol{a}_n) = aD(\boldsymbol{a}_1, \dots, \boldsymbol{u}, \dots, \boldsymbol{a}_n) + bD(\boldsymbol{a}_1, \dots, \boldsymbol{v}, \dots, \boldsymbol{a}_n)$
3. it is alternating: for any $i = 1, 2, \dots, n-1$, we have $D(\boldsymbol{a}_1, \dots, \boldsymbol{a}_i, \boldsymbol{a}_{i+1}, \dots, \boldsymbol{a}_n) = -D(\boldsymbol{a}_1, \dots, \boldsymbol{a}_{i+1}, \boldsymbol{a}_i, \dots, \boldsymbol{a}_n)$.

Prove or find a counter-example: the function D is just the determinant $D(\mathbf{A}) = \det(\mathbf{A})$.

5.1 Trace of a Matrix

5·20. Proposition. *Let $\mathbf{X}$ be an $n \times n$ matrix, let $\varepsilon > 0$ be "small" (in the sense that we discard terms of order ε^2 or higher). Then*

$$\det(\mathbf{I} + \varepsilon\mathbf{X}) = 1 + \varepsilon \sum_{j=1}^{n} (\mathbf{X})_{j,j}. \tag{5·20.1}$$

Proof. This follows from the fact that $1 \gg \varepsilon^2$ and the product of off-diagonal components would contribute a ε^2 term (or some higher power of ε). So

$$\det(\mathbf{I} + \varepsilon\mathbf{X}) = \prod_{j=1}^{n} (1 + \varepsilon(\mathbf{X})_{j,j}) + \mathcal{O}(\varepsilon^2). \tag{5·20.2}$$

Expanding out the product, and keeping only the first-order ε terms gives us the result. □

5·20.1. *Remark.* From this perspective, the "linear approximation" to the determinant "near the identity matrix" is precisely the sum of diagonal entries in the "perturbation" about the identity matrix. For this reason, it deserves to be defined.

5·21. Definition. Let $\mathbf{A} = (a_{i,j})$ be an $n \times n$ matrix. We define its **"Trace"** to be the sum of its diagonal components

$$\operatorname{tr}(A) = \sum_{j=1}^{n} a_{j,j}. \tag{5·21.1}$$

5·22. Proposition. *The trace of the transpose is the trace of the original matrix,* $\operatorname{tr}(\mathbf{A}^{\mathsf{T}}) = \operatorname{tr}(\mathbf{A})$.

Proof. Let $\mathbf{B} = \mathbf{A}^{\mathsf{T}}$. Then its components would be $(\mathbf{B})_{i,j} = (\mathbf{A})_{j,i}$ and in particular the diagonal components are the same. So the sum of the diagonal components would be equal. $\square$

5·23. Proposition. *Let* $\mathbf{A}$ *be an* $n \times n$ *matrix, let* c *be some number. Then* $\operatorname{tr}(c\mathbf{A}) = c\operatorname{tr}(\mathbf{A})$.

5·24. Proposition. *Let* $\mathbf{A}$ *be an* $m \times n$ *matrix, let* $\mathbf{B}$ *be an* $n \times m$ *matrix. Then* $\operatorname{tr}(\mathbf{AB}) = \operatorname{tr}(\mathbf{BA})$.

5·25. Corollary (Cyclic property)**.** *Let* $\mathbf{A}_1, \dots, \mathbf{A}_k$ *be matrices of appropriate dimension. Then* $\operatorname{tr}(\mathbf{A}_1\mathbf{A}_2 \dots \mathbf{A}_k) = \operatorname{tr}(\mathbf{A}_2 \dots \mathbf{A}_k\mathbf{A}_1)$.

Proof. We use associativity of matrix multiplication to write

$$\operatorname{tr}(\mathbf{A}_1\mathbf{A}_2 \dots \mathbf{A}_k) = \operatorname{tr}(\mathbf{A}_1(\mathbf{A}_2 \dots \mathbf{A}_k)), \tag{5·25.1}$$

and then using the previous proposition we have

$$\operatorname{tr}(\mathbf{A}_1(\mathbf{A}_2 \dots \mathbf{A}_k)) = \operatorname{tr}((\mathbf{A}_2 \dots \mathbf{A}_k)\mathbf{A}_1). \tag{5·25.2}$$

Invoking associativity of matrix multiplication again yields the result. $\square$

5·26. Proposition. *Let* $\mathbf{A}$*,* $\mathbf{B}$ *be* $n \times n$ *matrices. Then* $\operatorname{tr}(\mathbf{A} + \mathbf{B}) = \operatorname{tr}(\mathbf{A}) + \operatorname{tr}(\mathbf{B})$.

Exercises

▸ **Exercise 5.8.** Prove or find a counter-example: if $\mathbf{A}$ is an invertible $n \times n$ matrix, $0 < \varepsilon \ll 1$ is a small real number, and $\mathbf{B}$ is an arbitrary $n \times n$ matrix, then $\det(\mathbf{A} + \varepsilon\mathbf{B}) \approx \det(\mathbf{A})(1 + \varepsilon\operatorname{tr}(\mathbf{A}^{-1}\mathbf{B}))$ (plus higher order corrections in ε).

▸ **Exercise 5.9.** If $\mathbf{A}$ is an $n \times n$ matrix such that $\mathbf{A}^{\mathsf{T}} = \mathbf{A}^{-1}$, then what values could $\det(\mathbf{A})$ be?

▸ **Exercise 5.10.** In abstract algebra, the Vandermonde determinant is useful for studying the roots of polynomials. The Vandermonde determinant in three variables is given by the determinant

$$\det\begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{pmatrix} = (a-b)(b-c)(c-a).$$

Prove this formula actually holds. [Hint: expand both sides independently, then show they are equal to each other.]

Part III
Vector Spaces

> "No money in Vectors," he blurted, "that's a whole range of luxury items right there."
>
> Thomas Pynchon, *Against the Day* (2006)

Roadmap. We could stop here and die happily (after all, we have introduced a way to solve systems of linear equations using matrices, which was our mission statement), but it would be a shallow life. Instead, we will discuss one more layer of abstraction, one more shiny gadget that will help us understand systems of linear equations more profoundly: vector spaces. We can meaningfully discuss "spaces of solutions" to a problem, and it's the laboratory of mathematics which showcases "how mathematicians do stuff".

We will also be using set theoretic notation freely and easily. The reader unfamiliar with such notation should consult Appendix A as needed.

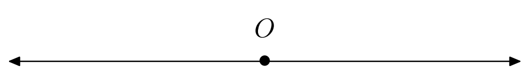
6 Vectors in $\mathbb{R}^n$

> "There are vectors," Kit replied, "and vectors. Over in Dr. Prandtl's shop, they're all straightforward lift and drift, velocity and so forth. You can draw pictures, of good old three-dimensional space if you like, or on the Complex plane, if Zhukovsky's Transformation is your glass of tea. Flights of arrows, teardrops. In Geheimrat Klein's shop, we were more used to expressing vectors without pictures, purely as an array of coefficients, no relation to anything physical, not even space itself, and writing them in any number of dimensions—according to Spectral Theory, up to infinity."
>
> Thomas Pynchon, *Against the Day* (2006)

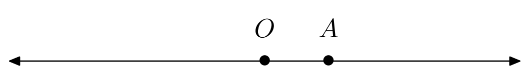
6·1. We learn about vectors at university specifically so we could do vector calculus. But we have only mentioned vectors in our notes on linear algebra in passing as a particular "species" of matrices. Is this an unfortunate collision of language? That is to say, are these two notions distinct [not secretly the same] but unfortunately use the same term?

Let us review what a "vector" was for the real plane $\mathbb{R}^2$.

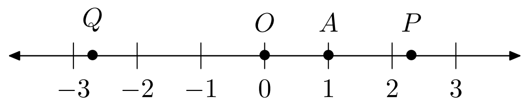
6·2. Real Number Line. Let us recall what happens in the simplest case of all: the real number line. The first thing we do is draw a line (in the Euclidean sense, which extends in both directions infinitely far) and pick some point O on the line:



We then pick a point $A \neq O$ on the line (which is not the same point as O):



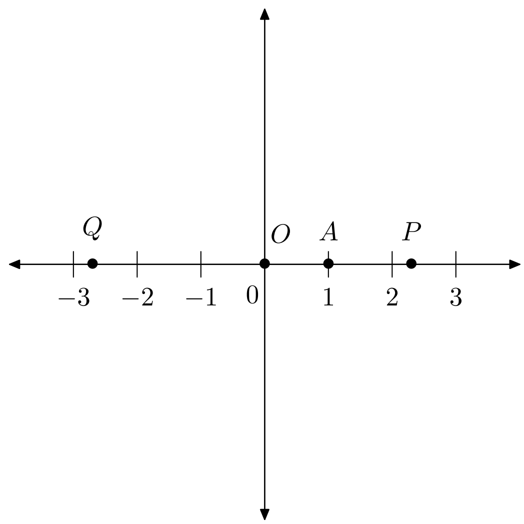
We take the distance between point O and A to be 1 unit. We then construct the rest of the "ticks" along this line, and identify every point with a number in the real numbers. Intuitively corresponding to the picture:



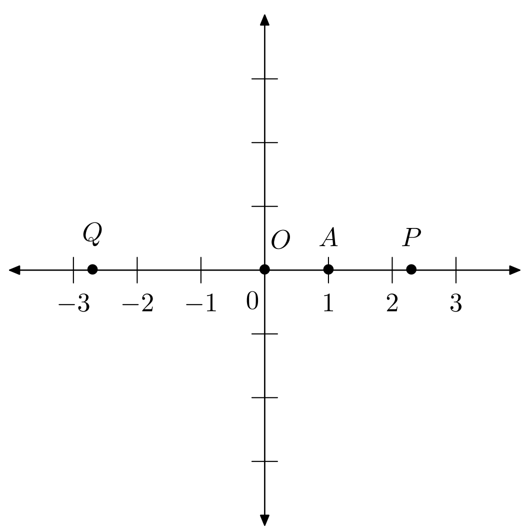
How do we make this identification? We take a point P on the line, find its distance [from O to P] as a multiple of the distance from O to A. In the case where, like point Q, it lies "in the other direction", we identify point Q with the negative real numbers by dividing the distance between O and Q with the distance between O and A (and multiplying the result by -1). This is a real number $x \in \mathbb{R}$. Conversely, if $x \in \mathbb{R}$, then we can identify with a point on the line by dilating the line segment $\overline{OA}$ by x.

When we identify point P on the line by the real number x, we call x the **"Coordinate"** of P. The point O has coordinate 0, and the distance between points P and Q (who have coordinates x_P and x_Q, respectively) by the magnitude of the difference in their coordinates $|x_Q - x_P|$.

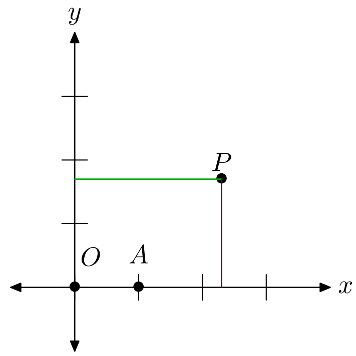
6·3. Constructing the Plane. We can construct the plane by taking a line which passes through O and forms a 90° angle with our real line. If we just "plop" down such a line, we get:



We can then form "ticks" along this new line, and call it the **"y Axis"** (our old line is the **"x Axis"**):



Instead of identifying a point in the plane with *one* real number, we now have a *pair* of real numbers. These are obtained by projecting onto the axes (the projection to the x-axis is in red, the projection to the y-axis is in green):

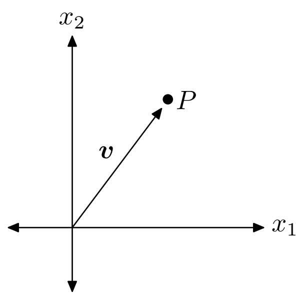


These give us points on the axes, which then give us coordinates x_P and y_P for those points on the axes. We combine these in an ordered pair (x_P, y_P) and call them the **"Coordinates"** of P. Conversely, given any pair of numbers $(x, y) \in \mathbb{R}^2$, we can construct a point in the plane by reversing the steps in this procedure.

6·4. Vectors in the Plane. Recall, we define a column 2-vector as a 2×1 matrix

$$\boldsymbol{v} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}. \tag{6·4.1}$$

We identify $\boldsymbol{p}$ with a point in the plane by constructing an oriented line segment from O (the point with coordinates $(0, 0)$ in the plane) and the point P (with coordinates (x_1, x_2)). We write this oriented line segment using the notation $\overrightarrow{OP}$. We call O the **"Base Point"** and P the **"Endpoint"** of $\overrightarrow{OP}$.



The directed line segment $\overrightarrow{OP}$ has a **"Direction"** (given by the angle formed with the positive x_1-axis) and a **"Magnitude"** (given by its length).

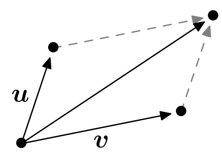
We identify any directed line segment $\overrightarrow{OP}$ with base point O with a vector $\boldsymbol{v}$ by taking the components of $\boldsymbol{v}$ to be the coordinates of P relative to base-point O.

Conversely, given any 2-vector $\boldsymbol{v} = (v_1, v_2)$, we identify it with a directed line segment [in the plane with axes and units] from O to P where P has coordinates (v_1, v_2).

Caution: In physics, we often work with vectors with base point Q and endpoint P in the plane (or in $\mathbb{R}^3$ or wherever) and quite cavalierly identify the oriented line segment $\overrightarrow{QP}$ with the line segment of equal length and direction $\overrightarrow{OP'}$ located at base-point O. This works because of the magic of $\mathbb{R}^n$ being a flat manifold. It doesn't work in general. In fact, in linear algebra, we anchor all vectors to the same base point O.

6·5. Definition. Let $\boldsymbol{v} = (v_1, v_2)$ be a vector in the plane. We define its **"Magnitude"** by the non-negative real number $\|\boldsymbol{v}\| = \sqrt{v_1^2 + v_2^2}$.

6·6. Parallelogram Law. When we have two vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ in the plane (or in space), we can form a parallelogram using vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ as edges and their shared base point as the origin. Their sum is the vector to the opposite diagonal vertex from the origin:



The reader may verify the origin plus the two vectors give us three vertices, and demanding a parallelogram gives us the remaining vertex. Further, the coordinates of the remaining vertex may be obtained by adding componentwise the coordinates of the endpoints for the vectors.

6·6.1. *Remark.* Fascinatingly, this "parallelogram law" is mistakenly attributed to Pseudo-Aristotle, but recent scholarship shows this is a misunderstanding. The first uses of the parallelogram law may be found in Fermat (of "Last Theorem" fame) and Thomas Hobbes (the pessimistic "rude, short, and brutish" philosopher). For further details, the reader is invited to enjoy David Marshall Miller's "The Parallelogram Rule from Pseudo-Aristotle to Newton" *Archive for History of Exact Sciences* **71** (2017) pp.157–191.

6·7. Scalar Multiplication. If we have a vector $\boldsymbol{v}$ corresponding to the oriented line segment $\overrightarrow{OP}$ and a real number r, we may form the scalar multiple $r\boldsymbol{v}$ by three cases:

1. Case 1 $r > 0$: we just move the endpoint along the line passing through O and P to have a magnitude r times greater than what the magnitude of $\overrightarrow{OP}$ is;
2. Case 2 $r = 0$: we have the coordinates of the resulting vector be all zeroes.
3. Case 3 $r < 0$: we find Q the point along the line passing through O and P of the same magnitude but opposite direction of $\overrightarrow{OP}$, and multiply the magnitude of the line segment from O to this new point Q by $|r| > 0$ to produce a point R and identify $\overrightarrow{OR}$ with our new vector.

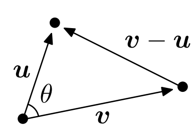
6·8. Consistency and Coherence Checks: Vector Subtraction. We now may observe, for any vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ in the plane, that $\boldsymbol{u}-\boldsymbol{v}$ corresponds to the vector sum of $\boldsymbol{u}$ with the scalar multiple $-1\boldsymbol{v}$. Similarly, repeatedly adding a vector $\boldsymbol{u}$ to itself $n \in \mathbb{N}$ times gives us the scalar multiple $n\boldsymbol{u}$.

In other words, scalar multiplication produces results which make sense in light of vector addition *via* the parallelogram law.

6·9. Angles Between Vectors. We can recall the law of cosines from trigonometry:

$$\|\boldsymbol{u}-\boldsymbol{v}\|^2 = \|\boldsymbol{u}\|^2 + \|\boldsymbol{v}\|^2 - 2\|\boldsymbol{u}\|\|\boldsymbol{v}\|\cos(\theta) \tag{6·9.1}$$

where θ is the angle formed between the edges of the vector. We refresh our memory of the location of the variables with the sketch:



Now, we can compute using coordinates

$$\|\boldsymbol{u}-\boldsymbol{v}\|^2$$

$=$ (by definition of the magnitude of a vector)

(6·9.2a) $\quad (u_1 - v_1)^2 + (u_2 - v_2)^2$

$=$ (expanding the terms)

(6·9.2b) $\quad (u_1^2 - 2u_1v_1 + v_1^2) + (u_2^2 - 2u_2v_2 + v_2^2)$

$=$ (associativity of addition)

(6·9.2c) $\quad (u_1^2 + u_2^2) + (v_1^2 + v_2^2) - 2u_1v_1 - 2u_2v_2$

$=$ (distributivity)

$$(6{\cdot}9.2\text{d}) \qquad (u_1^2 + u_2^2) + (v_1^2 + v_2^2) - 2(u_1v_1 + u_2v_2).$$

We see this is just $\|\boldsymbol{u}\|^2 + \|\boldsymbol{v}\|^2 - 2(\text{stuff})$. But we know what the "(stuff)" is, by the law of cosines,

$$-2(u_1v_1 + u_2v_2) = -2\|\boldsymbol{u}\|\|\boldsymbol{v}\|\cos(\theta), \tag{6·9.3}$$

hence *for nonzero vectors* we find,

$$\frac{(u_1v_1 + u_2v_2)}{\|\boldsymbol{u}\|\|\boldsymbol{v}\|} = \cos(\theta). \tag{6·9.4}$$

But what's more, we see the numerator of the right-hand side is just the dot product of vectors $\boldsymbol{u}\cdot\boldsymbol{v}$. We conclude

$$\frac{\boldsymbol{u}\cdot\boldsymbol{v}}{\|\boldsymbol{u}\|\|\boldsymbol{v}\|} = \cos(\theta). \tag{6·9.5}$$

We see this formula is symmetric if we switched places of $\boldsymbol{u}$ and $\boldsymbol{v}$, in the sense we get exactly the same result.

But further, we can now *define* the angle θ between *any* two *nonzero*(!!) vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ by the relation:

$$\boxed{\cos(\theta) := \frac{\boldsymbol{u}\cdot\boldsymbol{v}}{\|\boldsymbol{u}\|\|\boldsymbol{v}\|}.} \tag{6·9.6}$$

We stress these must be nonzero vectors (otherwise we divide by zero and horrible results follow).

6·10. Definition. If two nonzero vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ are such that

$$\boldsymbol{u}\cdot\boldsymbol{v} = 0, \tag{6·10.1}$$

then we call them **"Orthogonal"** (usually we say one is orthogonal to the other).

6·11. Unit Vectors and Directions. If we wish to make a statement about "directions", then we can make it precise by using **"Unit Vectors"** — vectors of "unit magnitude" (i.e., length one). We follow tradition and use hats to indicate we have a unit vector. For any nonzero vector $\boldsymbol{u}$ of arbitrary length, we can **"Normalize"** it to produce the unit vector

$$\widehat{\boldsymbol{u}} = \frac{\boldsymbol{u}}{\|\boldsymbol{u}\|}. \tag{6·11.1}$$

We see then that the angle between vectors may be found using their unit vectors's dot product, without worrying about dividing by anything:

$$\widehat{\boldsymbol{u}}\cdot\widehat{\boldsymbol{v}} = \cos(\theta). \tag{6·11.2}$$

6·12. Generalization to $n > 2$. Everything we have discussed so far has been restricted to the real plane $\mathbb{R}^2$. But we could generalize it to $\mathbb{R}^n$ for $n \in \mathbb{N}$ arbitrary [but fixed]. Vectors then have n components, but all our definitions generalize accordingly. Vector addition is given by adding components, scalar multiplication is given by multiplying each component by the given scalar, and so on.

7 Vector Spaces over $\mathbb{R}$

'Vector space'? Unreal, but not compellingly so...

Thomas Pynchon, *Against the Day* (2006)

7·1. We have seen how real 2-dimensional vector spaces were a bunch of arrows sharing the same base-point, with their own form of addition (via the parallelogram law) and scalar multiplication. We also saw how to encode these arrows as 2-tuples of real numbers called coordinates relative to some axes. We can do this in any $n \in \mathbb{N}$ dimensions, "drawing" n-dimensional arrows sharing the same base-point, using the parallelogram law for addition, dilation of arrow length for scalar multiplication, and encoding these arrows as n-tuples of coordinates. This "coordinitization" of vector spaces will be generalized in Section 9.

Now we will create an abstraction that captures the crucial aspects of that family of examples, the "family of arrows sharing a base-point with their own addition operation and scalar multiplication"-notion. In math, we do this by defining new "gadgets", equipping them with "structure" [functions of some sort], such that a bunch of "properties" [equations] hold.

7·2. Definition. A **"Real Vector Space"** consists of a set V equipped with two operations $\odot\colon \mathbb{R}\times V \to V$ and $\oplus\colon V \times V \to V$ such that

(1) Closure of $\oplus$: If $\boldsymbol{u}$, $\boldsymbol{v} \in V$ are two arbitrary elements of V, then $\boldsymbol{u}\oplus\boldsymbol{v} \in V$; in other words, V is closed under the $\oplus$ operation.
(2) Commutativity of $\oplus$: for any $\boldsymbol{u}$, $\boldsymbol{v} \in V$, we have $\boldsymbol{u}\oplus\boldsymbol{v} = \boldsymbol{v}\oplus\boldsymbol{u}$
(3) Associativity of $\oplus$: for any $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w} \in V$, we have $\boldsymbol{u}\oplus(\boldsymbol{v}\oplus\boldsymbol{w}) = (\boldsymbol{u}\oplus\boldsymbol{v})\oplus\boldsymbol{w}$
(4) Unit of $\oplus$: there exists an element $\mathbf{0} \in V$ such that for every $\boldsymbol{u} \in V$, $\mathbf{0}\oplus\boldsymbol{u} = \boldsymbol{u}\oplus\mathbf{0} = \boldsymbol{u}$.
(5) Existence of negation: for each $\boldsymbol{u} \in V$, there exists a $-\boldsymbol{u} \in V$ such that $\boldsymbol{u}\oplus -\boldsymbol{u} = -\boldsymbol{u}\oplus\boldsymbol{u} = \mathbf{0}$
(6) Closure of $\odot$: for any real number $c \in \mathbb{R}$ and element $\boldsymbol{u} \in V$, we have $c\odot\boldsymbol{v} \in V$.
(7) Left distributivity of $\odot$ over $\oplus$: for any $c \in \mathbb{R}$ and $\boldsymbol{u}$, $\boldsymbol{v} \in V$, we have $c\odot(\boldsymbol{u}\oplus\boldsymbol{v}) = (c\odot\boldsymbol{u})\oplus(c\odot\boldsymbol{v})$.
(8) Right distributivity of $\oplus$ over $\odot$: for any c, $d \in \mathbb{R}$ and $\boldsymbol{u} \in V$, we have $(c+d)\odot\boldsymbol{u} = (c\odot\boldsymbol{u})\oplus(d\odot\boldsymbol{u})$.
(9) Unit of $\odot$: for any $\boldsymbol{u} \in V$, $1\odot\boldsymbol{u} = \boldsymbol{u}$.

We call elements of V **"Vectors"**, we call the operators $\oplus$ **"Vector Addition"** and $\odot$ **"Scalar Multiplication"**. The vector $\mathbf{0}$ in condition (4) is called the **"Zero Vector"** of V.

7·2.1. *Remark.* We will use the $\oplus$ and $\odot$ notation briefly, just to explicitly distinguish vector addition from addition of numbers, and to distinguish scalar multiplication from multiplication of numbers.

7·2.2. *Remark.* We could replace all instances of $\mathbb{R}$ by $\mathbb{C}$, any real number by complex number, and we would obtain the definition of a **"Complex Vector Space"**. This suggests the notion of a "real vector space" could be generalized *even further* to a "vector space over [a suitably nice number system]".

7·3. Example. When $V = \mathbb{R}^n$, and $\oplus$ is defined componentwise, and $\odot$ is defined as multiplying each component by the given real number, then we see we have formed a real vector space. This is an important example, even if it seems trivial. Why? Because our definition is a *generalization* of this; if $\mathbb{R}^n$ were not an example of a real vector space, then our definition would *fail as a generalization.*

7·4. Example. Let $\mathrm{Mat}(\mathbb{R};m,n)$ be the set of all $m\times n$ matrices with real components. Then it forms a real vector space with $\oplus$ being addition of matrices, and $\odot$ being multiplying each component by a scalar. It is not enough to *assert* this forms a vector space: we must *prove* it satisfies *every condition* in the definition.

(1) Closure of $\oplus$: for any $\mathbf{A},\mathbf{B} \in \mathrm{Mat}(\mathbb{R};m,n)$, we have $(\mathbf{A}\oplus\mathbf{B}) \in \mathrm{Mat}(\mathbb{R};m,n)$.
PROOF: Let $\mathbf{A} = (a_{i,j}) \in \mathrm{Mat}(\mathbb{R};m,n)$ and $\mathbf{B} = (b_{i,j}) \in \mathrm{Mat}(\mathbb{R};m,n)$ be elements of $\mathrm{Mat}(\mathbb{R};m,n)$. We see $\mathbf{A}\oplus\mathbf{B} = (a_{i,j}+b_{i,j})$ which is an $m\times n$ real matrix. Thus $\mathbf{A}\oplus\mathbf{B} \in \mathrm{Mat}(\mathbb{R};m,n)$, and since this was for *arbitrary* $\mathbf{A}$ and $\mathbf{B}$, we have established closure.
(2) Commutativity of $\oplus$: for any $\mathbf{A},\mathbf{B} \in \mathrm{Mat}(\mathbb{R};m,n)$, we have $\mathbf{A}\oplus\mathbf{B} = \mathbf{B}\oplus\mathbf{A}$.
PROOF: Let $\mathbf{A} = (a_{i,j}) \in \mathrm{Mat}(\mathbb{R};m,n)$ and $\mathbf{B} = (b_{i,j}) \in \mathrm{Mat}(\mathbb{R};m,n)$ be elements of $\mathrm{Mat}(\mathbb{R};m,n)$. We want to prove $\mathbf{A}\oplus\mathbf{B} = \mathbf{B}\oplus\mathbf{A}$. But we see $(\mathbf{A}\oplus\mathbf{B})_{i,j} = a_{i,j}+b_{i,j} = b_{i,j}+a_{i,j}$ by the commutativity

of addition for real numbers, and this is precisely $b_{i,j} + a_{i,j} = (\mathbf{B} \oplus \mathbf{A})_{i,j}$. Since this is true for *every* component of $\mathbf{A}$ and $\mathbf{B}$, then it follows $\mathbf{A} \oplus \mathbf{B} = \mathbf{B} \oplus \mathbf{A}$. And since this is true for *arbitrary* $\mathbf{A}$ and $\mathbf{B}$, then it follows that $\oplus$ is commutative.

(3) Associativity of $\oplus$: for any $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathrm{Mat}(\mathbb{R}; m, n)$, we have $\mathbf{A} \oplus (\mathbf{B} \oplus \mathbf{C}) = (\mathbf{A} \oplus \mathbf{B}) \oplus \mathbf{C}$.
PROOF: Let $\mathbf{A} = (a_{i,j}) \in \mathrm{Mat}(\mathbb{R}; m, n)$, $\mathbf{B} = (b_{i,j}) \in \mathrm{Mat}(\mathbb{R}; m, n)$, and $\mathbf{C} = (c_{i,j}) \in \mathrm{Mat}(\mathbb{R}; m, n)$ be elements of $\mathrm{Mat}(\mathbb{R}; m, n)$. We see every component of the sum $(\mathbf{A} \oplus (\mathbf{B} \oplus \mathbf{C}))_{i,j} = a_{i,j} + (b_{i,j} + c_{i,j}) = (a_{i,j} + b_{i,j}) + c_{i,j}$ by associativity of addition over the real numbers, and this equals $(a_{i,j} + b_{i,j}) + c_{i,j} = ((\mathbf{A} \oplus \mathbf{B}) \oplus \mathbf{C})_{i,j}$. Since this holds for every component of the matrices, it follows that $\mathbf{A} \oplus (\mathbf{B} \oplus \mathbf{C}) = (\mathbf{A} \oplus \mathbf{B}) \oplus \mathbf{C}$. Since this is true for arbitrary matrices $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ in V, then the condition "$\oplus$ is assocative" is satisfied.

(4) Unit of $\oplus$: there exists an element $\mathbf{0} \in \mathrm{Mat}(\mathbb{R}; m, n)$ such that for every $\mathbf{A} \in \mathrm{Mat}(\mathbb{R}; m, n)$, $\mathbf{0} \oplus \mathbf{A} = \mathbf{A} \oplus \mathbf{0} = \mathbf{A}$.
PROOF: It suffices to prove $\mathbf{0} \oplus \mathbf{A} = \mathbf{A}$, because commutativity guarantees $\mathbf{A} \oplus \mathbf{0} = \mathbf{0} \oplus \mathbf{A}$. We see $(\mathbf{O} \oplus \mathbf{A})_{i,j} = 0 + (\mathbf{A})_{i,j} = (\mathbf{A})_{i,j}$. Since this is true for every component i and j, we conclude $\mathbf{0} \oplus \mathbf{A} = \mathbf{A}$. Since this is true for arbitrary $\mathbf{A} \in \mathrm{Mat}(\mathbb{R}; m, n)$, then it follows that the zero matrix $\mathbf{0}$ is the "vector" which satisfies the desired condition.

(5) Existence of negation: for every $\mathbf{A} \in \mathrm{Mat}(\mathbb{R}; m, n)$, there exists a $-\mathbf{A} \in \mathrm{Mat}(\mathbb{R}; m, n)$ such that $\mathbf{A} \oplus -\mathbf{A} = \mathbf{0}$.
PROOF: We multiply out the components $(-\mathbf{A})_{i,j} = -(\mathbf{A})_{i,j}$ hence $(\mathbf{A} \oplus -\mathbf{A})_{i,j} = (\mathbf{A})_{i,j} + (-(\mathbf{A})_{i,j}) = 0$ for each component i and j. Thus we conclude $\mathbf{A} \oplus -\mathbf{A} = \mathbf{0}$ and by commutativity $-\mathbf{A} \oplus \mathbf{A} = \mathbf{0}$. Since this is true for arbitrary element $\mathbf{A} \in \mathrm{Mat}(\mathbb{R}; m, n)$, the condition is satisfied.

(6) Closure of $\odot$: for any real number $c \in \mathbb{R}$ and element $\mathbf{A} \in \mathrm{Mat}(\mathbb{R}; m, n)$, we have $c \odot \mathbf{A} \in \mathrm{Mat}(\mathbb{R}; m, n)$.
PROOF: Multiplying the components of a $m \times n$ matrix by a real number produces a new matrix with components $(c \odot \mathbf{A})_{i,j} = c(\mathbf{A})_{i,j}$ which is what we wanted to prove.

(7) Left distributivity of $\odot$ over $\oplus$: for any $c \in \mathbb{R}$ and $\mathbf{A}$, $\mathbf{B} \in \mathrm{Mat}(\mathbb{R}; m, n)$, we have $c \odot (\mathbf{A} \oplus \mathbf{B}) = (c \odot \mathbf{A}) \oplus (c \odot \mathbf{B})$.
PROOF: We see the components of the left-hand side are $(c \odot (\mathbf{A} \oplus \mathbf{B}))_{i,j} = c((\mathbf{A})_{i,j} + (\mathbf{B})_{i,j}) = c(\mathbf{A})_{i,j} + c(\mathbf{B})_{i,j}$ by distributivity of multiplying real numbers over adding real numbers, and we see this is just the components of $((c \odot \mathbf{A}) \oplus (c \odot \mathbf{B}))_{i,j}$. That is to say, every component of the matrices satisfy $(c \odot (\mathbf{A} \oplus \mathbf{B}))_{i,j} = ((c \odot \mathbf{A}) \oplus (c \odot \mathbf{B}))_{i,j}$, hence by the definition of matrix equality $c \odot (\mathbf{A} \oplus \mathbf{B}) = (c \odot \mathbf{A}) \oplus (c \odot \mathbf{B})$. Thus the condition is satisfied.

(8) Right distributivity of $\oplus$ over $\odot$: for any c, $d \in \mathbb{R}$ and $\mathbf{A} \in \mathrm{Mat}(\mathbb{R}; m, n)$, we have $(c + d) \odot \mathbf{A} = (c \odot \mathbf{A}) \oplus (d \odot \mathbf{A})$.
PROOF: We see every component of the left-hand side satisfies $((c + d) \odot \mathbf{A})_{i,j} = (c + d)(\mathbf{A})_{i,j} = c(\mathbf{A})_{i,j} + d(\mathbf{A})_{i,j}$. But this is precisely the component $((c \odot \mathbf{A}) \oplus (c \odot \mathbf{B}))_{i,j}$ of the right hand side. Thus $((c + d) \odot \mathbf{A})_{i,j} = ((c \odot \mathbf{A}) \oplus (c \odot \mathbf{B}))_{i,j}$ holds for every component, and so by the definition of matrix equality we have $(c + d) \odot \mathbf{A} = (c \odot \mathbf{A}) \oplus (d \odot \mathbf{A})$. Thus the condition is satisfied.

(9) Unit of $\odot$: for any $\mathbf{A} \in \mathrm{Mat}(\mathbb{R}; m, n)$, we have $1 \odot \mathbf{A} = \mathbf{A}$.
PROOF: We find the components of the left-hand side are $(1 \odot \mathbf{A})_{i,j} = 1(\mathbf{A})_{i,j} = (\mathbf{A})_{i,j}$ equal to the corresponding components of the right-hand side, for every component. Hence by the definition of matrix equality we have $1 \odot \mathbf{A} = \mathbf{A}$. Since this is for arbitrary $\mathbf{A}$, the condition is satisfied.

We have proven $\mathrm{Mat}(\mathbb{R}; m, n)$ satisfies the conditions specified in our definition for a real vector space, and thus find it *is* a real vector space.

7·5. Puzzle. Consider the solutions to the linear equation in n unknowns

$$V = \{(x_1, \dots, x_n) \in \mathbb{R} \mid a_1 x_1 + \cdots + a_n x_n = b\} \tag{7·5.1}$$

where a_1, $\dots$, a_n, $b \in \mathbb{R}$ are fixed constants. Does V form a vector space under the usual vector addition and scalar multiplication borrowed from $\mathbb{R}^n$?

7·6. NOTATION CHANGE:. We will cease using $\oplus$ and $\odot$ consistently for vector addition and scalar multiplication. Instead, we will use the symbol $+$ for vector addition, and $\cdot$ (if anything) for scalar multiplication.

Exercises

▸ **Exercise 7.1.** Let A be any non-empty set (say, the set of letters in the alphabet, or whatever). Consider the collection of real-valued functions $V = \{f \colon A \to \mathbb{R}\}$. Define $\oplus$ and $\odot$ on V by:

1. for any f, $g \in V$, for any $a \in A$, $(f \oplus g)(a) = f(a) + g(a)$, where the $\oplus$ is defined for functions and $+$ is the addition of real numbers, and
2. for any $f \in V$ and $c \in \mathbb{R}$ and $a \in A$, $(c \odot f)(a) = cf(a)$.

Prove or find a counter-example: V is a real vector space.

[Hint: different choices of A will not provide counter-examples, but the condition that A is nonempty is non-negotiable.]

▸ **Exercise 7.2.** Recall a **"Polynomial"** with real coefficients looks like

$$p(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_n x^n \tag{7·6.1}$$

where $n \in \mathbb{N}$ is called the **"Degree"** of p. (We write $\deg(p)$ if we wanted to refer to the degree of p.) The set of *all* polynomials with real coefficients in the same unknown x (of all degrees) is denoted

$$\mathbb{R}[x] = \{p_0 + p_1 x + p_2 x^2 + \cdots + p_n x^n \mid n \in \mathbb{N}, p_j \in \mathbb{R}, j = 1, \ldots, j\}. \tag{7·6.2}$$

Prove or find a counter-example: the set of polynomials with real coefficients $\mathbb{R}[x]$ is a real vector space. Vector addition and scalar multiplication both are done componentwise.

8 Subspaces

8·1. Puzzle 7·5 (which readers who remember multivariate calculus recall defines a hypersurface) motivates the following definition:

8·2. Definition. Let V be a real vector space with vector addition $\oplus$ and scalar multiplication $\odot$. Let $U \subseteq V$ be some subset. We call U a **"Subspace"** of V if it forms a real vector space using the vector addition $\oplus$ from V and the scalar multiplication $\odot$ from V.

8·2.1. *Remark.* Several things to note about this definition:

1. The zero vector of U must be the zero vector of V.
2. The binary operators on U must be those of V restricted to U. We cannot change them.

8·2.2. *Remark.* This is a clunky definition. No one wants to prove U satisfies 9 conditions when we know V satisfies them. One of our first goals is to simplify the criteria for determining if U is a subspace of V or not.

8·3. Theorem. *Let V be a real vector space with vector addition $\oplus$ and scalar multiplication $\odot$. Then the subset $U \subseteq V$ forms a subspace of V provided:*

1. *for any $\boldsymbol{u}$, $\boldsymbol{v} \in U$, we have $\boldsymbol{u} \oplus \boldsymbol{v} \in U$; and*
2. *for any $c \in \mathbb{R}$ and $\boldsymbol{u} \in U$, we have $c \odot \boldsymbol{u} \in U$.*

In other words, if U is closed under the vector addition $\oplus$ and scalar multiplication $\odot$ from V, then U is a subspace of V.

Proof. Assume $U \subseteq V$ satisfies the two conditions

(a) for any $\boldsymbol{u}$, $\boldsymbol{v} \in U$, we have $\boldsymbol{u} \oplus \boldsymbol{v} \in U$; and
(b) for any $c \in \mathbb{R}$ and $\boldsymbol{u} \in U$, we have $c \odot \boldsymbol{u} \in U$.

We want to prove the following:

(1) Closure of $\oplus$: If $\boldsymbol{u}$, $\boldsymbol{v} \in U$ are two arbitrary elements of U, then $\boldsymbol{u} \oplus \boldsymbol{v} \in U$; in other words, U is closed under the $\oplus$ operation.
Proof: this is precisely assumption (a).

(2) Commutativity of $\oplus$: for any $\boldsymbol{u}$, $\boldsymbol{v} \in U$, we have $\boldsymbol{u} \oplus \boldsymbol{v} = \boldsymbol{v} \oplus \boldsymbol{u}$.
PROOF: any elements of U are elements of V, so reconsider $\boldsymbol{u}$ and $\boldsymbol{v}$ as elements of V. Then the condition holds (since V is a real vector space).
(3) Associativity of $\oplus$: for any $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w} \in U$, we have $\boldsymbol{u} \oplus (\boldsymbol{v} \oplus \boldsymbol{w}) = (\boldsymbol{u} \oplus \boldsymbol{v}) \oplus \boldsymbol{w}$.
PROOF: any elements of U are elements of V, so reconsider $\boldsymbol{u}$, $\boldsymbol{v}$, and $\boldsymbol{w}$ as elements of V. Then the condition holds (since V is a real vector space).
(4) Unit of $\oplus$: there exists an element $\mathbf{0} \in U$ such that for every $\boldsymbol{u} \in U$, $\mathbf{0} \oplus \boldsymbol{u} = \boldsymbol{u} \oplus \mathbf{0} = \boldsymbol{u}$.
PROOF: since U is closed under scalar multiplication by assumption (b), we know $0 \odot \boldsymbol{u} = \mathbf{0}$ which must be in U.
(5) Existence of negation: for each $\boldsymbol{u} \in U$, there exists a $-\boldsymbol{u} \in U$ such that $\boldsymbol{u} \oplus -\boldsymbol{u} = -\boldsymbol{u} \oplus \boldsymbol{u} = \mathbf{0}$
PROOF: since U is closed under scalar multiplication by assumption (b), we identify $-\boldsymbol{u} = -1 \odot \boldsymbol{u}$ which would be in U and satisfies the desired properties.
(6) Closure of $\odot$: for any real number $c \in \mathbb{R}$ and element $\boldsymbol{u} \in U$, we have $c \odot \boldsymbol{v} \in U$.
PROOF: This is assumption (b).
(7) Left distributivity of $\odot$ over $\oplus$: for any $c \in \mathbb{R}$ and $\boldsymbol{u}$, $\boldsymbol{v} \in U$, we have $c \odot (\boldsymbol{u} \oplus \boldsymbol{v}) = (c \odot \boldsymbol{u}) \oplus (c \odot \boldsymbol{v})$.
PROOF: any elements of U are elements of V, so reconsider $\boldsymbol{u}$ and $\boldsymbol{v}$ as elements of V. Then the condition holds (since V is a real vector space).
(8) Right distributivity of $\oplus$ over $\odot$: for any c, $d \in \mathbb{R}$ and $\boldsymbol{u} \in U$, we have $(c+d) \odot \boldsymbol{u} = (c \odot \boldsymbol{u}) \oplus (d \odot \boldsymbol{u})$.
PROOF: any elements of U are elements of V, so reconsider $\boldsymbol{u}$ as elements of V. Then the condition holds (since V is a real vector space).
(9) Unit of $\odot$: for any $\boldsymbol{u} \in U$, $1 \odot \boldsymbol{u} = \boldsymbol{u}$.
PROOF: any elements of U are elements of V, so reconsider $\boldsymbol{u}$ as elements of V. Then the condition holds (since V is a real vector space).

Hence U satisfies the conditions to be a real vector space when equipped with $\oplus$ and $\odot$ from V. □

8·4. Example. Let V be any real vector space. We can define the **"Trivial Subspace"** of V to be the set $0 = \{\mathbf{0} \in V\}$ consisting of just the zero vector. This is closed under addition $\mathbf{0} \oplus \mathbf{0} = \mathbf{0}$ and under scalar multiplication $\forall c \in \mathbb{R}, c \odot \mathbf{0} = \mathbf{0}$. Hence 0 is a subspace of V.

8·5. Corollary (Subspace iff closed under arbitrary linear combinations)**.** *Let V be a real vector space and $U \subseteq V$. Then U is a subspace of V if and only if for every $u_1, u_2 \in U$ and $c_1, c_2 \in \mathbb{R}$ we have $(c_1 \odot u_1) \oplus (c_2 \odot u_2) \in U$.*

Proof. ($\Longrightarrow$) Assume U is a subspace of V. Then for any $\boldsymbol{u}_1, \boldsymbol{u}_2 \in U$ and $c_1, c_2 \in \mathbb{R}$ we see $c_1 \odot \boldsymbol{u}_1$ and $c_2 \odot \boldsymbol{u}_2$ are both in U and therefore their vector sum is in U as well, i.e., $(c_1 \odot \boldsymbol{u}_1) \oplus (c_2 \odot \boldsymbol{u}_2) \in U$.

($\Longleftarrow$) Assume for every $\boldsymbol{u}_1, \boldsymbol{u}_2 \in U$ and $c_1, c_2 \in \mathbb{R}$ we have $(c_1 \odot \boldsymbol{u}_1) \oplus (c_2 \odot \boldsymbol{u}_2) \in U$. Then we see when $c_1 = 1$ and $c_2 = 1$ we have our assumption become:
(a) for every $\boldsymbol{u}_1, \boldsymbol{u}_2 \in U$ their vector sum $\boldsymbol{u}_1 \oplus \boldsymbol{u}_2 \in U$.
When $c_2 = 0$ (and/or $\boldsymbol{u}_2 = \mathbf{0}$), our assumption becomes:
(b) For every $c_1 \in \mathbb{R}$ and $\boldsymbol{u}_1 \in U$, $c_1 \odot \boldsymbol{u}_1 \in U$.
These are precisely stating U is closed under $\oplus$ and $\odot$, which implies U is a subspace of V. □

8·5.1. *Remark.* The notion of "arbitrary linear combinations [of elements of a subset of a vector space]" turns out to be the critical key idea here. We want to give it a name, because we will use it quite a bit.

8·6. Definition. Let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V$ be vectors. We call $\boldsymbol{u} \in V$ a **"Linear Combination"** of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ if there exists $c_1, \ldots, c_k \in \mathbb{R}$ such that

$$\boldsymbol{u} = c_1\boldsymbol{v}_1 + \cdots + c_k\boldsymbol{v}_k. \tag{8·6.1}$$

8·7. Definition. Let V be a real vector space, let $S \subseteq V$ be a (possibly infinite) set of a vectors. Then the **"Span"** of S is the set of *finite* linear combinations of elements of S:

$$\operatorname{span}(S) = \{\sum_{j=1}^{k} \lambda_j \boldsymbol{v}_j \mid \lambda_j \in \mathbb{R}, \boldsymbol{v}_j \in S, k \in \mathbb{N}, j = 1, \ldots, k\} \tag{8·7.1}$$

If $W \subseteq V$ is a subspace of V such that $\text{span}(S) = W$, then we call S a **"Spanning Set"** of W.

8·7.1. *Remark.* Did I mention that only finite linear combinations of elements of S are allowed in the $\text{span}(S)$? Because that "finite" part is critical.

8·8. Proposition (Spans are subspaces)**.** *Let V be a real vector space, $S \subseteq V$ a nonempty subset. Then* $\text{span}(S)$ *is a subspace of V.*

Proof. This follows from Corollary 8·5. The sum of two linear combinations is another linear combination. □

8·9. Puzzle: "Best" Spanning Sets? If we have a vector space V, is there a "best" spanning set $S \subseteq V$ (such that $\text{span}(S) = V$)? We may have "redundancies", for example if $s_1 \in S$ and $s_2 \in S$, then we don't really need $s_1 + s_2 \in S$. So it seems "minimal" is a good measure of "best-ness". Is there a "minimal" spanning set (in some appropriate sense)?

Exercises

▸ **Exercise 8.1.** Consider the set of polynomials with real coefficients of degree less than or equal to 2, $V = \{p \in \mathbb{R}[x] \mid \deg(p) \leq 2\}$ forms a real vector space where $(p_0 + p_1x + p_2x^2) \oplus (q_0 + q_1x + q_2x^2) = (p_0 + q_0) + (p_1 + q_1)x + (p_2 + q_2)x^2$ and $c \odot (p_0 + p_1x + p_2x^2) = (cp_0) + (cp_1)x + (cp_2)x^2$ for arbitrary $c \in \mathbb{R}$, $(p_0 + p_1x + p_2x^2)$, $(q_0 + q_1x + q_2x^2) \in V$. Is V a subspace of the set of all polynomials with real coefficients $\mathbb{R}[x]$? We know it's a subset, but is it a sub*space*?

▸ **Exercise 8.2.** Let W be a real vector space.

Prove or find a counter-example: If U is a subspace of V and V is a subspace of W, then is U a subspace of W?

▸ **Exercise 8.3.** Consider the set $C^{\infty}(\mathbb{R})$ of smooth real functions. Is this a subspace of $C(\mathbb{R})$ all continuous functions from the reals to the real numbers? Is it a subspace of $\{f\colon \mathbb{R} \to \mathbb{R}\}$ all functions (all of them — continuous, discontinuous, nowhere continuous — it doesn't matter, all of them)?

▸ **Exercise 8.4.** Consider the set of Riemann integrable functions on some interval $[a, b] \subseteq \mathbb{R}$. Prove or find a counter-example: this a subspace of all functions $\{f\colon [a, b] \to \mathbb{R}\}$?

[Hint: can you construct a sequence of integrable functions which converges to a nonintegrable function?]

▸ **Exercise 8.5.** Consider the subset $S = \{1, x, 1 - x^2\} \subseteq \mathbb{R}[x]$. Compute $\text{span}(S)$.

▸ **Exercise 8.6.** Prove or find a counter-example: if V is a vector space, then V is a subspace of itself.

8.1 Orthogonal Complements and Direct Sums

8·10. We have ways to "subtract" one subspace from another and, dually, combine two "disjoint" subspaces together.

8·11. Definition. Let $U \subseteq V$ be a subspace. We define its **"Orthogonal Complement"** of U to be the set (not subspace, but a set) of vectors

$$U^{\perp} = \{\boldsymbol{w} \in V \mid \text{for every } \boldsymbol{u} \in U, \boldsymbol{w} \cdot \boldsymbol{u} = 0\}. \tag{8·11.1}$$

8·11.1. *Remark.* Recall, we call two vectors $\boldsymbol{w}$ and $\boldsymbol{u}$ *orthogonal* if $\boldsymbol{w} \cdot \boldsymbol{u} = 0$ which, intuitively, tells us these vectors are perpendicular to each other. We see what this definition is telling us: an orthogonal complement to U consists of all vectors orthogonal to everything in U.

8·12. Proposition. *For any $U \subseteq V$ subspace, its orthogonal complement $U^{\perp}$ is a subspace of V.*

Proof. We will invoke Theorem 8·3 and prove $U^{\perp}$ is closed under vector addition and scalar multiplication.

Let $\boldsymbol{w}_1, \boldsymbol{w}_2 \in U^{\perp}$ be arbitrary. Then for any $\boldsymbol{u} \in U$ we have

$$\boldsymbol{u} \cdot (\boldsymbol{w}_1 + \boldsymbol{w}_2)$$

= (distributivity of scalar multiplication over vector addition)

$$\boldsymbol{u} \cdot \boldsymbol{w}_1 + \boldsymbol{u} \cdot \boldsymbol{w}_2 \tag{8·12.1}$$

= (since $\boldsymbol{w}_1, \boldsymbol{w}_2 \in U^{\perp}$, definition of $U^{\perp}$)

$$0 + 0 = 0 \tag{8·12.2}$$

hence $(\boldsymbol{w}_1 + \boldsymbol{w}_2) \in U^{\perp}$. So it is closed under vector addition.

Let $\boldsymbol{w} \in U^{\perp}$ and $c \in \mathbb{R}$ be arbitrary. For any $\boldsymbol{u} \in U$, we have

$$(c\boldsymbol{w}) \cdot \boldsymbol{u}$$

= (associativity)

$$c(\boldsymbol{w} \cdot \boldsymbol{u}) \tag{8·12.3}$$

= (definition of orthogonal complement)

$$c(0) = 0. \tag{8·12.4}$$

Hence $c\boldsymbol{w} \in U^{\perp}$ and moreover $U^{\perp}$ is closed under scalar multiplication.

Thus $U^{\perp}$ is a subspace of V by Theorem 8·3. ∎

8·13. Definition. Let $U_1 \subseteq V$ and $U_2 \subseteq V$ be subspaces with a trivial intersection $U_1 \cap U_2 = \{\mathbf{0}_V\}$. Then we define the **"Direct Sum"** of U_1 with U_2 to be the set $U_1 \oplus U_2 = \{\boldsymbol{u}_1 + \boldsymbol{u}_2 \in V \mid \boldsymbol{u}_1 \in U_1, \boldsymbol{u}_2 \in U_2\}$.

8·13.1. *Remark.* Intuitively, the direct sum is how we combine "different" subspaces together.

8·14. Proposition. *If $U_1 \subseteq V$ and $U_2 \subseteq V$ are subspaces with trivial intersection $U_1 \cap U_2 = \{\mathbf{0}_V\}$, then their direct sum $U_1 \oplus U_2$ is a subspace of V.*

8·15. Proposition. *For any subspace $U \subseteq V$, we have $V = U^{\perp} \oplus U$.*

9 Linear Dependence and Bases

9·1. We want to address the question of whether this is a "best" spanning set for a subspace, and we saw in some sense "redundant elements" should be avoided. If $\boldsymbol{s}_1 \in S$ and $\boldsymbol{s}_2 \in S$, then it would be redundant to have $\boldsymbol{s}_1 + \boldsymbol{s}_2 \in S$. Let us try to formalize this intuition of "redundant combinations".

9·2. Definition. Let V be a vector space, let $\boldsymbol{v}_1, \ldots, v_n \in V$ be nonzero vectors $\boldsymbol{v}_j \neq \mathbf{0}$ for $j = 1, \ldots, n$. We call them **"Linearly Dependent"** if there are coefficients (not all zero) $c_1, \ldots, c_n \in \mathbb{R}$ such that

$$c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_n\boldsymbol{v}_n = \mathbf{0}. \tag{9·2.1}$$

If the only solution for this is $c_1 = c_2 = \cdots = c_n = 0$ for all coefficients to be zero, then we call the vectors **"Linearly Independent"**.

9·3. Example. In $\mathbb{R}^2$, consider the vectors

$$\boldsymbol{v}_1 = \begin{pmatrix}1\\0\end{pmatrix}, \boldsymbol{v}_2 = \begin{pmatrix}0\\1\end{pmatrix}, \boldsymbol{v}_3 = \begin{pmatrix}1\\1\end{pmatrix}, \boldsymbol{v}_4 = \begin{pmatrix}1\\-1\end{pmatrix}. \tag{9·3.1}$$

Any three or more vectors from this list are linearly dependent since $\boldsymbol{v}_3 = \boldsymbol{v}_1 + \boldsymbol{v}_2$ and $\boldsymbol{v}_4 = \boldsymbol{v}_1 - \boldsymbol{v}_2$. But any two vectors from this list are linearly independent.

9·4. Theorem (Criterion for Linear Dependence). *A set of nonzero vectors* $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ *is linearly dependent if and only if at least one of the vectors* $\boldsymbol{v}_k$ *is expressible as a linear combination of the others*

$$\boldsymbol{v}_k = \sum_{\substack{j=1\\ j\neq k}}^{n} c_j \boldsymbol{v}_j = c_1\boldsymbol{v}_1 + \cdots + c_{k-1}\boldsymbol{v}_{k-1} + c_{k+1}\boldsymbol{v}_{k+1} + \cdots + c_n\boldsymbol{v}_n, \tag{9·4.1}$$

where not all coefficients $c_j \in \mathbb{R}$ *are zero.*

Proof. ($\Longrightarrow$) Assume the vectors $\boldsymbol{v}_1$, ..., $\boldsymbol{v}_n$ are linearly dependent. Then by Definition 9·2, there are coefficients c_1, ..., c_n (not all zero) such that

$$c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_n\boldsymbol{v}_n = \mathbf{0}. \tag{9·4.2}$$

Let k be the last index for which $c_k \neq 0$ (so for indices ℓ such that $k < \ell \leq n$, then $c_\ell = 0$). Then we can subtract $c_k\boldsymbol{v}_k$ from both sides to get

$$c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_k\boldsymbol{v}_k - c_k\boldsymbol{v}_k = \mathbf{0} - c_k\boldsymbol{v}_k, \tag{9·4.3}$$

and dividing both sides by $-c_k$ gives us $\boldsymbol{v}_k$ as a linear combination of $\boldsymbol{v}_1$, ..., $\boldsymbol{v}_{k-1}$. This concludes the forward direction of the proof.

($\Longleftarrow$) Assume there exists a vector $\boldsymbol{v}_k$ such that we can write it as a linear combination of the remaining vectors

$$\begin{aligned}\boldsymbol{v}_k &= \sum_{\substack{j=1\\ j\neq k}}^{n} c_j \boldsymbol{v}_j \\ &= c_1\boldsymbol{v}_1 + \cdots + c_{k-1}\boldsymbol{v}_{k-1} + c_{k+1}\boldsymbol{v}_{k+1} + \cdots + c_n\boldsymbol{v}_n,\end{aligned} \tag{9·4.4}$$

where not all $c_j \in \mathbb{R}$ are zero. Then subtracting $\boldsymbol{v}_k$ from both sides gives us

$$\mathbf{0} = c_1\boldsymbol{v}_1 + \cdots + c_{k-1}\boldsymbol{v}_{k-1} - \boldsymbol{v}_k + c_{k+1}\boldsymbol{v}_{k+1} + \cdots + c_n\boldsymbol{v}_n. \tag{9·4.5}$$

Then by Definition 9·2, since not all coefficients c_j are zero, we have the vectors are linearly dependent. ☐

9·5. Theorem (Nonzero determinant iff columns are linearly independent). *Let* $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\} \subseteq \mathbb{R}^n$ *be a list of* n *distinct* n*-vectors, and*

$$\mathbf{M} = (\boldsymbol{v}_1 | \dots | \boldsymbol{v}_n) \tag{9·5.1}$$

be a matrix whose columns are the given n *column vectors. Then* $\det(\mathbf{M}) \neq 0$ *if and only if* $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ *are linearly independent.*

Proof. ($\Longrightarrow$) Assume $\det(\mathbf{M}) \neq 0$. Then $\mathbf{M}$ is invertible (by Theorem 5·18). Then $\mathbf{M}\boldsymbol{x} = \mathbf{0}$ has a unique solution (§3·43), namely $\boldsymbol{x} = \mathbf{0}$. This is equivalent to saying

$$x_1\boldsymbol{v}_1 + x_2\boldsymbol{v}_2 + \cdots + x_n\boldsymbol{v}_n = 0 \tag{9·5.2}$$

implies $x_1 = x_2 = \cdots = x_n = 0$. But by Definition 9·2, this is precisely the condition for $\boldsymbol{v}_1$, ..., $\boldsymbol{v}_n$ being linearly independent.

($\Longleftarrow$) Assume $\boldsymbol{v}_1$, ..., $\boldsymbol{v}_n$ are linearly independent. Then by Definition 9·2, the only solution to

$$c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n = \mathbf{0} \tag{9·5.3}$$

is $c_1 = \cdots = c_n = 0$. In matrix form, if $\boldsymbol{x} = (c_1, \dots, c_n)$ is a column n-vector, then

$$\mathbf{M}\boldsymbol{x} = \mathbf{0} \tag{9·5.4}$$

has $\boldsymbol{x} = \mathbf{0}$ be its only solution. This is true if and only if $\mathbf{M}$ is invertible. But $\mathbf{M}$ is invertible if and only if $\det(\mathbf{M}) \neq 0$. And by our assumption, $\boldsymbol{x} = \mathbf{0}$ is the only solution, hence the result. ☐

9·6. Corollary. *An $n \times n$ matrix $\mathbf{M}$ is invertible if and only if its columns are linearly independent vectors.*

Proof. We know from the previous theorem $\mathbf{M}$ has nonzero determinant if and only if its columns are linearly independent vectors. We know from Theorem 5·18 $\mathbf{M}$ has a nonzero determinant if and only if $\mathbf{M}$ is invertible. Therefore, we know $\mathbf{M}$ is invertible if and only if its columns are linearly independent vectors. $\square$

9·7. Definition. Let V be a real vector space and B a set of vectors from V such that

1. it spans V: $\operatorname{span}(B) = V$
2. there is no $A \subseteq B$ such that $\operatorname{span}(A) = V$.

Then we call B a **"Basis"** of V.

9·7.1. *Remark* (Need to prove existence of basis). We have just defined a word, "basis", but we have no guarantee that a basis will exist. This must be proven. The proof is not enlightening, and requires the axiom of choice (pick some nonzero vector, now pick another which is linearly independent of the first, keep picking linearly independent vectors — how? By the axiom of choice, it's always possible *somehow*; then show an arbitrary vector may be written as a linear combination of our collection of chosen vectors).

9·8. Example. In $\mathbb{R}^2$, the vectors

$$\boldsymbol{z} = \begin{pmatrix}1\\1\end{pmatrix}, \quad \text{and} \quad \bar{\boldsymbol{z}} = \begin{pmatrix}1\\-1\end{pmatrix}. \tag{9·8.1}$$

Then $\{\boldsymbol{z}, \bar{\boldsymbol{z}}\}$ form a basis for $\mathbb{R}^2$.

Proof. We need to show

1. $\operatorname{span}\{\boldsymbol{z}, \bar{\boldsymbol{z}}\} = \mathbb{R}^2$
2. there is no $A \subseteq \{\boldsymbol{z}, \bar{\boldsymbol{z}}\}$ such that $\operatorname{span}(A) = \mathbb{R}^2$.

The first claim may be proven by picking any element $\boldsymbol{v} \in \mathbb{R}^2$, then showing it may be written as a linear combination of $\boldsymbol{z}$ and $\bar{\boldsymbol{z}}$. We see, if

$$\boldsymbol{v} = \begin{pmatrix}v_1\\v_2\end{pmatrix}, \tag{9·8.2}$$

then

$$\frac{v_1+v_2}{2}\boldsymbol{z} + \frac{v_1-v_2}{2}\bar{\boldsymbol{z}}$$

= (unfolding the definition of $\boldsymbol{z}$, $\bar{\boldsymbol{z}}$)

$$\frac{v_1+v_2}{2}\begin{pmatrix}1\\1\end{pmatrix} + \frac{v_1-v_2}{2}\begin{pmatrix}1\\-1\end{pmatrix} \tag{9·8.3}$$

= (scalar multiplication)

$$\frac{1}{2}\begin{pmatrix}v_1+v_2\\v_1+v_2\end{pmatrix} + \frac{1}{2}\begin{pmatrix}v_1-v_2\\-v_1+v_2\end{pmatrix} \tag{9·8.4}$$

= (distributivity)

$$\frac{1}{2}\left[\begin{pmatrix}v_1+v_2\\v_1+v_2\end{pmatrix} + \begin{pmatrix}v_1-v_2\\-v_1+v_2\end{pmatrix}\right] \tag{9·8.5}$$

= (vector addition)

$$\frac{1}{2}\begin{pmatrix}(v_1+v_2)+(v_1-v_2)\\(v_1+v_2)+(-v_1+v_2)\end{pmatrix} \tag{9·8.6}$$

= (arithmetic)

$$\frac{1}{2}\begin{pmatrix}2v_1\\2v_2\end{pmatrix} \tag{9·8.7}$$

= (scalar multiplication)

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \boldsymbol{v} \tag{9·8.8}$$

as desired. Hence any element of $\mathbb{R}^2$ may be written as a linear combination of $\boldsymbol{z}$ and $\bar{\boldsymbol{z}}$, hence $\operatorname{span}(\{\boldsymbol{z}, \bar{\boldsymbol{z}}\}) = \mathbb{R}^2$.

As to the second claim, there is no $A \subseteq \{\boldsymbol{z}, \bar{\boldsymbol{z}}\}$, suppose there were such an A. Then either $A = \{\boldsymbol{z}\}$ or $A = \{\bar{\boldsymbol{z}}\}$. Pick $\boldsymbol{v} \in \{\boldsymbol{z}, \bar{\boldsymbol{z}}\}$ but $\boldsymbol{v} \notin A$. Then we claim $\boldsymbol{v} \notin \operatorname{span}(A)$.

It suffices to show $\boldsymbol{z}$ is not a multiple of $\bar{\boldsymbol{z}}$ (which corresponds to $A = \{\bar{\boldsymbol{z}}\}$ — in the other case, it boils down to the same proof). If $\boldsymbol{z}$ were a multiple of $\bar{\boldsymbol{z}}$, then there is a $c \in \mathbb{R}$ nonzero such that

$$c\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} \tag{9·8.9}$$

This is a system of 2 equations in 1 unknown:

$$c = 1, \quad \text{and} \quad c = -1. \tag{9·8.10}$$

But this is impossible. So $\boldsymbol{z}$ cannot be a multiple of $\bar{\boldsymbol{z}}$, which means $\boldsymbol{z} \notin \operatorname{span}(\{\bar{\boldsymbol{z}}\})$. The same reasoning shows $\bar{\boldsymbol{z}}$ is not a multiple of $\boldsymbol{z}$, which means $\bar{\boldsymbol{z}} \notin \operatorname{span}(\{\boldsymbol{z}\})$.

Hence there is no $A \subseteq \{\boldsymbol{z}, \bar{\boldsymbol{z}}\}$ such that $\operatorname{span}(A) = \mathbb{R}^2$. □

9·9. Example. Let $\boldsymbol{e}_j \in \mathbb{R}^n$ have 1 in its j^{th} component and 0 in all other components. Then the set $\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ forms a basis of $\mathbb{R}^n$ and is called its **"Canonical Basis"**.

9·10. Vector spaces have many bases. We see that a vector space may have more than one basis. In fact, they will have many different possible bases (plural of basis). We saw one basis in $\mathbb{R}^2$ given by $\boldsymbol{z} = (1, 1)$ and $\bar{\boldsymbol{z}} = (1, -1)$. We also see there is the canonical basis for $\mathbb{R}^2$, which is different from the first basis.

The moral of the story is that we may have many inequivalent bases for any given vector space.

9·11. Lemma. *Let V be a real vector space. Let $B = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ form a basis for V. Let $T = \{\boldsymbol{w}_1, \dots, \boldsymbol{w}_m\}$ be a set of linearly independent vectors from V. Then $m \leq n$ (i.e., $|T| \leq |B|$).*

Proof. Since T consists of linearly independent vectors, we can write $\boldsymbol{w}_m$ as a linear combination of basis vectors

$$\boldsymbol{w}_m = c_1^{(m)}\boldsymbol{b}_1 + c_2^{(m)}\boldsymbol{b}_2 + \cdots + c_n^{(m)}\boldsymbol{b}_n. \tag{9·11.1}$$

We can reindex the basis vectors such that $c_1^{(m)} \neq 0$. In that case, we "swap out" $\boldsymbol{b}_1$ for $\boldsymbol{w}_m$ since we can write $\boldsymbol{b}_1$ as a linear combination:

$$\boldsymbol{b}_1 = \frac{1}{c_1^{(m)}}\boldsymbol{w}_m - \frac{c_2^{(m)}\boldsymbol{b}_2 + \cdots + c_n^{(m)}\boldsymbol{b}_n}{c_1^{(m)}}. \tag{9·11.2}$$

This gives us a new set of basis vectors B_1, and we consider $T_1 = T \setminus \{\boldsymbol{w}_m\}$ the collection of elements from T which are not $\boldsymbol{w}_m$. In particular, there are $m - 1$ elements of T_1.

We can reiterate this step, swapping one element out of T_1 and putting it into B_1 (and throwing away an element from B_1 which has been replaced) to produce a new basis B_2. We produce T_2 from T_1 by taking the remaining elements of T_1 which are not in B_2 into T_2. We see T_2 has $m - 2$ elemeents.

Eventually one of two possibilities occurs:

1. We'll reach B_k which no longer has any original basis elements from B in it — they are disjoint $B \cap B_k = \emptyset$. But this would imply there are elements in T_k which cannot be written as a linear combination of the basis, which is a contradiction; or
2. We'll exhaust T_k and have no more elements from T to add to B_k.

We iterate this until we get to B_m and T_m, because T_{m+1} will be empty. □

9·12. Theorem (Any two bases have same number of elements)**.** *Let V be a real vector space. Suppose there exists at least one basis B for V, and suppose B has finitely many element. Then any two bases for V have the same number of elements as each other.*

Proof. Let B_1, B_2 be any two bases for V. Let $m = |B_1|$ and $n = |B_2|$. We claim
1. $m \leq n$ by the previous lemma, and
2. $n \leq m$ by the previous lemma.

Hence $m = n$. □

9·13. Definition. Let V be a real vector space, let B be a basis for V. If B has finitely many elements, then we say V is **"Finite-Dimensional"**. In that case, we call the number of vectors in B the **"Dimension"** of V.

9·13.1. *Remark.* Reasoning about infinite-dimensional spaces can be tricky. We have already seen one example, $\mathbb{R}[x]$ the space of polynomials. The linear algebra of inifnite-dimensional spaces usually goes by the name "functional analysis". A particularly friendly subfield is "Fourier analysis", where many intuitions from finite-dimensional linear algebra carries over.

9·14. Definition. Let V be a finite-dimensional vector space, let $B = \{\boldsymbol{f}_1, \dots, \boldsymbol{f}_n\}$ be a basis for V. We define an **"Ordered Basis"** to be a tuple $(\boldsymbol{f}_1, \dots, \boldsymbol{f}_n)$.

Futhermore, if the vectors $\boldsymbol{f}_1$, ..., $\boldsymbol{f}_n$ form a basis such that

$$\boldsymbol{f}_i \cdot \boldsymbol{f}_j = 0 \quad \text{if } i \neq j, \tag{9·14.1}$$

then we call it an **"Orthogonal Basis"** for V. If, even further, we have

$$\boldsymbol{f}_i \cdot \boldsymbol{f}_j = \delta_{i,j} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases} \tag{9·14.2}$$

then we call it an **"Orthonormal Basis"**.

9·14.1. *Remark.* This might seem silly (and, I guess, it is), but sets are not ordered. There are times when we will want to specifically note the order of basis vectors. The ordering may be arbitrary (for example, an accidental artifact induced by the indexing), but important.

9·14.2. *Remark.* In differential geometry, we sometimes see the term "frame" used for an ordered basis.

9.1 Coordinates Relative to a Basis

9·15. Recall, when we began discussing vector spaces like $\mathbb{R}^1$ and $\mathbb{R}^2$ (back in section 6), we began by drawing a line, picking a point O (calling it the origin), and then picking another point P. We identified the oriented line segment $\overrightarrow{OP}$ as a unit vector. Then any other point Q could be identified as a multiple of $\overrightarrow{OP}$ such that $\|\overrightarrow{OQ}\|/\|\overrightarrow{OP}\| = |x| \in \mathbb{R}$ and if Q is not "in the P direction", we said $-|x|\overrightarrow{OP} = \overrightarrow{OQ}$. In this way, we identified x as the coordinate of Q.

9·16. In $\mathbb{R}^2$, we did the same thing, but we now have two axes. Any point S on the plane could be identified by a pair of real numbers $(x, y) \in \mathbb{R}^2$ by similar means.

9·17. In general, this is what happens with a vector in a vector space relative to a basis. We obtain "coordinates" for the vector, enabling us to write our vector as a linear combination of basis vectors. This is a crucial point, because an n-dimensional real vector space V *is not identical* to $\mathbb{R}^n$ — but by choosing a basis, we can identify vectors in V with tuples of real numbers in $\mathbb{R}^n$, namely their coordinates. This should be familiar, we've been working with $n \times 1$ matrices and calling them vectors (but really, they're just inhabitants of $\mathbb{R}^n$). We have been stretching the truth all this time.

This is a really critical point to appreciate: vectors are "points in the plane" *not* an $n \times 1$ matrix. **Vectors are not matrices**. But we can turn a vector in a finite-dimensional vector space *into* a column $n \times 1$ matrix, and vice-versa, *given some basis* for V.

Let us try to make things concrete.

9·18. Definition. Let V be a finite-dimensional vector space, let $B = (\boldsymbol{f}_1, \dots, \boldsymbol{f}_n)$ be an ordered basis for V, and let $\boldsymbol{v} \in V$ be an arbitrary vector. Then we call the coefficients $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ in

$$\boldsymbol{v} = \lambda_1 \boldsymbol{f}_1 + \dots + \lambda_n \boldsymbol{f}_n \tag{9·18.1}$$

the **"Coordinates"** of $\boldsymbol{v}$ over B (or "relative to B"). We may write

$$[\boldsymbol{v}]_B = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \tag{9·18.2}$$

for the coordinates of $\boldsymbol{v}$ relative to basis B.

9·18.1. *Remark.* If we can write $\boldsymbol{v} = \lambda_1 \boldsymbol{f}_1 + \lambda_2 \boldsymbol{f}_2 + \dots + \lambda_n \boldsymbol{f}_n$, then we can identify $\boldsymbol{v}$ with the column vector of its coordinates relative to the $\boldsymbol{f}_j$:

$$\boldsymbol{v} \text{ "="} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}. \tag{9·18.3}$$

The equality is in quotation marks because it's not an equality but an *isomorphism*, a slightly weaker notion of "the same". We can prove (once we formalize the notion of an isomorphism) that any finite-dimensional real vector space V is isomorphic to $\mathbb{R}^n$ the collection of column n-vectors with real entries; this is done by identifying a vector with its coordinates relative to some basis. But this *does not* mean V is equal to $\mathbb{R}^n$.

▸ **Problem 4.** Suppose we have a finite-dimensional vector space V. Suppose we have one ordered basis $B = (\boldsymbol{e}_1, \dots, \boldsymbol{e}_n)$ and a distinct ordered basis $B' = (\boldsymbol{f}_1, \dots, \boldsymbol{f}_n)$ which share no vectors — we have $\boldsymbol{f}_i \neq \boldsymbol{e}_j$ for all i, $j = 1, \dots, n$.

If we have a vector $\boldsymbol{v} \in V$ and have found its coordinates relative to $\boldsymbol{f}_j$,

$$\boldsymbol{v} = \lambda_1 \boldsymbol{f}_1 + \dots + \lambda_n \boldsymbol{f}_n, \tag{9·18.4}$$

then how do we transform these into coordinates relative to $\boldsymbol{e}_i$?

9.2 Changing Bases

9·19. Change of Basis Matrix. Let V be a finite-dimensional real vector space. Let $B = (\boldsymbol{e}_1, \dots, \boldsymbol{e}_n)$ and $C = (\boldsymbol{f}_1, \dots, \boldsymbol{f}_n)$ be two ordered bases for V. Then the change of bases from B to C transforms coordinates for vectors $[\boldsymbol{v}]_B$ according to the matrix

$$\mathbf{M}^B_C = \left(\; [\boldsymbol{e}_1]_C \;\middle|\; \dots \;\middle|\; [\boldsymbol{e}_n]_C \; \right), \tag{9·19.1}$$

so any vector $\boldsymbol{v} \in V$ expressed in coordinates $[\boldsymbol{v}]_B$ relative to B may be expressed in coordinates relative to C as

$$[\boldsymbol{v}]_C = \mathbf{M}^B_C [\boldsymbol{v}]_B. \tag{9·19.2}$$

Why would this work? Well, if we expand the right-hand side, we would find

$$\left([\boldsymbol{e}_1]_C \mid \dots \mid [\boldsymbol{e}_n]_C \right) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \lambda_1[\boldsymbol{e}_1]_C + \lambda_2[\boldsymbol{e}_2]_C + \dots + \lambda_n[\boldsymbol{e}_n]_C. \tag{9·19.3}$$

But since $[\boldsymbol{e}_j]_C$ is a linear combination of the basis vectors $\boldsymbol{f}_1, \dots, \boldsymbol{f}_n$, this expands out to form a linear combination of $\boldsymbol{f}_1, \dots, \boldsymbol{f}_n$.

9·20. Theorem. *If V is a finite dimensional vector space with ordered bases B and C, if $[\mathbf{M}]^B_C$ is the change-of-coordinate matrix from B to C, then the change-of-coordinate matrix from C back to B (i.e., $[\mathbf{M}]^C_B$) satisfies*

$$[\mathbf{M}]^C_B = ([\mathbf{M}]^B_C)^{-1}. \tag{9·20.1}$$

That is to say, they are inverses of each other.

This partly motivated the bizarre superscript/subscript convention, it resembles a fraction.

We can ketch the proof out in (§9·22).

9·21. Relating Coordinates Between Orthonormal Bases. If B and C are both orthonormal bases for V, there is no reason to believe they consist of the same basis vectors. One way to obtain a different set of orthonormal basis vectors from B is by an arbitrary rotation, and possibly reflection about an axis (or about a nonzero vector). These transformations produce a different basis, but do not affect the orthonormality of the new basis.

What does the change of coordinates matrix look like between them?

9·22. We can write out the matrix components explicitly for orthonormal coordinates $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ and other orthonormal coordinates $\boldsymbol{f}_1, \dots, \boldsymbol{f}_n$ as

$$\boldsymbol{f}_1 = (\boldsymbol{f}_1 \cdot \boldsymbol{e}_1)\boldsymbol{e}_1 + (\boldsymbol{f}_1 \cdot \boldsymbol{e}_2)\boldsymbol{e}_2 + \dots + (\boldsymbol{f}_1 \cdot \boldsymbol{e}_n)\boldsymbol{e}_n \tag{9·22.1}$$

$$\boldsymbol{f}_2 = (\boldsymbol{f}_2 \cdot \boldsymbol{e}_1)\boldsymbol{e}_1 + (\boldsymbol{f}_2 \cdot \boldsymbol{e}_2)\boldsymbol{e}_2 + \dots + (\boldsymbol{f}_2 \cdot \boldsymbol{e}_n)\boldsymbol{e}_n \tag{9·22.2}$$

$$\begin{matrix} \vdots & & \vdots & & \vdots & \ddots & \vdots \end{matrix}$$

$$\boldsymbol{f}_n = (\boldsymbol{f}_n \cdot \boldsymbol{e}_1)\boldsymbol{e}_1 + (\boldsymbol{f}_n \cdot \boldsymbol{e}_2)\boldsymbol{e}_2 + \dots + (\boldsymbol{f}_n \cdot \boldsymbol{e}_n)\boldsymbol{e}_n \tag{9·22.3}$$

The components of the matrix $[\mathbf{M}]^B_C = (\boldsymbol{f}_i \cdot \boldsymbol{e}_j)$. What is the inverse of this matrix?

We could do some complicated math, or we could wonder the simpler problem: what is $[\mathbf{M}]^B_C([\mathbf{M}]^B_C)^{\mathsf{T}}$?

$$([\mathbf{M}]^B_C([\mathbf{M}]^B_C)^{\mathsf{T}})_{i,k}$$

= (unfold the definition of matrix multiplication)

$$\sum_{j=1}^{n}([\mathbf{M}]^B_C)_{i,j}(([\mathbf{M}]^B_C)^{\mathsf{T}})_{j,k} \tag{9·22.4}$$

= (unfold the definition of $[\mathbf{M}]^B_C$ into components)

$$\sum_{j=1}^{n}(\boldsymbol{f}_i^{\mathsf{T}}\boldsymbol{e}_j)(\boldsymbol{e}_j^{\mathsf{T}}\boldsymbol{f}_k) \tag{9·22.5}$$

= (distributivity)

$$\boldsymbol{f}_i^{\mathsf{T}}\left(\sum_{j=1}^{n}\boldsymbol{e}_j\boldsymbol{e}_j^{\mathsf{T}}\right)\boldsymbol{f}_k \tag{9·22.6}$$

= (matrix multiplication, see Lemma 9·23 below)

$$\boldsymbol{f}_i^{\mathsf{T}}(\mathbf{I}_n)\,\boldsymbol{f}_k \tag{9·22.7}$$

= (defining property of the identity matrix, associativity of multiplication)

(9·22.8) $\boldsymbol{f}_i^{\mathsf{T}}\boldsymbol{f}_k$

= (by definition of orthonormality)

(9·22.9) $\delta_{i,k}$

In other words,

$$[\mathbf{M}]_C^B([\mathbf{M}]_C^B)^{\mathsf{T}} = \mathbf{I}. \tag{9·22.10}$$

This implies

$$([\mathbf{M}]_C^B)^{-1} = ([\mathbf{M}]_C^B)^{\mathsf{T}}. \tag{9·22.11}$$

In other words, the change of basis matrix is an orthogonal matrix (c.f., Exercise 3.15).

9·23. Lemma. *Let V be a finite-dimensional vector space, let $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ be an orthonormal basis for V. Then*

$$\sum_{j=1}^{n}\boldsymbol{e}_j\boldsymbol{e}_j^{\mathsf{T}} = \mathbf{I}_n. \tag{9·23.1}$$

Proof. We consider how this acts on an arbitrary vector $\boldsymbol{v} \in V$.

$$\left(\sum_{j=1}^{n}\boldsymbol{e}_j\boldsymbol{e}_j^{\mathsf{T}}\right)\boldsymbol{v}$$

= (expanding $\boldsymbol{v}$ in the basis)

(9·23.2) $\left(\sum_{j=1}^{n}\boldsymbol{e}_j\boldsymbol{e}_j^{\mathsf{T}}\right)\left(\sum_{k=1}^{n}c_k\boldsymbol{e}_k\right)$

= (by linearity)

(9·23.3) $\sum_{k=1}^{n}c_k\left(\sum_{j=1}^{n}\boldsymbol{e}_j\boldsymbol{e}_j^{\mathsf{T}}\boldsymbol{e}_k\right)$

= (by definition of orthonormality)

(9·23.4) $\sum_{k=1}^{n}c_k\left(\sum_{j=1}^{n}\boldsymbol{e}_j\delta_{j,k}\right)$

= (unrolling the inner sum over j)

(9·23.5) $\sum_{k=1}^{n}c_k\left(\boldsymbol{e}_1\delta_{1,k} + \cdots + \boldsymbol{e}_{k-1}\delta_{k-1,k} + \boldsymbol{e}_k\delta_{k,k} + \boldsymbol{e}_{k+1}\delta_{k+1,k} + \cdots + \boldsymbol{e}_n\delta_{n,k}\right)$

= (definition of $\delta_{j,k}$)

(9·23.6) $\sum_{k=1}^{n}c_k\left(\boldsymbol{e}_1 0 + \cdots + \boldsymbol{e}_{k-1}0 + \boldsymbol{e}_k 1 + \boldsymbol{e}_{k+1}0 + \cdots + \boldsymbol{e}_n 0\right)$

= (arithmetic)

(9·23.7) $\sum_{k=1}^{n}c_k\left(\boldsymbol{e}_k\right)$

= (multiplication)

(9·23.8) $\sum_{k=1}^{n}c_k\boldsymbol{e}_k$

= (since this is the expansion of $\boldsymbol{v}$ in the basis $\boldsymbol{e}_k$, "undoing" the first step of this chain of calculations)

(9·23.9) $\boldsymbol{v}$.

Since this was for arbitrary $\boldsymbol{v} \in V$, it follows that

$$\sum_{j=1}^{n} \boldsymbol{e}_j \boldsymbol{e}_j^{\mathsf{T}} = \mathbf{I}_n, \tag{9·23.10}$$

as desired. □

9.3 Graham–Schmidt Method

9·24. Puzzle. If we have an n-dimensional vector space V with n linearly independent [nonzero] vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$, then is there any way to construct an orthonormal basis out of them?

9·25. Solution. We will construct an orthonormal basis, one vector at a time.

The first step is to construct our initial vector

$$\widehat{\boldsymbol{v}_1} = \frac{\boldsymbol{x}_1}{\|\boldsymbol{x}_1\|}. \tag{9·25.1}$$

This is a unit vector, and now we will use it to start our collection. We could have easily have chosen $\boldsymbol{v}_1 = \boldsymbol{x}_1$, as well, it would just make things a little longer.

We now find the second vector $\boldsymbol{v}_2$. Since $\boldsymbol{x}_2$ and $\boldsymbol{x}_1$ are linearly independent, it follows that $\boldsymbol{x}_2$ and $\boldsymbol{v}_1$ are linearly independent. Then we hope to find coefficients c_1 and c_2 such that

$$\boldsymbol{v}_2 = c_1\widehat{\boldsymbol{v}_1} + c_2\boldsymbol{x}_2 \tag{9·25.2}$$

is a unit vector orthogonal to $\boldsymbol{v}_1$. So

$$\widehat{\boldsymbol{v}_1} \cdot \boldsymbol{v}_2 = 0, \tag{9·25.3}$$

which forces us to admit

$$0 = \widehat{\boldsymbol{v}_1} \cdot (c_1\widehat{\boldsymbol{v}_1} + c_2\boldsymbol{x}_2) \tag{9·25.4a}$$
$$= c_1\widehat{\boldsymbol{v}_1} \cdot \widehat{\boldsymbol{v}_1} + c_2\widehat{\boldsymbol{v}_1} \cdot \boldsymbol{x}_2 \tag{9·25.4b}$$
$$= c_1 + c_2\widehat{\boldsymbol{v}_1} \cdot \boldsymbol{x}_2 \tag{9·25.4c}$$

hence

$$c_1 = -c_2\widehat{\boldsymbol{v}_1} \cdot \boldsymbol{x}_2. \tag{9·25.4d}$$

Setting $c_2 = 1$ (since it's arbitrary), we find

$$\boldsymbol{v}_2 = -(\widehat{\boldsymbol{v}_1} \cdot \boldsymbol{x}_2)\widehat{\boldsymbol{v}_1} + \boldsymbol{x}_1 = \boldsymbol{x}_2 - (\widehat{\boldsymbol{v}_1} \cdot \boldsymbol{x}_2)\widehat{\boldsymbol{v}_1}. \tag{9·25.4e}$$

We can quickly check that $\widehat{\boldsymbol{v}_1} \cdot \boldsymbol{v}_2 = 0$.

We now can see that $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ span everything which $\boldsymbol{x}_1$, $\boldsymbol{x}_2$ spanned. Since $\boldsymbol{x}_3$ was independent of $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$, we have $\boldsymbol{x}_3 \notin \operatorname{span}(\{\boldsymbol{x}_1, \boldsymbol{x}_2)$. Therefore we will use $\boldsymbol{x}_3$ to construct $\boldsymbol{v}_3$ by writing

$$\boldsymbol{v}_3 = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + c_3\boldsymbol{x}_3. \tag{9·25.5}$$

We are trying to determine the unknown coefficients c_1, c_2, c_3. We know $\boldsymbol{v}_3$ will be orthogonal to $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$:

$$\boldsymbol{v}_3 \cdot \boldsymbol{v}_2 = 0, \quad \text{and} \quad \boldsymbol{v}_3 \cdot \boldsymbol{v}_1 = 0. \tag{9·25.6}$$

The first of these give us (recalling $\boldsymbol{v}_2 \cdot \boldsymbol{v}_1 = 0$),

$$\boldsymbol{v}_3 \cdot \boldsymbol{v}_2 = 0 = c_2\boldsymbol{v}_2 \cdot \boldsymbol{v}_2 + c_3\boldsymbol{x}_3 \cdot \boldsymbol{v}_2, \tag{9·25.7}$$

hence

$$c_2 = -c_3 \frac{\boldsymbol{x}_3 \cdot \boldsymbol{v}_2}{\boldsymbol{v}_2 \cdot \boldsymbol{v}_2}. \tag{9·25.8}$$

Similarly, we find

$$\boldsymbol{v}_3 \cdot \boldsymbol{v}_1 = 0 = c_1 \boldsymbol{v}_1 \cdot \boldsymbol{v}_1 + c_3 \boldsymbol{x}_3 \cdot \boldsymbol{v}_1, \tag{9·25.9}$$

give us

$$c_1 = -c_3 \frac{\boldsymbol{x}_3 \cdot \boldsymbol{v}_1}{\boldsymbol{v}_1 \cdot \boldsymbol{v}_1}. \tag{9·25.10}$$

Setting $c_3 = 1$ give us

$$\boldsymbol{v}_3 = \boldsymbol{x}_3 - \left(\frac{\boldsymbol{x}_3 \cdot \boldsymbol{v}_1}{\boldsymbol{v}_1 \cdot \boldsymbol{v}_1}\right)\boldsymbol{v}_1 - \left(\frac{\boldsymbol{x}_3 \cdot \boldsymbol{v}_2}{\boldsymbol{v}_2 \cdot \boldsymbol{v}_2}\right)\boldsymbol{v}_2. \tag{9·25.11}$$

Now we have three basis vectors in our collection.

We see that

$$\boldsymbol{v}_3 = \boldsymbol{x}_3 - (\boldsymbol{x}_3 \cdot \widehat{\boldsymbol{v}_1})\widehat{\boldsymbol{v}_1} - (\boldsymbol{x}_3 \cdot \widehat{\boldsymbol{v}_2})\widehat{\boldsymbol{v}_2}. \tag{9·25.12}$$

The general pattern seems to be

$$\boldsymbol{v}_{n+1} = \boldsymbol{x}_{n+1} - \sum_{k=1}^{n} \left(\frac{\boldsymbol{x}_{n+1} \cdot \boldsymbol{v}_k}{\boldsymbol{v}_k \cdot \boldsymbol{v}_k}\right)\boldsymbol{v}_k. \tag{9·25.13}$$

Is this actually true?

Well, we've proven it works for $n = 2$ and $n = 3$, so we can try proving it by induction. We assume this works for arbitrary $(n+1) \in \mathbb{N}$. Then the inductive case, supposing we have $n+1$ orthogonal vectors $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, ..., $\boldsymbol{v}_{n+1}$, and we have a vector $\boldsymbol{x}_{n+2} \notin \operatorname{span}(\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_{n+1}\})$. Then we claim

$$\boldsymbol{v}_{n+2} = \boldsymbol{x}_{n+2} - \sum_{k=1}^{n+1} \left(\frac{\boldsymbol{x}_{n+1} \cdot \boldsymbol{v}_k}{\boldsymbol{v}_k \cdot \boldsymbol{v}_k}\right)\boldsymbol{v}_k \tag{9·25.14}$$

is orthogonal to $\boldsymbol{v}_j$ for $j = 1, \dots, n+1$. To see this, we compute,

$$\boldsymbol{v}_j \cdot \boldsymbol{v}_{n+2}$$

= (unfolding definition of $\boldsymbol{v}_{n+2}$)

$$\boldsymbol{v}_j \cdot \left(\boldsymbol{x}_{n+2} - \sum_{k=1}^{n+1} \left(\frac{\boldsymbol{x}_{n+1} \cdot \boldsymbol{v}_k}{\boldsymbol{v}_k \cdot \boldsymbol{v}_k}\right)\boldsymbol{v}_k\right) \tag{9·25.15}$$

= (distributivity of dot product)

$$\boldsymbol{v}_j \cdot \boldsymbol{x}_{n+2} - \sum_{k=1}^{n+1} \left(\frac{\boldsymbol{x}_{n+1} \cdot \boldsymbol{v}_k}{\boldsymbol{v}_k \cdot \boldsymbol{v}_k}\right)\boldsymbol{v}_j \cdot \boldsymbol{v}_k \tag{9·25.16}$$

= (orthogonality of $\boldsymbol{v}_j \cdot \boldsymbol{v}_k = \delta_{j,k}\boldsymbol{v}_j \cdot \boldsymbol{v}_j$)

$$\boldsymbol{v}_j \cdot \boldsymbol{x}_{n+2} - \sum_{k=1}^{n+1} \left(\frac{\boldsymbol{x}_{n+1} \cdot \boldsymbol{v}_k}{\boldsymbol{v}_k \cdot \boldsymbol{v}_k}\right)\delta_{j,k}\boldsymbol{v}_j \cdot \boldsymbol{v}_j \tag{9·25.17}$$

= (defining property of $\delta_{j,k}$)

$$\boldsymbol{v}_j \cdot \boldsymbol{x}_{n+2} - \left(\frac{\boldsymbol{x}_{n+1} \cdot \boldsymbol{v}_j}{\boldsymbol{v}_j \cdot \boldsymbol{v}_j}\right)\boldsymbol{v}_j \cdot \boldsymbol{v}_j \tag{9·25.18}$$

= (commutativity of multiplication)

$$\boldsymbol{v}_j \cdot \boldsymbol{x}_{n+2} - \boldsymbol{x}_{n+1} \cdot \boldsymbol{v}_j \left(\frac{\boldsymbol{v}_j \cdot \boldsymbol{v}_j}{\boldsymbol{v}_j \cdot \boldsymbol{v}_j}\right) \tag{9·25.19}$$

= (since $\boldsymbol{v}_j \neq \mathbf{0}$ hence $\boldsymbol{v}_j \cdot \boldsymbol{v}_j \neq 0$)

(9·25.20) $\quad \boldsymbol{v}_j \cdot \boldsymbol{x}_{n+2} - \boldsymbol{x}_{n+1} \cdot \boldsymbol{v}_j$

$=$ (arithmetic)

(9·25.21) $\quad 0.$

Hence $\boldsymbol{v}_{n+2}$ is orthogonal to $\boldsymbol{v}_j$ for every $j = 1, \dots, n+1$.

9·26. Graham–Schmidt Algorithm. Given m linearly independent nonzero vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$, we can construct an orthonormal basis for $\operatorname{span}(\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_m\})$ as follows:

Step 1. Set $\boldsymbol{f}_1 = \widehat{\boldsymbol{x}_1}$. Then go to step 2.

Step 2. For each $\boldsymbol{x}_2, \dots, \boldsymbol{x}_m$, compute $\boldsymbol{v}_k$ by

$$\boldsymbol{v}_k = \boldsymbol{x}_k - \sum_{j=1}^{k} (\boldsymbol{x}_k \cdot \boldsymbol{f}_j)\boldsymbol{f}_j, \tag{9·26.1}$$

and then set

$$\boldsymbol{f}_k = \widehat{\boldsymbol{v}_k} = \frac{\boldsymbol{v}_k}{\|\boldsymbol{v}_k\|}. \tag{9·26.2}$$

This produces an orthonormal basis $B = \{\boldsymbol{f}_1, \dots, \boldsymbol{f}_m\}$.

9·26.1. *Remark.* If we have a subspace $U \subseteq V$ and have found an orthonormal basis B_U of B, then we can extend it to a basis B of V by taking $n = \dim(V)$ linearly independent vectors in V, and applying the Graham–Schmidt algorithm to add them to B_V.

9·27. Definition. Let $\boldsymbol{u}, \boldsymbol{v} \in V$ be vectors. Assume $\boldsymbol{u} \neq \boldsymbol{0}_V$. We define the **"Projection"** of $\boldsymbol{v}$ along the $\boldsymbol{u}$ direction to be the vector

$$\operatorname{Proj}_{\boldsymbol{u}}(\boldsymbol{v}) = \frac{\boldsymbol{u} \cdot \boldsymbol{v}}{\boldsymbol{u} \cdot \boldsymbol{u}}\boldsymbol{u} = (\widehat{\boldsymbol{u}} \cdot \boldsymbol{v})\widehat{\boldsymbol{u}} \tag{9·27.1}$$

where $\widehat{\boldsymbol{u}} = \boldsymbol{u}/\|\boldsymbol{u}\|$ is a unit vector.

9·27.1. *Remark.* We can see that the Graham–Schmidt algorithm can be rephrased as taking n linearly independent vectors $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n$, and forming

$$\boldsymbol{u}_1 = \boldsymbol{x}_1 \tag{9·27.2a}$$
$$\boldsymbol{u}_2 = \boldsymbol{x}_2 - \operatorname{Proj}_{\boldsymbol{u}_1}(\boldsymbol{x}_2) \tag{9·27.2b}$$
$$\boldsymbol{u}_3 = \boldsymbol{x}_3 - \operatorname{Proj}_{\boldsymbol{u}_1}(\boldsymbol{x}_3) - \operatorname{Proj}_{\boldsymbol{u}_2}(\boldsymbol{x}_3) \tag{9·27.2c}$$
$$\vdots$$
$$\boldsymbol{u}_n = \boldsymbol{x}_n - \sum_{k=1}^{n-1} \operatorname{Proj}_{\boldsymbol{u}_k}(\boldsymbol{x}_n). \tag{9·27.2d}$$

This produces a set of n orthogonal vectors, and we could normalize them ("put hats on them") to obtain n orthonormal vectors.

9·28. Definition. Let $\boldsymbol{u}, \boldsymbol{v} \in V$ be vectors. Assume $\boldsymbol{u} \neq \boldsymbol{0}_V$. We define the **"Orthogonal Decomposition"** of $\boldsymbol{v}$ with respect to $\boldsymbol{u}$ as consisting of two vectors:

1. the parallel part $\boldsymbol{v}^{\parallel} = \operatorname{Proj}_{\boldsymbol{u}}(\boldsymbol{v})$, and
2. the perpendicular part $\boldsymbol{v}^{\perp} = \boldsymbol{v} - \boldsymbol{v}^{\parallel}$.

10 Linear Transformations

10·1. We have, so far, introduced a new shiny toy, a new mathematical gadget called a "vector space". So far, we have discussed quite a few aspects about them, except for one very important thing: how do we "map" one vector space into another?

10·2. Definition. Let V, W be real vector spaces. A **"Linear Transformation"** is a function $L\colon V \to W$ such that for each $\boldsymbol{u}$, $\boldsymbol{v} \in V$ and for any $c_1, c_2 \in \mathbb{R}$, we have it map linear combinations in V to linear combinations in W:

$$L(c_1\boldsymbol{u} + c_2\boldsymbol{v}) = c_1L(\boldsymbol{u}) + c_2L(\boldsymbol{v}). \qquad (10\cdot2.1)$$

If further $V = W$, then we call L a **"Linear Operator"**. We may also just refer to the function f as *Linear*.

10·2.1. *Remark.* Some authors give two conditions for L being a linear transformation:

1. homogeneity: $L(c\boldsymbol{v}) = cL(\boldsymbol{v})$ for every $c \in \mathbb{R}$ and $\boldsymbol{v} \in V$
2. additive: $L(\boldsymbol{u} + \boldsymbol{v}) = L(\boldsymbol{u}) + L(\boldsymbol{v})$ for every $\boldsymbol{u}$, $\boldsymbol{v} \in V$.

Can you prove these two versions are secretly the same?

10·3. Example. Let V be a real vector space. The identity function $\mathrm{id}\colon V \to V$, defined by $\mathrm{id}(\boldsymbol{v}) = \boldsymbol{v}$ for all $\boldsymbol{v} \in V$, is a linear operator on V.

Proof. Let $\boldsymbol{u}$, $\boldsymbol{v} \in V$ be arbitrary. Let $c_1, c_2 \in \mathbb{R}$ be arbitrary. We want to prove

$$\mathrm{id}(c_1\boldsymbol{u} + c_2\boldsymbol{v}) = c_1\mathrm{id}(\boldsymbol{u}) + c_2\mathrm{id}(\boldsymbol{v}). \qquad (10\cdot3.1)$$

We see that the left-hand side expands to

$$\mathrm{id}(c_1\boldsymbol{u} + c_2\boldsymbol{v}) = c_1\boldsymbol{u} + c_2\boldsymbol{v}, \qquad (10\cdot3.2)$$

and the right-hand side expands to

$$c_1\mathrm{id}(\boldsymbol{u}) + c_2\mathrm{id}(\boldsymbol{v}) = c_1\boldsymbol{u} + c_2\boldsymbol{v}. \qquad (10\cdot3.3)$$

Then we invoke the well-known fact that,

$$c_1\boldsymbol{u} + c_2\boldsymbol{v} = c_1\boldsymbol{u} + c_2\boldsymbol{v} \qquad (10\cdot3.4)$$

to conclude we must have

$$\mathrm{id}(c_1\boldsymbol{u} + c_2\boldsymbol{v}) = c_1\mathrm{id}(\boldsymbol{u}) + c_2\mathrm{id}(\boldsymbol{v}). \qquad (10\cdot3.5)$$

as desired. □

10·4. Non-Example (Shifting is not a linear transformation)**.** Let V be a vector space, let $\boldsymbol{v}_0 \in V$ be a nonzero vector. Define $f\colon V \to V$ by

$$f(\boldsymbol{v}) = \boldsymbol{v} + \boldsymbol{v}_0. \qquad (10\cdot4.1)$$

This is not a linear transformation. Why not? Well, suppose we have $\boldsymbol{u} \in V$ and $\boldsymbol{v} \in V$, then

$$\begin{aligned} & f(\boldsymbol{u} + \boldsymbol{v}) \\ = \quad & \text{(unfold definition of } f) \\ (10\cdot4.2) \qquad & (\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{v}_0 \end{aligned}$$

However,

$$\begin{aligned} & f(\boldsymbol{u}) + f(\boldsymbol{v}) \\ = \quad & \text{(unfold definition of } f) \end{aligned}$$

(10·4.3) $(\boldsymbol{u}+\boldsymbol{v}_0)+(\boldsymbol{v}+\boldsymbol{v}_0)$

We see that, in general,

$$(\boldsymbol{u}+\boldsymbol{v}_0)+(\boldsymbol{v}+\boldsymbol{v}_0)\neq(\boldsymbol{u}+\boldsymbol{v})+\boldsymbol{v}_0. \tag{10·4.4}$$

Hence

$$f(\boldsymbol{u}+\boldsymbol{v})\neq f(\boldsymbol{u})+f(\boldsymbol{v}). \tag{10·4.5}$$

Or to summarize it in a single equation

$$\begin{array}{ccc} f(\boldsymbol{u}+\boldsymbol{v}) & \stackrel{???}{=} & f(\boldsymbol{u})+f(\boldsymbol{v}) \\ \| & & \| \\ (\boldsymbol{u}+\boldsymbol{v})+\boldsymbol{v}_0 & \neq & (\boldsymbol{u}+\boldsymbol{v}_0)+(\boldsymbol{v}+\boldsymbol{v}_0) \end{array} \tag{10·4.6}$$

which means f cannot be linear.

10·5. Example. Let $c\in\mathbb{R}$ be a nonzero constant $c\neq 0$, let V be a real vector space. Let $f\colon V\to V$ be defined by

$$f(\boldsymbol{v})=c\boldsymbol{v}. \tag{10·5.1}$$

Then f is a linear operator.

Proof. Let $\boldsymbol{u},\boldsymbol{v}\in V$ be arbitrary, let $c_1,c_2\in\mathbb{R}$ be arbitrary. We will show $f(c_1\boldsymbol{u}+c_2\boldsymbol{v})=c_1f(\boldsymbol{u})+c_2f(\boldsymbol{v})$. We begin by expanding

$f(c_1\boldsymbol{u}+c_2\boldsymbol{v})$

= (unfold definition of f)

(10·5.2) $c(c_1\boldsymbol{u}+c_2\boldsymbol{v})$

= (distributivity of scalar multiplication)

(10·5.3) $cc_1\boldsymbol{u}+cc_2\boldsymbol{v}$

= (associativity of scalar multiplication)

(10·5.4) $c(c_1\boldsymbol{u})+c(c_2\boldsymbol{v})$

= (folding the definition of f)

(10·5.5) $f(c_1\boldsymbol{u})+f(c_2\boldsymbol{v})$

This proves f is linear. □

10·6. Example. Let $\boldsymbol{u}\in V$ be a nonzero vector. Then projection along $\boldsymbol{u}$,

$$\mathrm{Proj}_{\boldsymbol{u}}\colon V\to V \tag{10·6.1a}$$

sends

$$\boldsymbol{v}\mapsto\frac{\boldsymbol{u}\cdot\boldsymbol{v}}{\boldsymbol{u}\cdot\boldsymbol{u}}\boldsymbol{u}. \tag{10·6.1b}$$

This is a linear operator.

10·7. Example. Let $\widehat{\boldsymbol{x}}\in V$ be a unit vector. We define the **"Householder transformation"**

$$H_{\boldsymbol{x}}\colon V\to V \tag{10·7.1a}$$

by

$$\boldsymbol{v}\mapsto\boldsymbol{v}-\widehat{\boldsymbol{x}}(\widehat{\boldsymbol{x}}\cdot\boldsymbol{v}). \tag{10·7.1b}$$

This describes a reflection about the plane whose normal vector is $\widehat{\boldsymbol{x}}$. We see this is the sum of two linear operators, the identity matrix, and the projection in the direction of $-\boldsymbol{x}$. The sum of linear operators is itself a linear operator.

10·8. Other examples. There are a few other examples which are useful, in particular, if V is a vector space and $U \subseteq V$ is a subspace, then the inclusion map

$$\iota\colon U \to V \tag{10·8.1}$$

defined by $\iota(\boldsymbol{u}) = \boldsymbol{u}$ for every $\boldsymbol{u} \in U$, this is a linear transformation. We could also go the other way around: we could construct a mapping

$$p\colon V \to U \tag{10·8.2}$$

which projects to U. It's a little trickier *at this point* to prove it, though.

10·9. Definition. When $L\colon V \to W$ is a linear transformation, we call:

- the inputs V the **"Domain"** of L,
- the possible outputs W the **"Codomain"** of L,
- the **"Image"** of L is the subset $L(V) = \{L(\boldsymbol{v}) \in W \mid \boldsymbol{v} \in V\}$ of vectors in W which are the output of L.

Note: the codomain consists of the *possible* outputs, the image consists of the *actual* outputs.

10·10. Definition. If $L\colon V \to W$ is a linear transformation, we can define its **"Inverse"** to be a linear transformation $L^{-1}\colon W \to V$ such that $L^{-1} \circ L = \mathrm{id}_V$ and $L \circ L^{-1} = \mathrm{id}_W$.

10·11. A lot of the terminology for matrices carries over to linear transformations. For example, if $L\colon V \to V$ is a linear operator, we call it **"Similar"** to a linear operator $M\colon V \to V$ if there exists an invertible linear operator $P\colon V \to V$ such that $L = P^{-1} \circ M \circ P$. Compare this to similar matrices, $\mathbf{A} \sim \mathbf{B}$ if there exists an invertible $\mathbf{P}$ such that $\mathbf{A} = \mathbf{P}^{-1}\mathbf{B}\mathbf{P}$. We may abuse notation and write $L \sim M$ when two linear operators are similar.

10.1 Matrices as "Coordinates" of Linear Transformations

10·12. We saw how basis vectors, for a finite-dimensional vector space V, allows us to introduce coordinates for vectors (in Definition 9·18). This was great because it allowed us to use some of our matrix machinery we built in Part II when computing vector operations. But there is more: basis vectors let us express a linear transformation as a matrix, and "the linear transformation acting on a vector" as mere matrix multiplication.

10·13. Definition. Let V, W be [finite-dimensional] vector spaces with bases $B_V = (\boldsymbol{e}_1, \dots, \boldsymbol{e}_m)$ and $B_W = (\boldsymbol{f}_1, \dots, \boldsymbol{f}_n)$ respectively. Let $L\colon V \to W$ be a linear transformation. Then the **"Matrix for L relative to B_V and B_W"** is the matrix $\mathbf{M}$ whose j^{th} column is the coordinate vector for $L(\boldsymbol{e}_j)$ relative to B_W. Then, for any $\boldsymbol{v} \in V$, we may compute $L(\boldsymbol{v})$ using $\mathbf{M}$ multiplied by the coordinate vector of $\boldsymbol{v}$ relative to basis $\boldsymbol{e}_j$.

10·13.1. *Remark.* Just because we *defined* something doesn't mean it works as intended, or even exists. We need to *prove it* in a theorem.

10·14. Theorem (This stuff works)**.** *Let $L\colon V \to W$ be a linear transformation from an m-dimensional real vector space V to an n-dimensional real vector space W. Let $B_V = (\boldsymbol{e}_1, \dots, \boldsymbol{e}_m)$ be a basis for V; let $B_W = (\boldsymbol{f}_1, \dots, \boldsymbol{f}_n)$ be a basis for W.*

Then the $n \times m$ matrix $\mathbf{M}$ — whose j^{th} column is the coordinate vector $[L(\boldsymbol{e}_j)]_{B_W}$ of $L(\boldsymbol{e}_j)$ relative to the basis B_W — is associated with L and has the following property: For any $\boldsymbol{v} \in V$, we have

$$[L(\boldsymbol{v})]_{B_W} = \mathbf{M}[\boldsymbol{v}]_{B_V} \tag{10·14.1}$$

where $[\boldsymbol{v}]_{B_V}$ is the $m \times 1$ coordinate vector of $\boldsymbol{v}$ relative to B_V, and $[L(\boldsymbol{v})]_{B_W}$ is the $n \times 1$ coordinate vector of $L(\boldsymbol{v})$ relative to B_W. Moreover, $\mathbf{M}$ is the only matrix with this property.

Proof sketch. The idea is to to construct such a matrix $\mathbf{M}$ from $L\colon V \to W$ and bases $B_V = (\boldsymbol{e}_1, \dots, \boldsymbol{e}_m)$ and $B_W = (\boldsymbol{f}_1, \dots, \boldsymbol{f}_n)$, as follows:

Step 1. Compute $L(\boldsymbol{e}_j)$ for $j = 1, \ldots, m$.
Step 2. Find the coordinate vector $[L(\boldsymbol{e}_j)]_{B_W}$ for $L(\boldsymbol{e}_j)$ relative to the basis B_W. This means expressing $L(\boldsymbol{e}_j)$ as a linear combination of the $\boldsymbol{f}_i$.
Step 3. The matrix $\mathbf{M}$ of L with respect to B_V and B_W is formed by choosing $[L(\boldsymbol{e}_j)]_{B_W}$ as the j^{th} column of $\mathbf{M}$.

In this way, any vector $\boldsymbol{v} = c_1\boldsymbol{e}_1 + \cdots + c_m\boldsymbol{e}_m$ is mapped to $L(\boldsymbol{v}) = c_1 L(\boldsymbol{e}_1) + c_2 L(\boldsymbol{e}_2) + \cdots + c_m L(\boldsymbol{e}_m)$ by definition of a linear transformation, and this coincides with matrix multiplication $\mathbf{M}[\boldsymbol{v}]_{B_V}$. ☐

10·15. What do we do if the bases for either vector space is not canonical or orthogonal? The trick is to form an augmented matrix

$$[\boldsymbol{f}_1 \quad \ldots \quad f_n \mid L(\boldsymbol{e}_1) \quad \ldots \quad L(\boldsymbol{e}_m)] \tag{10·15.1}$$

then applying elementary row operations, we transform it to reduced row echelon form, and then keep transforming it until it becomes

$$[\boldsymbol{f}_1 \quad \ldots \quad f_n \mid L(\boldsymbol{e}_1) \quad \ldots \quad L(\boldsymbol{e}_m)] \sim [\mathbf{I} \mid \mathbf{M}]. \tag{10·15.2}$$

We then identify $\mathbf{M}$ as the matrix for L relative to the basis B_V and B_W.

10.2 Injective, Surjective, Bijective Linear Transformations

10·16. Definition. Let $L\colon V \to W$ be a linear transformation. We call L

- **"Surjective"** (or *Onto*) if, to each and every $\boldsymbol{w} \in W$, there exists a $\boldsymbol{v} \in V$ such that $L(\boldsymbol{v}) = \boldsymbol{w}$
- **"Injective"** (or, confusingly, *into*) if for any $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ such that $L(\boldsymbol{v}_1) = L(\boldsymbol{v}_2)$, then we have $\boldsymbol{v}_1 = \boldsymbol{v}_2$ — equivalently, if $\boldsymbol{v}_1 \neq \boldsymbol{v}_2$, then $L(\boldsymbol{v}_1) \neq L(\boldsymbol{v}_2)$.
- **"Bijective"** if it is both surjective and injective.

10·16.1. *Remark.* These terms (injective, surjective, bijective) hold for *any* function on sets. That is to say, these are not "linear algebra specific terms".

10·17. Example (Surjective map)**.** Let $U \subseteq V$ be a subspace. The map $L\colon V \to U$, defined by for any $\boldsymbol{u} \in U$, $L(\boldsymbol{u}) = \boldsymbol{u}$, and for any $\boldsymbol{v} \in V$ but $\boldsymbol{v} \notin U$ we have $L(\boldsymbol{v}) = \boldsymbol{0}$. This is a surjective linear transformation.

Proof. Surjectivity isn't hard, we're told every $\boldsymbol{u} \in U$ are mapped to $L(\boldsymbol{u}) = \boldsymbol{u}$. Linearity may be a bit more difficult. If we had some basis B_U of U which extends to a basis of V, then we see

$$L(\sum_{j=1}^{m} c_j \boldsymbol{b}_j + \sum_{k=m+1}^{n} d_k \boldsymbol{f}_k) = \sum_{j=1}^{m} c_j \boldsymbol{b}_j \tag{10·17.1}$$

where $\boldsymbol{b}_j \in B_U$ for each $j = 1, \ldots, m$ and $\boldsymbol{f}_k \notin B_U$ are basis vectors for the rest of V (which would be mapped to zero), and $c_j \in \mathbb{R}$ for $j = 1, \ldots, m$ and $d_k \in \mathbb{R}$ for $k = m+1, \ldots, n$. This is indeed linear, by definition. ☐

10·18. Surjective Linear Maps. A surjective linear map is sometimes denoted with a two-headed arrow $L\colon V \twoheadrightarrow W$. We intuitively think of surjectivity as "covering" the entire codomain.

10·19. Example (Injective map)**.** Let $U \subseteq V$ be a subspace. Then $L\colon U \to V$, defined by $L(\boldsymbol{u}) = \boldsymbol{u}$, is an injective linear map.

Proof. Let $\boldsymbol{u}_1, \boldsymbol{u}_2 \in U$ be arbitrary. Assume $\boldsymbol{u}_1 \neq \boldsymbol{u}_2$. Then $L(\boldsymbol{u}_1) = \boldsymbol{u}_1 \neq \boldsymbol{u}_2 = L(\boldsymbol{u}_1)$, hence $L(\boldsymbol{u}_1) \neq L(\boldsymbol{u}_2)$. Then by definition, L is injective. ☐

10·20. Injective maps embed. An injective linear map is sometimes denoted with the arrow $L\colon V \hookrightarrow W$ with a hooked arrow. This intuitively corresponds to embedding V into W. That is to say, there exists a subspace of W which is "the same" as V.

10·21. Isomorphisms. A bijective linear transformation is also called a **"Isomorphism"** of vector spaces. If $L\colon V \to W$ is a bijective linear transformation, then we may write $V \cong W$ to indicate there exists a bijective linear transformation between them.

What this means is that, when viewed as vector spaces, V and W are "the same". To every element $\boldsymbol{v} \in V$ there is a unique $\boldsymbol{w} \in W$ such that $L(\boldsymbol{v}) = \boldsymbol{w}$.

10·22. Definition. Let U, V, W be real vector spaces, let $L\colon U \to V$ and $M\colon V \to W$ be linear transformations. We define the **"Composition"** of L followed by M as a linear transformation denoted $M \circ L\colon U \to W$ (written from right to left) such that for any $\boldsymbol{u} \in U$, $(M \circ L)(\boldsymbol{u}) = M(L(\boldsymbol{u}))$.

10·23. Properties of Composition. These are properties of composition which are true:

1. Associativity: for any $f\colon W \to X$, $g\colon X \to Y$, and $h\colon Y \to Z$, we have $(h \circ g) \circ f = h \circ (g \circ f)$.
2. Right Identity law: if $f\colon X \to Y$ is any function, and id_X is the identity function on X (so every $x \in X$ satisfies $\mathrm{id}_X(x) = x$), then $f \circ \mathrm{id}_X = f$.
3. Left Identity law: if $f\colon X \to Y$ is any function, and id_Y is the identity function on Y (so every $y \in Y$ satisfies $\mathrm{id}_X(y) = y$), then $\mathrm{id}_Y \circ f = f$.

This is true for all functions, not just linear transformations.

10·23.1. *Remark.* For the collection of linear operators acting on a vector space V, we see we can think of composition as a sort of "multiplication" operator (which is associative and has a "number one"-like quantity, the identity map id_V). Further, we have the sum of linear operators $L_1, L_2\colon V \to V$ defined as $(L_1 + L_2)(\boldsymbol{v}) = L_1(\boldsymbol{v}) + L_2(\boldsymbol{v})$ for all $\boldsymbol{v} \in V$. We may define scalar multiplication similarly, for any $c \in \mathbb{R}$, $(cL_1)(\boldsymbol{v}) = c\,(L_1(\boldsymbol{v}))$. This gives us a vector space structure on the collection of linear operators on V, *and* an associative multiplication operator; together these form a gadget called a *Associative Algebra.*

Oftentimes we forget all about the vector space structure, and use the composition of operators to form a *Monoid.* If we encode the state of a system as a vector in V, then linear operators can be used to describe how the state changes. This is what happens in quantum mechanics. We can use it for any dynamical system, where the evolution of state by an infinitesimal amount of time is described by a linear operator. The properties of the linear operator reflect physical properties of the dynamical system.

10·24. Definition. Let V, W be real vector spaces. Let $T\colon V \to W$.

1. We define the **"Right Inverse"** of T to be the linear transformation $R\colon W \to V$ such that for each $\boldsymbol{w} \in W$, $(T \circ R)(\boldsymbol{w}) = \boldsymbol{w}$.
2. We define the **"Left Inverse"** of T to be the linear transfromation $L\colon W \to V$ such that for each $\boldsymbol{v} \in V$, $(L \circ T)(\boldsymbol{v}) = \boldsymbol{v}$.
3. We define the **"Two-Sided Inverse"** (or more frequently, just "*Inverse*") of T to be the linear transformation $N\colon W \to V$ such that N is both a left-inverse and right-inverse of L.

10·25. Proposition (Uniqueness of Inverse)**.** *If $L\colon V \to W$ is a linear transformation with a two-sided inverse $M\colon V \to W$, then M is unique.*

Proof. Suppose $M_1, M_2\colon V \to W$ are a pair of two-sided inverses for L. Let $\mathrm{id}_V\colon V \to V$ be the identity mapping on V, $\mathrm{id}_W\colon W \to W$ be the identity mapping on W. Then

$$\mathrm{id}_W = \mathrm{id}_W$$

$\equiv$ (since M_1, M_2 are right-inverses of L)

(10·25.1) $$(L \circ M_1) = (L \circ M_2)$$

$\equiv$ (compose on left by M_1)

(10·25.2) $$M_1 \circ (L \circ M_1) = M_1 \circ (L \circ M_2)$$

$\equiv$ (associativity of composing functions)

(10·25.3) $$(M_1 \circ L) \circ M_1 = (M_1 \circ L) \circ M_2$$

$\equiv$ (since M_1 is a left-inverse of L)

(10·25.4) $$\mathrm{id}_V \circ M_1 = \mathrm{id}_V \circ M_2$$

$\equiv$ (defining property of identity function)

(10·25.5) $\quad M_1 = M_2$

Hence any two two-sided inverses of L must be equal to each other. $\square$

10·26. Notation. Since the two-sided inverse is unique, we denote it by T^{-1} as we do for numbers.

10·27. Proposition (Right inverses exist for surjective maps)**.** *Let V and W be real vector spaces, $T\colon V \to W$ be a linear transformation. Then T is surjective if and only if there exists a right-inverse $R\colon W \to V$ for T (that is, $T \circ R = \mathrm{id}_W$).*

Proof. ($\Longrightarrow$) Assume T is surjective. We want to find a $R\colon W \to V$ such that for each $\boldsymbol{w} \in W$, $T\left(R(\boldsymbol{w})\right) = \boldsymbol{w}$. We know for each $\boldsymbol{w} \in W$ there is at least one $\boldsymbol{v}$ such that $T(\boldsymbol{v}) = \boldsymbol{w}$, by definition of surjectivity. We could take a basis $B_W = \{\boldsymbol{f}_1, \dots, \boldsymbol{f}_n\}$ for W, then for each basis element $\boldsymbol{f}_j \in B_W$ take some corresponding $\boldsymbol{v}_j \in V$ such that $T(\boldsymbol{v}_j) = \boldsymbol{f}_j$. We construct R by $R(\boldsymbol{f}_j) = \boldsymbol{v}_j$ and demanding linearity (which is possible because T is lienar). Then

$$(T \circ R)(\boldsymbol{w})$$

$=$ (expanding out using our basis B_W)

(10·27.1) $$(T \circ R)\left(\sum_{j=1}^{n} w_j \boldsymbol{f}_j\right)$$

$=$ (unfolding composition of maps)

(10·27.2) $$T\left(R\left(\sum_{j=1}^{n} w_j \boldsymbol{f}_j\right)\right)$$

$=$ (by R being linear)

(10·27.3) $$T\left(\sum_{j=1}^{n} w_j R\left(\boldsymbol{f}_j\right)\right)$$

$=$ (by construction of R defined by $R(\boldsymbol{f}_j) = \boldsymbol{v}_j$)

(10·27.4) $$T\left(\sum_{j=1}^{n} w_j \boldsymbol{v}_j\right)$$

$=$ (by T being linear)

(10·27.5) $$\sum_{j=1}^{n} w_j T\left(\boldsymbol{v}_j\right)$$

$=$ (by construction of $\boldsymbol{v}_j$ such that $T(\boldsymbol{v}_j) = \boldsymbol{f}_j$)

(10·27.6) $$\sum_{j=1}^{n} w_j \boldsymbol{f}_j$$

$=$ (folding back $\boldsymbol{w}$ from its expansion relative to B_W)

(10·27.7) $$\boldsymbol{w}$$

Hence R is a right-inverse, as desired.

($\Longleftarrow$) Assume $R\colon W \to V$ is a right-inverse for T, i.e., $T \circ R = \mathrm{id}_W$. Then for each $\boldsymbol{w} \in W$, $T\left(R(\boldsymbol{w})\right) = \boldsymbol{w}$. But since $R(\boldsymbol{w}) = \boldsymbol{v}$ for *some* $\boldsymbol{v} \in V$, we see $T(\boldsymbol{v}) = \boldsymbol{w}$. Since $\boldsymbol{w}$ was arbitrary, this means every $\boldsymbol{w}$ has at least one $\boldsymbol{v} \in V$ for which $T(\boldsymbol{v}) = \boldsymbol{w}$ (namely $\boldsymbol{v} = R(\boldsymbol{w})$). Hence T is surjective, by definition. $\square$

10·28. Proposition (Left inverses exist for injective maps). *Let V, W be real vector spaces, $T\colon V \to W$ be a linear transformation. Then T is injective if and only if there exists a left inverse $L\colon W \to V$ for T, i.e., $L \circ T = \mathrm{id}_V$.*

Proof. ($\implies$) Suppose T is injective. Then for each $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ such that $\boldsymbol{v}_1 \neq \boldsymbol{v}_2$ we have $T(\boldsymbol{v}_1) \neq T(\boldsymbol{v}_2)$. If we set $L(T(\boldsymbol{v}_1)) = \boldsymbol{v}_1$ and for any $\boldsymbol{w} \notin T(V)$ is mapped to the zero vector $L(\boldsymbol{w}) = \mathbf{0}_V$ (really this can be any arbitrary vector, provided linearity is preserved), then L is a left-inverse function.

($\impliedby$) Suppose there exists a left-inverse L for T. Then for any $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ we see if

$$T(\boldsymbol{v}_1) = T(\boldsymbol{v}_2), \tag{10·28.1}$$

then we can apply L to both sides $L\left(T(\boldsymbol{v}_1)\right) = L\left(T(\boldsymbol{v}_2)\right)$ but by definition of L being a left inverse, this means

$$\boldsymbol{v}_1 = \boldsymbol{v}_2. \tag{10·28.2}$$

Hence T is injective. □

10·29. Example. Let V be a n-dimensional real vector space (for some $n \in \mathbb{N}$). Then there is a bijection $L\colon V \to \mathbb{R}^n$.

Proof. Take $B = \{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\}$ to be a basis for V. We then define L to map these basis vectors in V to the canonical basis in $\mathbb{R}^n$, $L(\boldsymbol{b}_j) = \boldsymbol{e}_j$. By linearity, we have linear combinations mapped to linear combinations

$$L\left(\sum_{j=1}^{n} v_j \boldsymbol{b}_j\right) = \sum_{j=1}^{n} v_j L(\boldsymbol{b}_j) = \sum_{j=1}^{n} v_j \boldsymbol{e}_j. \tag{10·29.1}$$

We see this is a bijection because it's determined entirely by how it acts on the basis vectors B, and each $\boldsymbol{b}_j \in B$ is mapped to a distinct $\boldsymbol{e}_j$ [injectivity]. Every canonical basis vector $\boldsymbol{e}_j$ is "hit" by exactly one $\boldsymbol{b}_j \in B$ [surjectivity]. We can define the inverse mapping $L^{-1}(\boldsymbol{e}_j) = \boldsymbol{b}_j$ and demand linearity. □

10·30. General Picture. We can combine these insights to get some sense of what these terms mean. For example, a surjective linear map is one whose codomain is isomorphic to a subspace of the domain. An injective linear map is one whose image is isomorphic with the domain.

10.3 Kernels and Images

10·31. Definition. Let $L\colon V \to W$ be a linear transformation. We define the **"Kernel"** of L to be the collection of vectors mapped to the zero vector of W: $\ker(L) = \{\boldsymbol{v} \in V \mid L(\boldsymbol{v}) = \mathbf{0}_W\}$.

10·31.1. *Remark.* We can also talk about the "kernel" of a matrix, or other mathematical mappings when there is a notion of "zero" (or a "zero-like quantity").

10·32. Proposition. *If $L\colon V \to W$ is a linear transformation, then $\ker(L)$ is a subspace of V.*

Proof. Claim 1: for any $\boldsymbol{v}$, $\boldsymbol{w} \in \ker(L)$, we have $\boldsymbol{v} + \boldsymbol{w} \in \ker(L)$.

We can see this from $L(\boldsymbol{v} + \boldsymbol{w}) = L(\boldsymbol{v}) + L(\boldsymbol{w})$ by linearity, and then $L(\boldsymbol{v}) + L(\boldsymbol{w}) = \mathbf{0}_W + \mathbf{0}_W = \mathbf{0}_W$. Hence $\boldsymbol{v} + \boldsymbol{w} \in \ker(L)$.

Claim 2: for any $\boldsymbol{v} \in \ker(L)$ and $c \in \mathbb{R}$, we have $(c\boldsymbol{v}) \in \ker(L)$.

We can see this from $L(c\boldsymbol{v}) = cL(\boldsymbol{v})$ due to linearity, and $cL(\boldsymbol{v}) = c\mathbf{0}_W = \mathbf{0}_W$. Hence $c\boldsymbol{v} \in \ker(L)$.

Then by Theorem 8·3, $\ker(L)$ is a subspace of V. □

10·33. Proposition. *Let $L\colon V \to W$ be a linear transformation. If $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ are mapped to the same element $L(\boldsymbol{v}_1) = L(\boldsymbol{v}_2)$, then their difference lives in the kernel of L, $\boldsymbol{v}_2 - \boldsymbol{v}_1 \in \ker(L)$.*

Proof. Assume $L(\boldsymbol{v}_1) = L(\boldsymbol{v}_2)$. Then

$$
\begin{aligned}
& L(\boldsymbol{v}_1) = L(\boldsymbol{v}_2) \\
\equiv\ & \text{(subtracting } L(\boldsymbol{v}_1) \text{ from both sides)} \\
(10{\cdot}33.1)\quad & L(\boldsymbol{v}_2) - L(\boldsymbol{v}_1) = \mathbf{0}_W \\
\equiv\ & \text{(linearity)} \\
(10{\cdot}33.2)\quad & L(\boldsymbol{v}_2 - \boldsymbol{v}_1) = \mathbf{0}_W
\end{aligned}
$$

hence $\boldsymbol{v}_2 - \boldsymbol{v}_1 \in \ker(L)$ as desired. □

10·34. Theorem. *Let $L\colon V \to W$ be a linear transformation. Then L is an injective linear map if and only if $\ker(L) = 0$ is the trivial subspace.*

Proof. ($\implies$) Assume L is an injective map. For every $\boldsymbol{v} \in V$ such that $\boldsymbol{v} \neq \mathbf{0}_V$ we have $L(\boldsymbol{v}) \neq L(\mathbf{0}_V) = \mathbf{0}_W$. Then $L(\boldsymbol{v}) \neq \mathbf{0}_W$, which implies $\boldsymbol{v} \notin \ker(L)$ when $\boldsymbol{v} \neq \mathbf{0}_V$. Hence $\ker(L) = \{\mathbf{0}_V\}$.

($\impliedby$) Assume $\ker(L) = 0 = \{\mathbf{0}_V\}$. Then for any $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ such that $L(\boldsymbol{v}_1) = L(\boldsymbol{v}_2)$, we see $L(\boldsymbol{v}_2) - L(\boldsymbol{v}_1) = \mathbf{0}_W$. By linearity, we know $L(\boldsymbol{v}_2) - L(\boldsymbol{v}_1) = L(\boldsymbol{v}_2 - \boldsymbol{v}_1)$, hence $\boldsymbol{v}_2 - \boldsymbol{v}_1 \in \ker(L)$. But this implies $\boldsymbol{v}_2 - \boldsymbol{v}_1 = \mathbf{0}_V$, which means $\boldsymbol{v}_2 = \boldsymbol{v}_1$. Hence L is injective. □

10·35. Dimensions of Kernel. Let $L\colon V \to W$ be a linear transformation, V a finite-dimensional vector space. Suppose $\dim\ker(L) = k < \dim(V)$. What does this mean? Well, we have a k-dimensional subspace of V which "collapses" under application of L, in the sense that $L(\ker(L)) = 0$ is the trivial subspace of W.

But if $n = \dim(V)$, then what happens to the other $n - k$ dimensions of V under L? Well, there are two possibilities:

1. some elements of $V \setminus \ker(L)$ would be mapped to $\mathbf{0}_W$, or
2. no element of $V \setminus \ker(L)$ could be mapped to $\mathbf{0}_W$.

If some element $\boldsymbol{v}$ in $V \setminus \ker(L)$ [i.e. $\boldsymbol{v} \in V$ but $\boldsymbol{v} \notin \ker(L)$] is mapped to $\mathbf{0}_W$, then $L(\boldsymbol{v}) = \mathbf{0}_W$ which by definition makes it $\boldsymbol{v} \in \ker(L)$. This is impossible, so we are in the second possibility: no element of $V \setminus \ker(L)$ could be mapped to $\mathbf{0}_W$.

Could $V \setminus \ker(L)$ form a subspace of V? Technically, no, because $\mathbf{0}_V \in \ker(L)$, so it would be impossible for $\mathbf{0}_V \in V \setminus \ker(L)$. Alright, well, what about the set $U = \{\mathbf{0}_V\} \cup (V \setminus \ker(L))$, could this form a subspace of V?

Let us consider a basis for $\ker(L)$. We could do this by finding k linearly independent vectors, then applying the Graham–Schmidt algorithm (§9·26) to form a basis B_K of $\ker(L)$. We can consider the canonical basis for V, then apply the Graham–Schmidt algorithm to extend B_K to an orthonormal basis B of all of V. The elements $B_U = \{\boldsymbol{b} \in B \mid \boldsymbol{b} \notin B_K\}$ form a basis for $U = \operatorname{span}(B_U)$. Moreover, $L(V) = L(U)$.

We see that $\dim(U) = |B_U|$ is the number of basis elements which do not belong to the kernel, and $\dim(\ker(L))$ is the number of the remaining basis vectors. Consequently,

$$\dim(U) + \dim(\ker(L)) = \dim(V). \tag{10·35.1}$$

We also see that $\dim(U) = \dim(L(V))$. This gives us the celebrated result

$$\boxed{\dim(L(V)) + \dim(\ker(L)) = \dim(V).} \tag{10·35.2}$$

10·36. Definition. If $L\colon V \to W$ is a linear transformation, we call $\dim(\ker(L))$ its **"Nullity"** and $\dim(L(V))$ is **"(Column) Rank"**.

10·37. Importance of Linear Transformations. Just as a concluding remark, I'd like to emphasize the importance of linear transformations. So far, we have spent nearly 20 pages talking about vector spaces before even thinking about linear transformations. But this is for pedagogical reasons, to help the reader get acquainted with the objects of linear algebra.

Secretly, all information concerning a vector space may be obtained from linear transformations to, or from, the vector space.

This sounds preposterous and conspiratorial. But every possible subspace is a kernel of some linear transformation (and the image of another). Further, if we realize that a linear transformation, when expressed relative to a basis, is a matrix, then we see a lot of the machinery we constructed for matrices plays an important role. There is one extraordinarily powerful *coup* we can introduced for matrices [eigenstuff], which — when applied to linear transformations — demonstrates the power of these linear transformations.

11 Eigenstuff

11·1. Note to self. I wanted to include this as the ending of part II, but I realized the usefulness of eigenstuff is in having eigenvectors forming a basis, and then diagonalizing the matrix. This requires putting this section in part III.

11.1 Eigenstuff for Matrices

11·2. Example (Motivating Example)**.** Consider the matrix

$$\mathbf{M} = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}. \tag{11·2.1}$$

We find that there are two "directions" (distinct vectors) which are just dilated when we multiply by $\mathbf{M}$,

$$\mathbf{M}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \tag{11·2.2a}$$

and

$$\mathbf{M}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = 3\begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{11·2.2b}$$

This isn't a neat parlor trick: it turns out any invertible $n\times n$ matrix will have at most n vectors which are "dilated" by the matrix.

11·3. Definition. Let $\mathbf{A}$ be an $n\times n$ matrix. We define an **"Eigenvector"** of $\mathbf{A}$ to be a [column] n-vector $\boldsymbol{v}$ such that there is a nonzero $\lambda\in\mathbb{R}$ [called the **"Eigenvalue"** associated with $\boldsymbol{v}$] satisfying

$$\mathbf{A}\boldsymbol{v} = \lambda\boldsymbol{v}. \tag{11·3.1}$$

11·3.1. *Remark* (Linear Operators can have eigenstuff)*.* We also have an eigenvector for a linear operator $L\colon V\to V$ be a vector $\boldsymbol{v}\in V$ such that there is a nonzero $\lambda\in\mathbb{R}$ satisfying $L(\boldsymbol{v}) = \lambda\boldsymbol{v}$. We don't even require V to be finite-dimensional (but it's far easier when $\dim(V)<\infty$).

11·4. Finding Eigenvalues and Eigenvectors. This is great, but how do we find eigenvalues and eigenvectors? The first thing to note is we can rewrite Eq (11·3.1) by subtracting $\lambda\boldsymbol{v}$ from both sides:

$$\mathbf{A}\boldsymbol{v} - \lambda\boldsymbol{v} = \mathbf{0}. \tag{11·4.1}$$

We insert a secret identity operator (the matrix analog of "multiply by 1"):

$$\mathbf{A}\boldsymbol{v} - \lambda\mathbf{I}\boldsymbol{v} = \mathbf{0}. \tag{11·4.2}$$

We can factor out $\boldsymbol{v}$ by distributivity:

$$(\mathbf{A} - \lambda\mathbf{I})\boldsymbol{v} = \mathbf{0}. \tag{11·4.3}$$

For this equation to hold, either $\boldsymbol{v} = 0$ or $(\mathbf{A} - \lambda\mathbf{I}) = 0$, right?

Wrong: $(\mathbf{A} - \lambda\mathbf{I})$ could be nonzero and noninvertible. That is when

$$\det(\mathbf{A} - \lambda\mathbf{I}) = 0. \tag{11·4.4}$$

But the left-hand side is not identically zero. In fact, the left-hand side is a polynomial in λ. *This polynomial is how we find eigenvalues for matrices.*

Once we have an eigenvalue, we can plug it in and then solve the system of equations for the eigenvector. But first, let us define this polynomial quantity.

11·5. Definition. Let $\mathbf{A}$ be an $n \times n$ matrix. The **"Characteristic Polynomial"** of $\mathbf{A}$ is

$$p(\lambda) = \det(\mathbf{A} - \lambda\mathbf{I}). \tag{11·5.1}$$

Some authors use $\det(\lambda\mathbf{I} - \mathbf{A})$, it doesn't matter since they have the same roots (which are the eigenvalues of $\mathbf{A}$ and the *actual* quantity of interest).

11·6. Pop quiz. If we multiply a row of $\mathbf{A}$ by a nonzero scalar $c \in \mathbb{R}$, then will this change the characteristic polynomial for $\mathbf{A}$?

11·7. Example. Recall our motivating example at the start of this section, we had

$$\mathbf{M} = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}. \tag{11·7.1}$$

Its characteristic polynomial is

$$\det\begin{pmatrix} 2-\lambda & -1 \\ -1 & 2-\lambda \end{pmatrix} = (2-\lambda)^2 - 1 = \lambda^2 - 4\lambda + 3. \tag{11·7.2}$$

We find this has roots $\lambda = 1$ and $\lambda = 3$.

We can find the eigenvector for $\lambda = 1$ by solving

$$2x_1 - x_2 = x_1 \tag{11·7.3a}$$

$$-x_1 + 2x_2 = x_2. \tag{11·7.3b}$$

These give us 2 copies of the same line described by

$$-x_1 = -x_2, \quad \text{or} \quad x_1 = x_2. \tag{11·7.4}$$

We have a generic eigenvector look like

$$\boldsymbol{v}_1 = m\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

where $m \in \mathbb{R}$. Usually we normalize the eigenvector to be a unit vector (so we fix any such parameters), which gives us

$$\boldsymbol{v}_1 = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}. \tag{11·7.5}$$

This is one eigenvector.

The other eigenvector, the one associated with $\lambda = 3$, requires solving the system of equations

$$2x_1 - x_2 = 3x_1 \tag{11·7.6a}$$

$$-x_1 + 2x_2 = 3x_2. \tag{11·7.6b}$$

This gives us two copies of the same line, described by the equation

$$x_1 = -x_2. \tag{11·7.7}$$

The unit eigenvector is then

$$\boldsymbol{v}_2 = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}. \tag{11·7.8}$$

The reader may verify these satisfy the equation $\mathbf{M}\boldsymbol{v} = \lambda\boldsymbol{v}$ for eigenvectors of $\mathbf{M}$.

11·8. Everything we've said carries over to linear operators acting on a vector space $L\colon V \to V$.

11·9. Lemma. *If* $\mathbf{A}$ *is an* $n\times n$ *matrix with eigenvalues* $\lambda_1, \dots, \lambda_n$*, then*

$$\det(\mathbf{A}) = \prod_{j=1}^{n}\lambda_j \tag{11·9.1}$$

and

$$\operatorname{tr}(\mathbf{A}) = \sum_{j=1}^{n}\lambda_j. \tag{11·9.2}$$

Proof. We suppose there are n eigenvalues for our $n\times n$ matrix $\lambda_1, \dots, \lambda_n$. We have the following, starting from the characteristic polynomial for $\mathbf{A}$:

$p_{\mathbf{A}}(\lambda)$

= (definition of characteristic polynomial)

(11·9.3) $\det(\mathbf{A}-\lambda\mathbf{I})$

= (fundamental theorem of algebra, Theorem 11·19)

(11·9.4) $(\lambda_1-\lambda)(\cdots)(\lambda_n-\lambda)$

(Recall (§11·19), the fundamental theorem of algebra states if $p(\lambda)$ is a polynomial of degree n with roots $\lambda_1, \dots, \lambda_n$, then $p(\lambda) = c(\lambda-\lambda_1)(\cdots)(\lambda-\lambda_n)$.) Now, if we set $\lambda = 0$ to the characteristic polynomial, we find

$$\det(\mathbf{A}) = \prod_{j=1}^{n}\lambda_j, \tag{11·9.5}$$

as desired.

For the trace, we again start with the characteristic polynomial, but divided by $(-\lambda)^n$,

$$\frac{p_{\mathbf{A}}(\lambda)}{(-\lambda)^n} = \det\left(\mathbf{I}+\frac{\mathbf{A}}{\lambda}\right). \tag{11·9.6}$$

Set $\varepsilon = 1/\lambda$ and take λ large enough so $0<\varepsilon\ll 1$, then by Proposition 5·20,

$$\det\left(\mathbf{I}+\frac{\mathbf{A}}{\lambda}\right) = 1+\frac{\operatorname{tr}(\mathbf{A})}{\lambda}+\mathcal{O}(\lambda^{-2}). \tag{11·9.7}$$

Here $\mathcal{O}(\lambda^{-2})$ means there are terms involving factors of λ^{-2} or some power of it, which we do not care about, and "sweep under the rug".

But we see, by expanding out the left-hand side,

$$\frac{\det(\lambda\mathbf{I}+\mathbf{A})}{\lambda^n} = \prod_{j=1}^{n}\frac{\lambda+\lambda_j}{\lambda} = \prod_{j=1}^{n}\left(1+\frac{\lambda_j}{\lambda}\right). \tag{11·9.8}$$

Again, taking $\varepsilon = 1/\lambda$ and expanding out the product gives us

$$\frac{\det(\lambda\mathbf{I}+\mathbf{A})}{\lambda^n} = \prod_{j=1}^{n}\left(1+\frac{\lambda_j}{\lambda}\right) = 1+\frac{1}{\lambda}\sum_{j=1}^{n}\lambda_j+\mathcal{O}(\lambda^{-2}). \tag{11·9.9}$$

Then equating results, we find

$$\operatorname{tr}(\mathbf{A}) = \sum_{j=1}^{n}\lambda_j \tag{11·9.10}$$

as desired. □

11·9.1. *Remark.* As a consistency check, observe if $\mathbf{A}$ is singular, then it has a zero eigenvalue. The product of its eigenvalues would be zero. Its determinant (as a singular matrix) would be zero. So our lemma is consistent with this special case.

11.2 Diagonalization

11·10. Definition. We call an $n \times n$ matrix $\mathbf{M}$ **"Diagonalizable"** if there exists a diagonal $n \times n$ matrix $\mathbf{D}$ such that $\mathbf{M} \sim \mathbf{D}$; i.e., if there is an invertible $n \times n$ matrix $\mathbf{P}$ such that $\mathbf{M} = \mathbf{P}^{-1}\mathbf{D}\mathbf{P}$.

11·11. Lemma. *The identity matrix is similar only to itself.*

Proof. For $\mathbf{I}_n$, pick any invertible matrix $\mathbf{P}$. We find

$\mathbf{P}^{-1}\mathbf{I}_n\mathbf{P}$

= (associativity of matrix multiplication)

(11·11.1) $\mathbf{P}^{-1}(\mathbf{I}_n\mathbf{P})$

= (defining property of identity matrix)

(11·11.2) $\mathbf{P}^{-1}\mathbf{P}$

= (defining property of matrix inverse)

(11·11.3) $\mathbf{I}_n$.

Hence the result. □

11·12. Theorem. *Similar $n \times n$ matrices $\mathbf{A} \sim \mathbf{B}$ have the same eigenvalues.*

Proof. Let $\mathbf{P}$ be such that $\mathbf{A} = \mathbf{P}^{-1}\mathbf{B}\mathbf{P}$. We will prove the characteristic polynomial for $\mathbf{A}$ is the same as for $\mathbf{B}$. We just unfold the characteristic polynomial for $\mathbf{B}$,

$p_{\mathbf{B}}(\lambda)$

= (definition of characteristic polynomial)

(11·12.1) $\det(\lambda\mathbf{I}_n - \mathbf{B})$

= (unfolding definition of $\mathbf{B}$)

(11·12.2) $\det(\lambda\mathbf{I}_n - \mathbf{P}^{-1}\mathbf{A}\mathbf{P})$

= (identity matrix is always similar to itself)

(11·12.3) $\det(\lambda\mathbf{P}^{-1}\mathbf{I}_n\mathbf{P} - \mathbf{P}^{-1}\mathbf{A}\mathbf{P})$

= (distributivity)

(11·12.4) $\det(\mathbf{P}^{-1}(\lambda\mathbf{I}_n - \mathbf{A})\mathbf{P})$

= (determinant of product is product of determinants)

(11·12.5) $\det(\mathbf{P}^{-1})\det(\lambda\mathbf{I}_n - \mathbf{A})\det(\mathbf{P})$

= (commutativity of multiplication of numbers)

(11·12.6) $\det(\lambda\mathbf{I}_n - \mathbf{A})\det(\mathbf{P}^{-1})\det(\mathbf{P})$

= (product of determinants is determinant of product)

(11·12.7) $\det(\lambda\mathbf{I}_n - \mathbf{A})\det(\mathbf{P}^{-1}\mathbf{P})$

= (definition of matrix inverse)

(11·12.8) $\det(\lambda\mathbf{I}_n - \mathbf{A})\det(\mathbf{I})$

= (determinant of identity matrix is 1)

(11·12.9) $\det(\lambda\mathbf{I}_n - \mathbf{A})$

= (definition of characteristic polynomial)

(11·12.10) $p_{\mathbf{A}}(\lambda)$

Then $\mathbf{A}$ and $\mathbf{B}$ have identical characteristic polynomials and, moreover, this means they have identical eigenvalues. □

11·13. Theorem. *An $n \times n$ matrix $\mathbf{A}$ can be diagonalized if and only if it has n linearly independent eigenvectors.*

Proof. ($\implies$) Assume $\mathbf{A}$ can be diagonalized. Then there exists an invertible matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that

$$\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}. \tag{11·13.1a}$$

We can multiply both sides on the left by $\mathbf{P}$ to get

$$\mathbf{A}\mathbf{P} = \mathbf{P}\mathbf{D}. \tag{11·13.1b}$$

If $\mathbf{P} = (\boldsymbol{p}_1|\dots|\boldsymbol{p}_n)$ is written out as n column vectors, and if $\mathbf{D} = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$, then we have our equation become:

$$(\mathbf{A}\boldsymbol{p}_1|\dots|\mathbf{A}\boldsymbol{p}_n) = (\lambda_1\boldsymbol{p}_1|\dots|\lambda_n\boldsymbol{p}_n). \tag{11·13.1c}$$

This is a system of n eigenvectors $\boldsymbol{p}_1, \dots, \boldsymbol{p}_n$ and n eigenvalues $\lambda_1, \dots, \lambda_n$. Since $\mathbf{P}$ is invertible, its columns are linearly independent by Corollary 9·6. Hence the columns of $\mathbf{P}$ (which are the eigenvectors of $\mathbf{A}$) form a basis and, in particular, are all nonzero.

($\impliedby$) Assume $\mathbf{A}$ has n linearly independent eigenvectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ with associated eigenvalues $\lambda_1, \dots, \lambda_n$. Construct the matrix

$$\mathbf{P} = (\boldsymbol{x}_1 \mid \cdots \mid \boldsymbol{x}_n). \tag{11·13.2a}$$

The columns of $\mathbf{P}$ are linearly independent, hence $\mathbf{P}$ is invertible by Corollary 9·6. We find

$$\mathbf{A}\mathbf{P} = (\mathbf{A}\boldsymbol{x}_1 \mid \cdots \mid \mathbf{A}\boldsymbol{x}_n) \tag{11·13.2b}$$

and since the $\boldsymbol{x}_i$ are all eigenvectors, we have,

$$\mathbf{A}\mathbf{P} = (\lambda_1\boldsymbol{x}_1 \mid \cdots \mid \lambda_n\boldsymbol{x}_n). \tag{11·13.2c}$$

But in the first half of the proof, we saw the right-hand side is precisely equal to $\mathbf{P}\mathbf{D}$ where $\mathbf{D} = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$. This establishes $\mathbf{A} \sim \mathbf{D}$ and that $\mathbf{A}$ is diagonalizable. □

11·13.1. *Remark.* We accidentally proved too much in the forward direction. Namely, we established the eigenvectors form a basis.

11·14. Theorem. *If the roots of the characteristic polynomial for an $n \times n$ matrix $\mathbf{A}$ are all distinct (i.e., there are n distinct roots with no duplicates), then $\mathbf{A}$ is diagonalizable.*

In other words, if $\mathbf{A}$ has n distinct eigenvalues, then $\mathbf{A}$ is diagonalizable.

Proof. Let $\mathbf{A}$ have eigenvalues $\lambda_1, \dots, \lambda_n$ and associated eigenvectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$. Our goal is to prove the eigenvectors are linearly independent (since they would form the columns of a matrix $\mathbf{P}$, as outlined in the proof of the previous theorem).

Assume for contradiction that the eigenvectors are not all linearly independent. Then we can find some $\boldsymbol{x}_j$ which is a linear combination of the vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{j-1}$ and that these $j-1$ vectors $S = \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_{j-1}\}$ are linearly independent.

So we find

$$\boldsymbol{x}_j = c_1\boldsymbol{x}_1 + \cdots + c_{j-1}\boldsymbol{x}_{j-1}. \tag{11·14.1}$$

This is the first step.

Now we multiply on the left of both sides of Eq (11·14.1) by $\mathbf{A}$ which gives us

$$\mathbf{A}\boldsymbol{x}_j = c_1\mathbf{A}\boldsymbol{x}_1 + \cdots + c_{j-1}\mathbf{A}\boldsymbol{x}_{j-1}. \tag{11·14.2}$$

But these are eigenvectors, so we can plug in their eigenvalues

$$\lambda_j\boldsymbol{x}_j = c_1\lambda_1\boldsymbol{x}_1 + \cdots + c_{j-1}\lambda_{j-1}\boldsymbol{x}_{j-1}. \tag{11·14.3}$$

This is the second step.

Now we return to Eq (11·14.1), and multiply both sides by λ_j

$$\lambda_j \boldsymbol{x}_j = c_1\lambda_j \boldsymbol{x}_1 + \cdots + c_{j-1}\lambda_j \boldsymbol{x}_{j-1}. \tag{11·14.4}$$

We subtract from this equation the result of our second step, i.e., Eq (11·14.3)

$$\mathbf{0} = \lambda_j \boldsymbol{x}_j - \lambda_j \boldsymbol{x}_j \tag{11·14.5a}$$
$$= (c_1\lambda_j \boldsymbol{x}_1 + \cdots + c_{j-1}\lambda_j \boldsymbol{x}_{j-1}) - (c_1\lambda_1 \boldsymbol{x}_1 + \cdots + c_{j-1}\lambda_{j-1} \boldsymbol{x}_{j-1}) \tag{11·14.5b}$$
$$= c_1(\lambda_j - \lambda_1)\boldsymbol{x}_1 + \cdots + c_{j-1}(\lambda_j - \lambda_{j-1})\boldsymbol{x}_{j-1}. \tag{11·14.5c}$$

We see for this to work, we need every term to vanish. Since $\boldsymbol{x}_i \neq \mathbf{0}$ for every $i = 1, \dots, n$, we need the coefficients to vanish. But since $\lambda_j \neq \lambda_i$ for $i \neq j$, it would be impossible for $\lambda_j - \lambda_i = 0$. We are forced to conclude that $c_i = 0$ for $i = 1, \dots, j-1$.

This contradicts the assumption that the eigenvectors are linearly dependent, and we conclude they are all linearly independent. Then by Theorem 11·13 it follows $\mathbf{A}$ is diagonalizable. □

11·15. Importance of diagonalizable matrices. If $\mathbf{A}$ is diagonalizable, then $\mathbf{A} = \mathbf{PDP}^{-1}$. We see

$\mathbf{A}^2$

= (unfolding $\mathbf{A}$)

(11·15.1a) $(\mathbf{PDP}^{-1})(\mathbf{PDP}^{-1})$

= (associativity of matrix multiplication)

(11·15.1b) $\mathbf{P}\left(\mathbf{D}(\mathbf{P}^{-1}\mathbf{P})\mathbf{D}\right)\mathbf{P}^{-1}$

= (defining property of matrix inverse)

(11·15.1c) $\mathbf{P}\left(\mathbf{DID}\right)\mathbf{P}^{-1}$

= (defining property of identity matrix)

(11·15.1d) $\mathbf{P}\left(\mathbf{DD}\right)\mathbf{P}^{-1}$

= (definition of matrix power)

(11·15.1e) $\mathbf{PD}^2\mathbf{P}^{-1}$

We can similarly find

$\mathbf{A}^3$

= (unfolding definition of matrix power)

(11·15.2a) $\mathbf{A}^2\mathbf{A}$

= (unfolding definition of $\mathbf{A}$ and previous calculation)

(11·15.2b) $(\mathbf{PD}^2\mathbf{P}^{-1})(\mathbf{PDP}^{-1})$

= (associativity of matrix multiplication)

(11·15.2c) $\mathbf{P}\left(\mathbf{D^2}(\mathbf{P}^{-1}\mathbf{P})\mathbf{D}\right)\mathbf{P}^{-1}$

= (defining property of matrix inverse)

(11·15.2d) $\mathbf{P}\left(\mathbf{D}^2\mathbf{ID}\right)\mathbf{P}^{-1}$

= (defining property of identity matrix)

(11·15.2e) $\mathbf{P}\left(\mathbf{D}^2\mathbf{D}\right)\mathbf{P}^{-1}$

= (definition of matrix power)

(11·15.2f) $\mathbf{P}\mathbf{D}^{3}\mathbf{P}^{-1}$.

The pattern is clear, now; if we assume (the so-called "inductive hypothesis"), for arbitrary $n \in \mathbb{N}$,

$$\mathbf{A}^{n} = \mathbf{P}\mathbf{D}^{n}\mathbf{P}^{-1}. \tag{11·15.3}$$

Then we have

$\mathbf{A}^{n+1}$

= (unfolding definition of matrix power)

(11·15.4a) $\mathbf{A}^{n}\mathbf{A}$

= (unfolding definition of $\mathbf{A}$ and inductive hypothesis)

(11·15.4b) $(\mathbf{P}\mathbf{D}^{n}\mathbf{P}^{-1})(\mathbf{P}\mathbf{D}\mathbf{P}^{-1})$

= (associativity of matrix multiplication)

(11·15.4c) $\mathbf{P}\left(\mathbf{D}^{\mathbf{n}}(\mathbf{P}^{-1}\mathbf{P})\mathbf{D}\right)\mathbf{P}^{-1}$

= (defining property of matrix inverse)

(11·15.4d) $\mathbf{P}\left(\mathbf{D}^{n}\mathbf{I}\mathbf{D}\right)\mathbf{P}^{-1}$

= (defining property of identity matrix)

(11·15.4e) $\mathbf{P}\left(\mathbf{D}^{n}\mathbf{D}\right)\mathbf{P}^{-1}$

= (definition of matrix power)

(11·15.4f) $\mathbf{P}\mathbf{D}^{n+1}\mathbf{P}^{-1}$.

This is an inductive proof for the claim:

$$\boxed{\mathbf{A}^{n} = \mathbf{P}\mathbf{D}^{n}\mathbf{P}^{-1}.} \tag{11·15.5}$$

CAUTION: not all invertible matrices are diagonalizable. Do not make this mistake! The following example provides a counter-example.

11·16. Example. The matrix

$$\mathbf{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{11·16.1}$$

is not diagonalizable in $\mathrm{Mat}(\mathbb{R}; 2)$.

Proof. We see the characteristic polynomial for $\mathbf{J}$ is

$$p(\lambda) = \det\begin{pmatrix} -\lambda & -1 \\ 1 & -\lambda \end{pmatrix} = \lambda^{2} + 1. \tag{11·16.2}$$

This has roots at $\lambda_{\pm} = \pm\sqrt{-1}$, which is not a real number. In $(\mathbb{C}; 2)$, we could diagonalize $\mathbf{J}$ with eigenvectors $\boldsymbol{v}_{+} = (\mathrm{i}, 1)$ and $\boldsymbol{v}_{-} = (-\mathrm{i}, 1)$. There is no way to construct a matrix $\mathbf{P} \in \mathrm{Mat}(\mathbb{R}; 2)$ that would diagonalize $\mathbf{J}$. □

11·17. Puzzle. When will a real $n \times n$ matrix be diagonalizable?

11·18. Lemma. *Let $\mathbf{A}$ be a real $n \times n$ matrix. If $\mathbf{A}$ is symmetric (i.e., $\mathbf{A} = \mathbf{A}^{\mathsf{T}}$), then eigenvectors associated with distinct eigenvalues are orthogonal.*

Proof. Assume $\mathbf{A}$ is symmetric. We will prove the eigenvectors (associated with distinct eigenvalues) of $\mathbf{A}$ are orthogonal. Let λ_i, λ_j be eigenvalues with respective eigenvectors $\boldsymbol{x}_i$, $\boldsymbol{x}_j$ which are distinct $\lambda_i \neq \lambda_j$. Then

$\lambda_i(\boldsymbol{x}_i \cdot \boldsymbol{x}_j)$

= (compatibility of scalar multiplication and dot product)

(11·18.1) $(\lambda_i \boldsymbol{x}_i)\cdot\boldsymbol{x}_j$

= (since $\boldsymbol{x}_i$ is an eigenvector with eigenvalue λ_i)

(11·18.2) $(\mathbf{A}\boldsymbol{x}_i)\cdot\boldsymbol{x}_j$

= (definition of dot product using matrices)

(11·18.3) $(\mathbf{A}\boldsymbol{x}_i)^{\mathsf{T}}\boldsymbol{x}_j$

= (transpose of product is reverse product of transposes)

(11·18.4) $(\boldsymbol{x}_i^{\mathsf{T}}\mathbf{A}^{\mathsf{T}})\boldsymbol{x}_j$

= (associativity of matrix multiplication, and restore dot product)

(11·18.5) $\boldsymbol{x}_i\cdot(\mathbf{A}^{\mathsf{T}}\boldsymbol{x}_j)$

= (since $\mathbf{A}$ is symmetric)

(11·18.6) $\boldsymbol{x}_i\cdot(\mathbf{A}\boldsymbol{x}_j)$

= (since $\boldsymbol{x}_j$ is an eigenvalue)

(11·18.7) $\boldsymbol{x}_i\cdot(\lambda_j\boldsymbol{x}_j)$

= (scalar multiplication is compatible with dot product)

(11·18.8) $\lambda_j(\boldsymbol{x}_i\cdot\boldsymbol{x}_j)$

then we have (subtracting one side from the other)

$$(\lambda_i-\lambda_j)(\boldsymbol{x}_i\cdot\boldsymbol{x}_j)=0. \tag{11·18.9}$$

Either $\lambda_i=\lambda_j$ or $\boldsymbol{x}_i\cdot\boldsymbol{x}_j=0$. But we assumed the eigenvalues are distinct, so $\lambda_i\neq\lambda_j$. Hence $\boldsymbol{x}_i\cdot\boldsymbol{x}_j=0$ as desired. □

11·19. Theorem (Fundamental Theorem of Algebra)**.** *Any polynomial of degree n $p(x)=p_0+p_1x+p_2x^2+\cdots+x^n$ may be factorized as a product of its roots $p(x)=(x-x_1)(x-x_2)(\cdots)(x-x_n)$.*

I am taking this as "given", its proof lies outside the scope of these notes. In upcoming notes on intermediate linear algebra, a proof will be given.

11·20. Definition. Let $\mathbf{A}$ be an $n\times n$ matrix. We say an eigenvalue λ_j of $\mathbf{A}$ has **"Multiplicity"** k_j if the characteristic polynomial of $\mathbf{A}$ has k_j factors of $(\lambda-\lambda_j)$ appearing in it, i.e.,

$$p(\lambda)=(\lambda-\lambda_j)^{k_j}\prod_{\substack{i\neq j\\ \lambda_i\neq\lambda_j}}^{n-k_j}(\lambda-\lambda_i) \tag{11·20.1}$$

11·21. Definition. Let $\mathbf{A}$ be an $n\times n$ matrix with eigenvalue λ_j. We define the **"Eigenspace"** of $\mathbf{A}$ for eigenvalue λ_j to be the kernel of $\lambda_j\mathbf{I}-\mathbf{A}$ (or, equivalently, the span of all vectors whose eigenvalue is λ_j).

11·21.1. *Remark* (Checking the definition). We see this is a "good definition", since a vector $\boldsymbol{v}$ is an eigenvector (or linear combination of eigenvectors) with eigenvalue λ, then $\mathbf{A}\boldsymbol{v}=\lambda\mathbf{I}\boldsymbol{v}$ or equivalently $(\mathbf{A}-\lambda\mathbf{I})\boldsymbol{v}=\mathbf{0}$. Hence $\boldsymbol{v}\in\ker(\mathbf{A}-\lambda\mathbf{I})$. This matches our intuition of an "eigenspace", we should prove that it is actually a subspace (hence actually merits the suffix "-space").

11·22. Lemma. *If λ_j is an eigenvalue of $\mathbf{A}$ with multiplicity k_j, then its eigenspace has dimension $k_j=\dim(\ker(\lambda_j\mathbf{I}-\mathbf{A}))$.*

11·23. Lemma. *If $\mathbf{A}$ is an $n\times n$ matrix with eigenvalue λ and two linearly independent eigenvectors $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ both with eigenvalue λ, then $\boldsymbol{v}_2-(\boldsymbol{v}_2\cdot\widehat{\boldsymbol{v}}_1)\widehat{\boldsymbol{v}}_1$ is an eigenvector of $\mathbf{A}$ with eigenvalue λ.*

Proof. We find by direct computation,

$$\mathbf{A}(\boldsymbol{v}_2 - (\boldsymbol{v}_2 \cdot \widehat{\boldsymbol{v}}_1)\widehat{\boldsymbol{v}}_1)$$

= (distributivity)

$$\mathbf{A}\boldsymbol{v}_2 - \mathbf{A}(\boldsymbol{v}_2 \cdot \widehat{\boldsymbol{v}}_1)\widehat{\boldsymbol{v}}_1 \tag{11·23.1}$$

= (since $\boldsymbol{v}_2$ is an eigenvector)

$$\lambda\boldsymbol{v}_2 - \mathbf{A}(\boldsymbol{v}_2 \cdot \widehat{\boldsymbol{v}}_1)\widehat{\boldsymbol{v}}_1 \tag{11·23.2}$$

= (linearity)

$$\lambda\boldsymbol{v}_2 - (\boldsymbol{v}_2 \cdot \widehat{\boldsymbol{v}}_1)\mathbf{A}\widehat{\boldsymbol{v}}_1 \tag{11·23.3}$$

= (since $\widehat{\boldsymbol{v}}_1$ is an eigenvector)

$$\lambda\boldsymbol{v}_2 - (\boldsymbol{v}_2 \cdot \widehat{\boldsymbol{v}}_1)\lambda\widehat{\boldsymbol{v}}_1 \tag{11·23.4}$$

= (commutativity of multiplication for numbers)

$$\lambda\boldsymbol{v}_2 - \lambda(\boldsymbol{v}_2 \cdot \widehat{\boldsymbol{v}}_1)\widehat{\boldsymbol{v}}_1 \tag{11·23.5}$$

= (distributivity)

$$\lambda(\boldsymbol{v}_2 - (\boldsymbol{v}_2 \cdot \widehat{\boldsymbol{v}}_1)\widehat{\boldsymbol{v}}_1) \tag{11·23.6}$$

Hence we conclude $(\boldsymbol{v}_2 - (\boldsymbol{v}_2 \cdot \widehat{\boldsymbol{v}}_1)\widehat{\boldsymbol{v}}_1)$ is an eigenvector of $\mathbf{A}$ with eigenvalue λ. ☐

11·23.1. *Remark.* As an immediate corollary to this, we can apply the Graham–Schmidt algorithm (§9·26) to eigenvectors of the same eigenvalue λ to construct an orthonormal basis for the eigenspace of λ.

11·24. Theorem (Spectral theorem for real matrices)**.** *Let* $\mathbf{A}$ *be a real* $n \times n$ *matrix. Assume* $\det(\mathbf{A}) \neq 0$*. Then* $\mathbf{A}$ *is diagonalizable by an orthogonal matrix* $\mathbf{P}$ *(i.e.,* $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$ *where* $\mathbf{D}$ *is diagonal) if and only if* $\mathbf{A}$ *is symmetric, that is,*

$$\mathbf{A} = \mathbf{A}^{\mathsf{T}}. \tag{11·24.1}$$

Proof. ($\Longrightarrow$) Assume $\mathbf{A}$ is diagonalizable, so $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$ where $\mathbf{P}$ is orthogonal. Then $\mathbf{P}^{-1} = \mathbf{P}^{\mathsf{T}}$. Then $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{\mathsf{T}}$ is clearly symmetric, since $\mathbf{A}^{\mathsf{T}} = (\mathbf{P}^{\mathsf{T}})^{\mathsf{T}}\mathbf{D}\mathbf{P}^{\mathsf{T}}$. Recall the transpose is idempotent $(\mathbf{P}^{\mathsf{T}})^{\mathsf{T}} = \mathbf{P}$ which implies $\mathbf{A}^{\mathsf{T}} = \mathbf{P}\mathbf{D}\mathbf{P}^{\mathsf{T}} = \mathbf{A}$. Hence $\mathbf{A}$ is symmetric.

($\Longleftarrow$) Assume $\mathbf{A}$ is symmetric. For each eigenvalue λ_j of multiplicity $k_j > 1$ (i.e., there are $k_j > 1$ linearly independent eigenvectors with the same eigenvalue λ_j), we find k_j linearly independent eigenvectors.

Then applying our beloved Graham–Schmidt algorithm (§9·26), we transform these eigenvectors into orthonormal vectors for the eigenspace.

Then we have the eigenvectors for distinct eigenvalues be orthogonal by Lemma 11·18, and we have just constructed orthonormal eigenvectors when they share the same eigenvalue, and taken altogether these form an orthonormal basis. These form the columns of matrix $\mathbf{P}$, which is an orthogonal matrix (§9·22), and we have $\mathbf{D} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{P}^{\mathsf{T}}\mathbf{A}\mathbf{P}$ be the diagonal matrix of eigenvalues. Then we have the data for diagonalizing $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{T}$. ☐

11.3 Matrix Exponential

11·25. Matrix Exponential. In particular, we can define the matrix exponential as

$$\exp(\mathbf{A}) = \mathbf{P}\exp(\mathbf{D})\mathbf{P}^{-1} \tag{11·25.1}$$

where

$$\exp(\mathbf{D}) = \operatorname{diag}(\exp(d_1), \ldots, \exp(d_n)) \tag{11·25.2}$$

the matrix exponential of the diagonal matrix is just the diagonal of exponentials.

If further $\mathbf{D}$ consists of strictly positive entries, we could define the matrix logarithm as

$$\log(\mathbf{A}) = \mathbf{P}\log(\mathbf{D})\mathbf{P}^{-1} \tag{11·25.3}$$

where, again, the matrix logarithm of the diagonal is just the component-wise logarithm of its entries,

$$\log(\mathbf{D}) = \operatorname{diag}(\log(d_1), \dots, \log(d_n)). \tag{11·25.4}$$

11·26. Theorem. *For any matrix* $\mathbf{A}$*, we have*

$$\det(\exp(\mathbf{A})) = \mathrm{e}^{\operatorname{tr}(\mathbf{A})}. \tag{11·26.1}$$

Proof. We see that $\exp(\mathbf{A}) = \mathbf{P}\exp(\mathbf{D})\mathbf{P}^{-1}$ has eigenvalues e^{λ_j} where λ_j are the eigenvalues of $\mathbf{A}$. Then by Lemma 11·9,

$$\det(\exp(\mathbf{A})) = \prod_{j=1}^{n} \mathrm{e}^{\lambda_j} \tag{11·26.2}$$

and the right-hand side can be written as

$$\det(\exp(\mathbf{A})) = \mathrm{e}^{\sum_{j=1}^{n}\lambda_j}. \tag{11·26.3}$$

But by Lemma 11·9,

$$\begin{aligned}\det(\exp(\mathbf{A})) &= \mathrm{e}^{\sum_{j=1}^{n}\lambda_j}\\ &= \mathrm{e}^{\operatorname{tr}(\mathbf{A})}.\end{aligned} \tag{11·26.4}$$

Hence the result. □

11·26.1. *Remark.* In quantum field theory, we often work with infinite-dimensional vector spaces (like the smooth functions on spacetime). Linear operators on these vector spaces include derivatives. For peculiar reasons, physicists want to compute the "determinant" of the differentiation operator. The previous theorem offers one way to approach such a concept. We could define "eigenfunctions" for a differential operator D as $D(f) = \lambda f$, then the trace is just the sum over all eigenvalues. We could define $\det(\exp(D)) = \exp(\sum\lambda)$, for example. This is done more precisely with zeta functions, and is known as the zeta functional regularization of the functional determinant.

11·27. Corollary. *For any matrix* $\mathbf{A}$ *with real or complex entries, we have* $\exp(\mathbf{A})$ *be nonsingular.*

Proof. We see $\operatorname{tr}(\mathbf{A})$ is finite — call it $z = \operatorname{tr}(\mathbf{A})$ — and by the previous theorem

$$\det(\exp(\mathbf{A})) = \mathrm{e}^{\operatorname{tr}(\mathbf{A})} = \mathrm{e}^{z}. \tag{11·27.1}$$

But $\mathrm{e}^{z} \neq 0$ ever for $z \in \mathbb{C}$ (or $z \in \mathbb{R}$), which means the determinant of $\exp(\mathbf{A})$ is never zero. Hence $\exp(\mathbf{A})$ must be invertible. □

11·28. Analytic Function of a Matrix. More generally, if $f\colon \mathbb{R} \to \mathbb{R}$ is a function with a Taylor series about x_0 given by

$$f(x_0 + h) = \sum_{n=0}^{\infty} \frac{a_n}{n!} h^n, \tag{11·28.1}$$

then it may be applied to a diagonalizable matrix $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$ provided every entry of $\mathbf{D}$ lies within the neighborhood of convergence for the Taylor series. If $\mathbf{D} = \operatorname{diag}(x_0 + d_1, \dots, x_0 + d_n)$, then

$$f(\mathbf{A}) = \mathbf{P} f(\mathbf{D})\mathbf{P}^{-1} \tag{11·28.2}$$

where $f(\mathbf{D}) = \operatorname{diag}(f(x_0 + d_1), \dots, f(x_0 + d_n))$. This follows from $\mathbf{A}^n = \mathbf{P}\mathbf{D}^n\mathbf{P}^{-1}$ for every $n \in \mathbb{N}_0$ and just plugging it into the series expansion.

12 Conclusion: The End?

> *If stories have ends, then this story ends here.*
> *I think, though it is not my field of specialisation, that some stories end, but others carry on. They are eternal. They secretly carry on after the story appears to be finished, continuing in silence. These stories do not talk. They are never heard. I think my story may be like that.*
>
> Dan Abnett, *Saturnine* (2020)

12·1. We've come quite a ways from "solving a system of linear equations", wading through not just one, but two new abstractions: matrix algebras and vector spaces. The destination for elementary linear algebra is always the spectral theorem for real matrices — a symmetric square real matrix is diagonalizable.

The next topics of discussion would be, well, what do we do with a real square matrix which is not symmetric? Can we get it into a "diagonal-ish" form?

12·2. Other Number Fields. The other direction for discussion is, we have been working with *real* matrices, *real* vector spaces, everything using the *real* numbers. What if we used the complex numbers instead? We need to abstract away the notion of the dot product and use something similar, called the *inner product*. The spectral theorem holds for complex matrices, but with some slight changes.

If I ever get around to it, this is the subject of my notes on *intermediate linear algebra*: now, *right now*, having finished reading the previous sections, you know how to multiply the hell out of matrices. We can use this knowledge as a "toy model" to demonstrate how mathematicians present knowledge and figure out what theorems to prove.

12·3. Numerical Linear Algebra. There is also a lot of nuance behind the calculations we do on the computer, especially with linear algebra. This opens up an exciting new field to us: numerical linear algebra. Furthermore, this may be studied as a gateway to functional analysis. It is beautiful, and there are many lovely good books on the subject.

12·4. Functional Analysis. If the reader knows real analysis,[4] then the reader will be aware that many definitions could be applied to square matrices. Conversely, if we view indices as function arguments, so $v\colon \{1,2,3\} \to \mathbb{R}$ sends $j \in \{1,2,3\}$ to a real number denoted v_j — well, what is stopping us from changing the domain to, say, an open interval? Or all of $\mathbb{R}$? Or $\mathbb{R}^n$? From this perspective, we can look at a real-valued function $f(\boldsymbol{x})$ as a vector and $\boldsymbol{x}$ as a dummy variable. What does the dot product look like in this case? Matrix multiplication? Presumably, "sums are replaced by integrals", but are there bases?

Since it's usually hard to reason about infinities, we could view numerical linear algebra as "finite functional analysis". The two complement each other like peanut butter and jelly.

12·5. Goodbye. Wow, look how far we've come! You could see your house from here. And you didn't even complain once. Or maybe you did, I can't say, I can't hear that well...

Dixi.

[4] For readers who do not know real analysis but want to learn it, I recommend starting with Stephen Abott's *Understanding Analysis* as your first book.

Part IV
Appendices

A Set Theory in a Nutshell

A.1. Modern mathematics is based on [Zermelo–Frankel] set theory. We will review the notation and properties here without proof. We also present this as a "naive set theory" using words instead of dry logic notation. The interested reader is encouraged to read Halmos' *Naive Set Theory* for a more in-depth treatment.

A.2. "Definition". A set is a "well-defined" unordered collection of "stuff" (possibly other sets, possibly numbers, or matrices, or whatever). We define a set in terms of its members, and we denote "x is a member of a set A" by writing "$x \in A$" (or rarely, "$A \ni x$" for "A contains element x").

If we have an element x which does not belong to A, we write this as $x \notin A$.

Note: "$\in$" (and "$\notin$") take an object to its left, a set to its right, and produces a proposition (or "formula").

A.3. "Well-Definedness". Although we didn't specify what exactly a "well-defined unordered collection" means, we can loosely describe it by the law that there are no circular chains of elements: so things like $A_1 \in A_2 \in \cdots \in A_1$ are illegal. It is grammatically fine, but so is the sentence "Colorless green ideas sleep furiously".

A consequence to this is we cannot form the *set* of all sets (why would anyone want to?). Instead, we construct a "bigger" species of collections known as "classes", whose members are sets. This leads us to things like NBG axioms (or Morse–Kelly axioms) for set theory. In every sense possible, it's beyond the scope of any concern involving sets, especially our own.

A.4. What's allowed as an element. Any *object* is allowed as an element: sets, functions, numbers, matrices, vectors, spaces, points, etc. We can combine any of these things together into a set — there is no "type restriction" saying we cannot combine a set of numbers with a set of matrices.

However, propositions, predicates, truth-hood, falsehood, etc., are not allowed.

If we were studying a language, its words could be elements of a set. The word "truth" within the language may be an element of a set. But this is different than *truth.* This is the situation with a finger pointing at the moon, and the actual moon itself.

A.4.1. *Remark.* It may be circular to say, "Sets are collections of objects" and "Objects are whatever we can permit as elements of sets"... and you'd be right. The general heuristic is, a proposition is something which is true or false, a predicate is something which takes an object [or several objects] and produces a proposition, and an object is everything else.

A.4.2. *Remark* (Sets are objects). Sets are objects, of course. When discussing the syntax ("grammar") of the notation, we may specifically restrict inputs to be sets of some kind. We did this by stating "$\in$" expects a set to its right (as opposed to an arbitrary object is allowed to its left).

A.5. Notation. We distinguish predicates from functions by writing predicates with square brackets $P[x]$ whereas functions use parentheses $f(x)$.

A.6. Subsets. We can encode the idea of one set being entirely contained in another as follows: if every $a \in A$ satisfies $a \in B$, then A is called a **"Subset"** of B and we write $A \subseteq B$. If further there exists at least one $b \in B$ such that $b \notin A$, then we call A a **"Proper Subset"** of B and indicate this by $A \subset B$. Otherwise we sometimes call B an *improper subset* of A. The reader should be careful, not all authors distinguish proper subsets from improper subsets.

Again, the symbol "$\subseteq$" takes one set to its left, a set to its right, and produces a proposition.

A.7. Theorem. *Every set is a subset of itself: For every set A, $A \subseteq A$.*

A.8. Theorem. *If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

For example: "Every cat is a mammal, and every mammal is an animal, it follows every cat is an animal".

A.9. Set Equality. We call two sets A and B **"Equal"** if every element $a \in A$ also belongs to B, and if every element $b \in B$ also belongs to A. In this case, we write $A = B$.

On the other hand, if there exists an $a \in A$ such that $a \notin B$, or if there exists a $b \in B$ such that $b \notin A$, then we write $A \neq B$ to indicate A is not equal to B.

A.10. Theorem. *Set equality is an equivalence relation, i.e., satisfies all of the following:*

1. *Reflexivity: for any set A, $A = A$*
2. *Symmetry: for any set A and B, if $A = B$, then $B = A$*
3. *Transitivity: for any sets A, B, C, if $A = B$ and $B = C$, then $A = C$.*

A.11. Theorem. *Let A and B be sets. Then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.*

A.12. For a set consisting of finitely many elements, we can write the set explicitly as a comma separated list of its elements sandwiched between squiggle braces:

$$A = \{x_1, x_2, \dots, x_n\}. \tag{A.12.1}$$

Usually this is tedious, so we try to write a description of sets in other ways.

A.13. Empty Set. The set with zero elements is called the empty set, and denoted $\emptyset = \{\}$. The empty set is always a subset of everything: for any set A, we have $\emptyset \subseteq A$.

A.14. Famous Sets. We have the following notation for familiar sets:

1. $\mathbb{N} = \{1, 2, 3, \dots\}$ for the natural numbers (i.e., positive integers)
2. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ for the integers
3. $\mathbb{Q}$ for the rational numbers
4. $\mathbb{R}$ for the real numbers
5. $\mathbb{C}$ for the complex numbers

We typically assume $\mathbb{N} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{R} \subseteq \mathbb{C}$.

A.15. Union (merging sets). If A and B are sets, then we can form a new set $A \cup B$ whose elements are precisely those that belong either to A or to B (or both). So every $a \in A$ also belongs to $a \in A \cup B$, and every $b \in B$ also belongs to $b \in A \cup B$.

A.16. Example. We can write $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$ for the non-negative integers. We see $\mathbb{N} \subseteq \mathbb{N}_0$ is a proper subset.

A.17. Intersection. If A and B are sets, then we can form the collection $A \cap B$ of elements belonging to both A and B: $x \in A \cap B$ if and only if $x \in A$ and $x \in B$.

When $A \cap B = \emptyset$, there are no elements that belong to *both* A and B, then we call A and B **"Disjoint"**.

A.18. Functions. If A and B are sets, then we can define a **"Function"** $f \colon A \to B$ to be such that for each $a \in A$ there is exactly one $b \in B$ such that $b = f(a)$.

A.19. Ordered Pair. We can define an ordered pair (a, b) to be such that $(a, b) = (x, y)$ if and only if $a = x$ and $b = y$. We can generalize this idea from a pair to a tuple of n guys $(a_1, a_2, \dots, a_n)$ defined such that $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n)$ if and only if $a_1 = b_1$ and $a_2 = b_2$ and … and $a_n = b_n$.

A.20. Cartesian Product. If we have sets A and B, we can define the collection of ordered pairs (a, b) for each $a \in A$ and for each $b \in B$. This is precisely the Cartesian product $A \times B$. We have $(a, b) \in A \times B$ for each $a \in A$ and $b \in B$.

We can generalize this to as many factors as we want: the set of ordered triples $A \times B \times C$, quadrouples $A \times B \times C \times D$, and so on. This is a bit of an abuse of notation, but it's ok.

A.21. Iterated Products. It's not uncommon to write A^n where $n \in \mathbb{N}$ as a synonym for $A \times A \times \cdots \times A$ (with n factors). For example, we write $\mathbb{R}^n$ all the time.

A.22. Notation. If $f\colon A\times B\to C$, instead of writing $f((a,b))$, we will write $f(a,b)$. This is convention.

A.23. Infix Notation. Sometimes we introduce a function $f\colon A\times B\to C$ with the understanding it is infixed, i.e., we will use it as $a\ f\ b$ instead of $f(a,b)$. This happens a lot with binary operators. I mean, honestly, who thinks $+(a,b)$ makes any sense?

A.24. Composing Functions. If $f\colon A\to B$ and $g\colon B\to C$ are functions, then we may "feed" the "output" of f into g and produce a new function denoted $g\circ f$ (and we read it from right to left). So for any $a\in A$, we have $(g\circ f)(a) = g\,(f(a))$.

This is associative: for any $f\colon A\to B$, $g\colon B\to C$, $h\colon C\to D$, we have $(h\circ g)\circ f = h\circ(g\circ f)$.

A.25. Cardinality: Size of a set. We indicate the number of elements in a finite set A by writing $|A|$. If A has infinitely many elements, we can also write $|A|$, but now $|A|=\infty$.

There are really two infinities we care about in mathematics: countably infinite (when a set is bijective with $\mathbb{N}$, i.e., we can form a sequence enumerating all elements of the set), and uncountably infinite (when it is too large to be enumerated). Though surprising, it is true, that $\mathbb{Z}$ and $\mathbb{Q}$ are countably infinite in size, though $\mathbb{R}$ and $\mathbb{C}$ are uncountably infinite.

A.26. Set Builder Notation. If we want to form a subset of A satisfying elements $a\in A$ some property or formula $P[a]$, then we write this using the notation:

$$\{a\in A \mid P[a]\} \tag{A.26.1}$$

and read this as:

"$\{$"	the set of
"$a\in A$"	the elements $a\in A$
"$\mid$"	such that
"$P[a]$"	a satisfies the property P, i.e., $P[a]$ is true
"$\}$"	[breath].

If we have some function $f\colon A\to B$, we can write

$$\{f(a)\mid a\in A, P[a]\} \tag{A.26.2}$$

or if there's ambiguity

$$\{f(a)\in B\mid a\in A, P[a]\} \tag{A.26.3}$$

We read this as

"$\{$"	the set of
"$f(a)$"	the result of f applied to a
"$\mid$"	such that
"$a\in A$"	the set is generated by every $a\in A$
","	and
"$P[a]$"	a satisfies the property P, i.e., $P[a]$ is true
"$\}$"	[breath].

This notation is fairly standard. Some authors use colons instead of vertical bars to indicate "such that"; other authors use *both* interchangeably.

When there is no constraint on a, we omit the vertical bar. For example, if we wanted to write the set of functions from A to B, we could write $\{f\colon A\to B\}$.

A.26.1. *Remark* (Free variables implicitly universally quantified). When there are free variables, like a in $\{f(a)\mid a\in A, P[a]\}$, we implicitly quantify over them and think "This is the set consisting of $f(a)$ for every a such that $a\in A$ and $P[a]$ holds".

A.27. Notation: Set of Functions. There are two notations to denote the set of functions from A to B, $\{f\colon A\to B\}$.

1. $\mathrm{Hom}(A,B)$ which is borrowed from category theory, and

2. B^A exponential notation, which is confusing.

Sometimes, to emphasize we are thinking of A and B as sets, we write $\mathbf{Set}(A, B)$ or $\mathrm{Hom}_{\mathbf{Set}}(A, B)$ — as opposed to thinking of them as vector spaces, and looking at the set of linear transformations between them, when we would write $\mathbf{Vect}(A, B)$ or $\mathrm{Hom}_{\mathbf{Vect}}(A, B)$ for the set of all linear transformations, emphasizing our intention that they be viewed as vector spaces.

A.28. Concluding Remarks. There are alternative foundations to mathematics, but in practice it doesn't matter much. There are various different axiomatizations to set theory, most of whom concern themselves to incorporating classes (and even *bigger* collections) into the framework. It seems that set theory is a "kludge" designed to work around the shortcomings of first-order logic.[5]

Type theory is gaining attention, but it is quirky enough to avoid discussing it much. It involves a very clever way to encode a proposition as a type, the proof as a term. The disadvantage with type theory lies with discussing "heterogeneous" collections, among other constraints.

Higher-order logic is kind of a "half way" between type theory and set theory. There are two types, one for propositions, the second for "objects".

The honest truth is that mathematicians work with a linear combination of these three foundations without realizing it, or caring. In these notes, we continue this time honored tradition.

[5]For example, quantifiers in first-order logic only quantify over constants, not functions. But if we encode a function as a set of ordered pairs $(x, f(x))$, then a "function of sets" is a constant and may be quantified over.

B Neo-Ricardian Economics

B.1. Matrix form of equations. We can express an economy in terms of its input matrix $\mathbf{A}$, and its output matrix $\mathbf{B}$
$$\mathbf{A}\boldsymbol{x}_n = \mathbf{B}\boldsymbol{x}_{n+1} \tag{B.1.1}$$
where $\boldsymbol{x}_n$ is the stock of commodities at time $t = n$ production cycles (after some initial production cycle), and $\boldsymbol{x}_{n+1}$ is the stock of commodities *after* the production cycle. We are trying to find price vectors $\boldsymbol{p}$ such that
$$\mathbf{A}\boldsymbol{p} = \mathbf{B}\boldsymbol{p}. \tag{B.1.2}$$
We assume that, for each sector i, the total inputs is no less than the amount produced
$$\sum_{j=1}^{n} a_{i,j} \leq \sum_{j=1}^{n} b_{i,j}. \tag{B.1.3}$$
Since usually $\mathbf{B}$ is diagonal, this simplifies to
$$\sum_{j=1}^{n} a_{i,j} \leq b_{j,j}.$$
The trick is to first introduce a new vector
$$\boldsymbol{q} = \mathbf{B}\boldsymbol{p} \implies \boldsymbol{p} = \mathbf{B}^{-1}\boldsymbol{q}, \tag{B.1.4}$$
then rewrite our problem as
$$\mathbf{A}\boldsymbol{p} = \mathbf{B}\boldsymbol{p} \iff \mathbf{A}\mathbf{B}^{-1}\boldsymbol{q} = \boldsymbol{q}. \tag{B.1.5}$$
For a subsistence economy, when no industry sector has an output, this is the situation we are trying to solve.

B.2. Production with a Surplus. When at least one industry sector produces more output than is needed across the entire economy, then there is surplus produced. In this case, there is a rate of profit r, and we are trying to solve the system of equations:
$$(1 + r)\mathbf{A}\boldsymbol{p} = \mathbf{B}\boldsymbol{p}. \tag{B.2.1}$$
We do the same trick, by writing
$$\boldsymbol{q} = \mathbf{B}\boldsymbol{p}, \tag{B.2.2}$$
then plugging this into the equations for an economy with a surplus gives us
$$(1 + r)\mathbf{A}\boldsymbol{p} = \mathbf{B}\boldsymbol{p} \iff (1 + r)\mathbf{A}\mathbf{B}^{-1}\boldsymbol{q} = \boldsymbol{q}. \tag{B.2.3}$$
This is an eigenvalue problem! We divide both sides by $(1 + r)$ to find
$$\mathbf{A}\mathbf{B}^{-1}\boldsymbol{q} = \frac{1}{1 + r}\boldsymbol{q}, \tag{B.2.4}$$
where $\lambda = 1/(1+r)$ is the eigenvalue and $\boldsymbol{q}$ is the eigenvector. We are looking for real λ such that $0 < \lambda \leq 1$ — when $\lambda = 1$, there is no profit $r = 0$; similarly, it is rare to find $r > 1$ (i.e., $\lambda < 1/2$). The real constraint is that every entry of $\boldsymbol{q}$ must be positive (otherwise some commodities have negative value, which makes no sense).

B.3. Example (Sraffa [3, see §5]). Consider the economy given by the equations of production

$$280 \text{ qr. wheat} + 12 \text{ t. iron} \to 575 \text{ qr. wheat} \tag{B.3.1a}$$

$$120 \text{ qr. wheat} + 8 \text{ t. iron} \to 20 \text{ t. iron} \tag{B.3.1b}$$

We have

$$\mathbf{A} = \begin{pmatrix} 280 & 12 \\ 120 & 8 \end{pmatrix}, \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 575 & 0 \\ 0 & 20 \end{pmatrix}, \tag{B.3.2}$$

and

$$\mathbf{AB}^{-1} = \begin{pmatrix} 280/575 & 12/20 \\ 120/575 & 8/20 \end{pmatrix}. \tag{B.3.3}$$

We can find the eigenvalues using the characteristic polynomial

$$p(\lambda) = \left(\frac{280}{575} - \lambda\right)\left(\frac{8}{20} - \lambda\right) - \frac{12}{20}\cdot\frac{120}{575}, \tag{B.3.4}$$

which has solutions $\lambda_1 = 2/23$ and $\lambda_2 = 4/5$. These correspond to $1 + r = 23/2$ and $1 + r = 5/4$ — or $r = 1050\%$ and $r = 25\%$, respectively. The price vectors are

$$\boldsymbol{p}_1 = p_w \begin{pmatrix} 1 \\ -115/6 \end{pmatrix}, \quad \text{and} \quad \boldsymbol{p}_2 = p_w \begin{pmatrix} 1 \\ 15 \end{pmatrix}. \tag{B.3.5}$$

The viable price vector is $\boldsymbol{p}_2$ where the price of 1 ton of iron p_i is equal to the price of 15 quarters of wheat, $p_i = 15p_w$.

B.4. Example (Sraffa [3, see §25]). Consider the more complicated equations of production:

$$200 \text{ qr. wheat} + 40 \text{ t. iron} + 40 \text{ t. coal} \to 480 \text{ qr. wheat} \tag{B.4.1a}$$

$$60 \text{ qr. wheat} + 90 \text{ t. iron} + 120 \text{ t. coal} \to 180 \text{ t. iron} \tag{B.4.1b}$$

$$150 \text{ qr. wheat} + 50 \text{ t. iron} + 125 \text{ t. coal} \to 450 \text{ t. coal} \tag{B.4.1c}$$

Observe the inputs are 410 qr wheat, 285 tons coal, 180 tons iron. We can compute the product $\mathbf{AB}^{-1}$ as

$$\mathbf{AB}^{-1} = \begin{pmatrix} (5/12) & (2/9) & (4/45) \\ (1/8) & (1/2) & (4/15) \\ (5/16) & (5/18) & (5/18) \end{pmatrix}. \tag{B.4.2}$$

This has characteristic polynomial

$$p(\lambda) = \frac{35}{1296} - \frac{\lambda}{3} + \frac{43}{36}\lambda^2 - \lambda^3. \tag{B.4.3}$$

We find its eigenvalues are $\lambda_1 = 5/6$, $\lambda_2 = 7/36$, and $\lambda_3 = 1/6$ which correspond to rates of profit $r_1 = 1/5$, $r_2 = 29/7$, and $r_3 = 5$.

If we consider $r_1 = 1/5$ as the rate of profit, the first equation

$$(6/5)(200p_w + 40p_i + 40p_c) = 480p_w \tag{B.4.4a}$$

may be rewritten as

$$40p_w + 8p_i + 8p_c = 80p_w \tag{B.4.4b}$$

which reduces to

$$p_i + p_c = 5p_w. \tag{B.4.4c}$$

Now if we look at the second equation,

$$(6/5)(60p_w + 90p_i + 120p_c) = 180p_i \tag{B.4.5a}$$

which simplifies to

$$12p_w + 18p_i + 24p_c = 30p_i, \tag{B.4.5b}$$

which gives us

$$p_w + 2p_c = p_i. \tag{B.4.5c}$$

But if we add p_c to both sides,

$$p_w + 3p_c = p_i + p_c, \tag{B.4.6}$$

we can use Eq (B.4.4c) to rewrite the right-hand side as

$$p_w + 3p_c = 5p_w, \tag{B.4.7}$$

hence

$$\boxed{p_c = \frac{4}{3}p_w.} \tag{B.4.8}$$

If we plug this back into Eq (B.4.4c) we find

$$\boxed{p_i = \frac{11}{3}p_w.} \tag{B.4.9}$$

Or if we want it in one big equation

$$\boxed{11p_c = 4p_i = \frac{44}{3}p_w.} \tag{B.4.10}$$

We briefly mention the other choices of the rate of profit leads to negative prices. For example, if we took r_3, the first equation of production gives us

$$6(200p_w + 40p_i + 40p_c) = 480p_w \tag{B.4.11a}$$

which simplifies to

$$5p_w + p_i + p_c = 2p_w \tag{B.4.11b}$$

and thus

$$p_i + p_c = -3p_w. \tag{B.4.11c}$$

If $p_w > 0$, then either $p_i < 0$ or $p_c < 0$. If $p_w < 0$, then $p_w < 0$. Either way, we have negative prices.

For $r_2 = 29/7$, we would have

$$(36/7)(200p_w + 40p_i + 40p_c) = 480p_w \tag{B.4.12a}$$

which reduces to

$$(36/7)(5p_w + p_i + p_c) = 12p_w, \tag{B.4.12b}$$

or equivalently

$$35p_w + 7p_i + 7p_c = \frac{1}{3}p_w \tag{B.4.12c}$$

hence

$$7p_i + 7p_c = -\frac{104}{3}p_w. \tag{B.4.12d}$$

And we're in exactly the same situation as before, we must have a negative price.

B.5. Numerical values. A lot of these examples have nice numerical values. But if we, for example, reduced the surplus of the wheat sector to zero in the previous example, giving us the equations of production:

$$200\text{ qr. wheat} + 40\text{ t. iron} + 40\text{ t. coal} \to 410\text{ qr. wheat} \tag{B.5.1a}$$
$$60\text{ qr. wheat} + 90\text{ t. iron} + 120\text{ t. coal} \to 180\text{ t. iron} \tag{B.5.1b}$$
$$150\text{ qr. wheat} + 50\text{ t. iron} + 125\text{ t. coal} \to 450\text{ t. coal} \tag{B.5.1c}$$

Then the matrix $\mathbf{AB}^{-1}$ has characteristic polynomial

$$p(\lambda) = \frac{35}{1107} - \frac{1679}{4428}\lambda + \frac{467}{369}\lambda^2 - \lambda^3. \tag{B.5.2}$$

The closed form expression for the eigenvalues is rather unpleasant and shockingly involves imaginary quantities

$$\lambda_1 = \frac{467}{1107} + \frac{252805}{2214\sqrt[3]{118352413 + 738\mathrm{i}\sqrt{3946737549}}} + \frac{\sqrt[3]{118352413 + 738\mathrm{i}\sqrt{3946737549}}}{2214} \tag{B.5.3a}$$

$$\begin{aligned}\lambda_2 = \frac{467}{1107} &- \frac{252805}{4428\sqrt[3]{118352413 + 738\mathrm{i}\sqrt{3946737549}}} - \frac{252805\mathrm{i}}{1476\sqrt{3}\sqrt[3]{118352413 + 738\mathrm{i}\sqrt{3946737549}}}\\ &- \frac{\sqrt[3]{118352413 + 738\mathrm{i}\sqrt{3946737549}}}{4428} + \frac{\mathrm{i}\sqrt[3]{118352413 + 738\mathrm{i}\sqrt{3946737549}}}{1476\sqrt{3}}\end{aligned} \tag{B.5.3b}$$

$$\begin{aligned}\lambda_3 = \frac{467}{1107} &- \frac{252805}{4428\sqrt[3]{118352413 + 738\mathrm{i}\sqrt{3946737549}}} + \frac{252805\mathrm{i}}{1476\sqrt{3}\sqrt[3]{118352413 + 738\mathrm{i}\sqrt{3946737549}}}\\ &- \frac{\sqrt[3]{118352413 + 738\mathrm{i}\sqrt{3946737549}}}{4428} - \frac{\mathrm{i}\sqrt[3]{118352413 + 738\mathrm{i}\sqrt{3946737549}}}{1476\sqrt{3}}\end{aligned} \tag{B.5.3c}$$

There is no closed form expression for the eigenvalues of $\mathbf{AB}^{-1}$ *as real numbers.* We need to use numerical approximations:

$$\lambda_1 \approx 0.872546 \tag{B.5.4a}$$
$$\lambda_2 \approx 0.147691 \tag{B.5.4b}$$
$$\lambda_3 \approx 0.245346. \tag{B.5.4c}$$

Only λ_1 corresponds to a rate of profit between 0 and 100% (namely, a rate of profit $r_1 \approx 0.146072$). This gives the exchange rate of

$$p_i(\lambda_1) \approx 2.85062 p_w, \quad \text{and} \quad p_c(\lambda_1) \approx 1.09298 p_w. \tag{B.5.5}$$

If we tried the other rates of profit, we would find

$$p_i(\lambda_2) \approx -3.2122 p_w, \quad \text{and} \quad p_c(\lambda_2) \approx 0.726998 p_w, \tag{B.5.6}$$

which is implausible; and lastly

$$p_i(\lambda_3) \approx -6.33286 p_w, \quad \text{and} \quad p_c(\lambda_3) \approx 2.84669 p_w. \tag{B.5.7}$$

Again, this last case is implausible.

B.6. Perturbing Coal surplus, supply and demand. Suppose we restore the surplus of wheat. If we parametrize the surplus of coal as a variable Δc, then the equations of production become:

$$200\text{ qr. wheat} + 40\text{ t. iron} + 40\text{ t. coal} \to 480\text{ qr. wheat} \tag{B.6.1a}$$

$$60\text{ qr. wheat} + 90\text{ t. iron} + 120\text{ t. coal} \to 180\text{ t. iron} \tag{B.6.1b}$$

$$150\text{ qr. wheat} + 50\text{ t. iron} + 125\text{ t. coal} \to (285 + \Delta c)\text{ t. coal} \tag{B.6.1c}$$

We see that as Δc increases, the value of coal (as measured in its exchange-rate with wheat) decreases. We perform these calculations, at increments of $\Delta c = 10$ tons of coal, and find:

	Value of 1 ton of coal		
Δc	p_c in multiples of p_w	p_c in multiples of p_i	rate of profit
0	$2.39536p_w$	$0.57506p_i$	3.79928%
10	$2.28951p_w$	$0.555297p_i$	3.93706%
20	$2.19192p_w$	$0.536871p_i$	4.07416%
30	$2.10173p_w$	$0.519652p_i$	4.2106%
40	$2.01814p_w$	$0.503524p_i$	4.34639%
50	$1.94051p_w$	$0.488387p_i$	4.48152%
60	$1.86823p_w$	$0.474151p_i$	4.616%
70	$1.80081p_w$	$0.460739p_i$	4.74984%
80	$1.73777p_w$	$0.448081p_i$	4.88303%
90	$1.67874p_w$	$0.436114p_i$	5.0156%
100	$1.62335p_w$	$0.424783p_i$	5.14753%

We see as the surplus of coal c increases, its exchange rate with iron and wheat decreases. In other words, *as supply increases, price decreases*. That is to say, the "law of supply" is an emergent phenomenon in Neo-Ricardian economics.

The curious reader may experiment with the Mathematica code used to produce this table:

```
inverse_profit[c_]:=Eigenvalues[{{200/480,40/180,40/(285+c)},
 {60/480,90/180,120/(285+c)},
 {150/480,50/180,125/(285+c)}}]

prices[c_,profit_]:=Reduce[{profit*(60 wheat + 90 iron + 120 coal) == 180 iron,
 profit*(150 wheat + 50 iron + 125 coal) == (285 + c) coal},
 {iron, coal}]

exchange[c_] := prices[c, 1/(inverse_profit[c])[[1]]]

Table[{10*c,
   N[exchange[10*c]][[2]][[2]],
   N[exchange[10*c]][[2]][[2]]/N[exchange[10*c]][[1]][[2]] iron,
   N[(1/inverse_profit[c] - 1)[[1]]},
 {c,0,10}]
```

The `inverse_profit` produces a list of eigenvalues for $\mathbf{AB}^{-1}$, the first eigenvalue corresponds to the economically significant solution. We then find the exchange-rate of iron, wheat, and coal using `prices`, and finally produce a `Table` of rows consisting of Δc, the price of 1 ton of coal in terms of the value of wheat p_w, and the price of 1 ton of coal in terms of the value of iron p_i.

C References

[1] David Cherney, Tom Denton, Rohit Thomas, and Andrew Waldron,
Linear Algebra.
Freely published ebook, 2016.
https://www.math.ucdavis.edu/~linear/

[2] Bernard Kolman and David R. Hill,
Introductory Linear Algebra: An Applied First Course.
Eighth edition, Prentice–Hall, 2005.

[3] Pierro Sraffa,
Production of Commodities by Means of Commodities.
Cambridge University Press, 1960.

[4] Leonhard Euler,
Elements of Algebra.
E387, translated by Scott L. Hecht (2015).

[5] David Marshall Miller,
"The Parallelogram Rule from Pseudo-Aristotle to Newton".
Archive for History of Exact Sciences **71** (2017) pp.157–191.
doi:10.1007/s00407-016-0183-2