Math 240

Aaron Greicius

Northwestern University

Table of contents I

Table of contents II

1.1 executive summary

Definitions: linear equations, linear systems, homogenous/nonhomogenous, solutions to linear system, consistent/inconsistent systems, parametric equations, row operations, row equivalence, augmented matrix

Procedures: introduction to row reduction

Theorems: row equivalent systems have the same set of solutions

Linear equations

Definition 1.1

A **linear equation** in the n variables (or **unknowns**) $x_1, x_2, \dots x_n$ is an equation that can be written in the form

$$a_1x_1 + a_2x_2 + \cdots a_nx_n = b,$$

where $a_1, \dots, a_n, b$ are constants.

The linear equation is called **homogenous** when $b = 0$.

Examples.

1. Consider $\sqrt{3}x + \sin(5) = 2z - e^4y$. This is a linear equation in the unknowns x, y, z as we can write it as $\sqrt{3}x + e^4y - 2z = -\sin(5)$. Note that this is a nonhomogenous linear equation.
2. The equation $x^2 + y^2 = 1$ is a nonlinear equation in the unknowns x and y.

Linear systems

Definition 1.2

A **system of linear equations** (or **linear system**) is a set of linear equations.

We display a system of m equations in the n unknowns $x_1, x_2, \dots x_n$ as follows:

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

A **homogenous** linear system is one where $b_i = 0$ for all i:

$$\begin{array}{ccccccc} a_{11}x_1 & + & a_{12}x_2 & +\cdots+ & a_{1n}x_n & = & 0 \\ a_{21}x_1 & + & a_{22}x_2 & +\cdots+ & a_{2n}x_n & = & 0 \\ & \vdots & & \vdots & & \vdots & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & +\cdots+ & a_{mn}x_n & = & 0 \end{array}$$

Comment. It will be helpful to get comfortable to the double-indexed constants a_{ij} as soon as possible. Here is a good way to understand this:

- i, the first index, indicates the i-th row, or equivalently, the i-th equation;
- j, the second index, indicates the j-th column, which is associated to the j-th variable.

Solutions to linear systems

Definition 1.3

A **solution to a linear equation**

$$a_1x_1 + a_2x_2 + \cdots a_nx_n = b$$

is a sequence (or **ordered n-tuple**) $(s_1, s_2, \ldots, s_n)$ for which the substitution $x_i = s_i$ makes the equation true. We say $(s_1, \ldots, s_n)$ **solves the equation** in this case .

A **solution to a system of linear equations**

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

is a sequence (or **ordered n-tuple**) $(s_1, s_2, \ldots, s_n)$ which solves all m of the system's equations. We say $(s_1, s_2, \ldots, s_n)$ **solves the system** in this case.

Given a linear system we will seek to find the set S of all solutions to the system. As we will soon see, this set will take one of three qualitative forms:

(i) S is empty; i.e., there are no solutions. We say the system is **inconsistent** in this case. Otherwise a system is called **consistent**.

(ii) S contains a single element; i.e., there is exactly one solution.

(iii) S contains infinitely many elements; i.e., there are infinitely solutions.

Example 1: $\begin{aligned} x-y&=0\\ x-y&=1\end{aligned}$

The first equation says $x=y$. If this were true, the second equation would imply $0=1$, a contradiction. Thus there are no solutions. The set of solutions is $S=\{\ \}=:\varnothing$, the empty set.

Example 2: $\begin{aligned} x-y&=0\\ x+y&=1\end{aligned}$

First equation says $x=y$. Then second equation says $2x=1$, $x=1/2$. Thus $(x,y)=(1/2,1/2)$ is the unique solution, and $S=\{(1/2,1/2)\}$.

Example 3: $\begin{aligned} x-\ \ y&=1\\ 2x-2y&=2\end{aligned}$

The second equation is just twice the first. So we need only find all solutions to $x-y=1$. Note that we can set $x=t$ for any real number $t\in\mathbb{R}$. Solving for y in terms of t we get $(x,y)=(t,t-1)$ for any $t\in\mathbb{R}$, and thus $S=\{(t,t-1)\colon t\in\mathbb{R}\}$, an infinite set! This is called a parametric description of S. Alternatively we can describe the infinite solutions with the parametric equations $x=t$, $y=t-1$, t any real number.

Example

Consider the system of 3 equations in 3 unknowns

$$\begin{aligned} 2x - y - z &= 3 \\ x \quad\;\; - z &= 2 \\ x - y \quad\;\; &= 1 \end{aligned}$$

Comments.

1. Q: why the funny formatting? A: we always associate the j-th variable with the j column of our equation array, for reasons that will become clear soon. Mandate: given some linear system, possibly expressed in a funky way, always convert it to this column-aligned format.
2. The triple (or 3-tuple) $(x, y, z) = (5, 2, 5)$ is NOT a solution to the system. It satisfies equation (1), but not equation (2) and not equation (3).
3. The triples $(x, y, z) = (4, 3, 2)$ and $(x, y, z) = (0, -1, -2)$ ARE solutions to this system. You can check that both triples solve equations (1), (2) and (3) of the system.
4. How do we find ALL solutions to a linear system?

Some systems are easier to solve than others.

System 1	System 2
$2x + 3y + -z = 18$	$x + y + z = 10$
$x + 2y - 2z = 8$	$y - 3z = -2$
$-\frac{1}{2}x + -\frac{1}{2}y + \frac{1}{2}z = -3$	$z = 2$

The staircase pattern of System 2 allows us to easily solve by "backwards substitution".

Eq 3 tells us that $\boxed{z = 2}$.

Substitute $z = 2$ into Eq 2, and solve for y to get $\boxed{y = 4}$.

Substitute $y = 4$ and $z = 2$ into Eq 1 and solve for x to get $\boxed{x = 4}$. We see that $\boxed{(x, y, z) = (4, 4, 2)}$ is the only solution to System 2.

Our method for solving a more complicated system, like System 1, will be to transform the system into a simpler one resembling System 2.

Key point: in order for this method to work, we need to make sure that the transformed system has EXACTLY the same solutions as the original system!

Elementary row operations

We will only allow the following types of transformations of a system, called **elementary row operations**. In what follows, let e_i stand for the i-th equation of the given system.

- Scalar mult. Multiply an equation by a nonzero number $c \neq 0$. That is, replace e_i with $c \cdot e_i$ for $c \neq 0$.
- Swap Interchange the order of any two equations. That is, swap equations e_i and e_j.
- Addition Add a multiple of one row to another. That is, replace e_i with $e_i + ce_j$ for some c.

We must convince ourselves that applying any one of these operations to a single row of a system will produce a new system with EXACTLY the same set of solutions.

If this is so, then by applying these operations in series we will be able to reduce a complicated system to a simpler system with the same set of solutions.

Example

Consider again

$$\begin{aligned} 2x + 3y + -z &= 18 \\ x + 2y - 2z &= 8 \\ -\tfrac{1}{2}x + -\tfrac{1}{2}y + \tfrac{1}{2}z &= -3 \end{aligned}$$

Begin applying row operations as follows

$$\xrightarrow{2e_3} \quad \begin{aligned} 2x + 3y + -z &= 18 \\ x + 2y - 2z &= 8 \\ -x + -y + z &= -6 \end{aligned}$$

$$\xrightarrow{e_1 - e_2} \quad \begin{aligned} x + y + z &= 10 \\ x + 2y - 2z &= 8 \\ -x + -y + z &= -6 \end{aligned}$$

$$\xrightarrow[e_2 - e_1]{e_3 + e_1} \quad \begin{aligned} x + y + z &= 10 \\ y - 3z &= -2 \\ 2z &= 4 \end{aligned}$$

$$\xrightarrow{\frac{1}{2}e_3} \quad \begin{aligned} x + y + z &= 10 \\ y - 3z &= -2 \\ z &= 2 \end{aligned}$$

Example concluded

Now put the logic together.

$$\begin{aligned} 2x + 3y + -z &= 18 \\ x + 2y - 2z &= 8 \\ -x + -y + z &= -6 \end{aligned} \quad \xrightarrow{\text{row op.'s}} \quad \begin{aligned} x + y + z &= 10 \\ y - 3z &= -2 \\ z &= 2 \end{aligned}$$

We saw already that the second system has exactly one solution, namely the triple $(x, y, z) = (4, 4, 2)$.

Since transforming a system by row operations preserves solutions, the first and second system have exactly the same solutions.

Thus $\boxed{(x, y, z) = (4, 4, 2)}$ is the only solution to the original system!

Let's make official some concepts and claims of this lecture.

Definition 1.4

We say two systems of linear equations are **row equivalent** if the one can be obtained from the other by a sequence of row operations.

Theorem 1.1 (Row equivalence theorem)

Row equivalent systems of linear equations have equal sets of solutions.

Augmented matrices

The '$+$' and '$=$' symbols in systems of equations just get in the way when performing row operations. As such we will often replace a system with its **associated augmented matrix** and perform our row operations on this.

Example. The system

$$\begin{aligned} 2x + \ 3y + -z &= \ 18 \\ x + \ 2y - \ 2z &= \ \ 8 \\ -x + -y + \ \ z &= -6 \end{aligned}$$

is represented by the augmented matrix

$$\left[\begin{array}{rrr|r} 2 & 3 & -1 & 18 \\ 1 & 2 & -2 & 8 \\ -1 & -1 & 1 & -6 \end{array}\right]$$

The vertical line is unnecessary, but I often include it to remind us where the equal signs were.

1.2 executive summary

Definitions: leading 1's, row echelon form, reduced row echelon form, free variables, leading variables, general solution.

Procedures: Gaussian elimination, Gauss-Jordan elimination, solving a linear system of equations (=Gaussian elimination+assigning free vars. parameter names+solving for leading variables in terms of free ones.)

Theorems: let A be a row reduced form of the augmented matrix corr. to a given linear system.
The system of equations is inconsistent iff the last column of A has a leading 1.
If the system is consistent, then it has either exactly one solution, or infinitely many solutions. The former occurs when there are no free variables. The latter occurs when there is a free variable.
A consistent system with more unknowns than equations has infinitely many solutions.
A homogenous system is always consistent.
A homogenous system with more unknowns than equations has infinitely many solutions.

Strategy for solving systems of equations

Given system

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

represent it with the augmented matrix

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right],$$

then perform row operations to get a new, simpler matrix whose corresponding system is easier to solve.

We wish to

a. Give a deterministic algorithm guaranteed to reduce a given matrix A to a well-defined simpler matrix B.
b. Give a recipe for writing down all the solutions (if any) to the new system of equations corresponding to B.

Here is our mathematical stand-in for the notion of a "simple" matrix.

Definition 2.1

A matrix is in **row echelon form** if

1. in any nonzero row the first (i.e., leftmost) nonzero entry is a 1 (called the **leading 1** of the row);
2. all zero rows are grouped at the bottom of the matrix;
3. given any two nonzero rows, the leading 1 of the lower row occurs strictly to the right of the leading 1 of the upper row ("staircase pattern").

A matrix is in **reduced row echelon form** if in addition to (1)-(3) it also satisfies:

4. each column containing a leading 1 has zeros everywhere else.

(Reduced) row echelon form

In practice to decide whether a matrix is in in (reduced) row echelon form, follow this flow chart:

1. First see whether all zero rows are at the bottom.
2. For each nonzero row, determine whether the first nonzero entry is a 1, and put a box around it.
3. Make sure your boxes make a staircase pattern.
4. (For reduced row echelon form only.) Decide whether each column with a box has 0's everywhere else.

Example.

$$\begin{bmatrix} \boxed{1} & 0 & 0 & -3 & -7 \\ 0 & 0 & \boxed{1} & 2 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The matrix is in row echelon form as the boxed leading 1's make a staircase pattern.

The matrix is NOT in reduced row echelon form as the last column has a nonzero entry above it.

Gaussian elimination

Gaussian elimination is an algorithm which, given a matrix A, transforms it one row operation at a time to a matrix B in row echelon form.

Step 1 Find leftmost nonzero column and use row swap operation to move nonzero entry to top.

Step 2 Use scaling operation to make this top entry a leading 1.

Step 3 Add multiples of top row to lower rows to clear entries below the leading 1.

Step 4 Cover top row and begin again with Step 1 applied to remaining matrix. Continue until matrix is in row echelon form.

The next slide presents a detailed example of this procedure.
Use this as a model when doing your own examples and exercises, including the naming of row operations used.

Example

$$\begin{bmatrix} 0 & 0 & -2 & 0 & 7 & 12 \\ 2 & 4 & -10 & 6 & 12 & 28 \\ 2 & 4 & -5 & 6 & -5 & -1 \end{bmatrix} \xrightarrow{r_1 \leftrightarrow r_2} \begin{bmatrix} 2 & 4 & -10 & 6 & 12 & 28 \\ 0 & 0 & -2 & 0 & 7 & 12 \\ 2 & 4 & -5 & 6 & -5 & -1 \end{bmatrix}$$

$$\xrightarrow{\frac{1}{2} r_1} \begin{bmatrix} 1 & 2 & -5 & 3 & 6 & 14 \\ 0 & 0 & -2 & 0 & 7 & 12 \\ 2 & 4 & -5 & 6 & -5 & -1 \end{bmatrix}$$

(now done with first row) $$\xrightarrow{r_3 - 2r_1} \begin{bmatrix} 1 & 2 & -5 & 3 & 6 & 14 \\ 0 & 0 & -2 & 0 & 7 & 12 \\ 0 & 0 & 5 & 0 & -17 & -29 \end{bmatrix}$$

$$\xrightarrow{-\frac{1}{2} r_2} \begin{bmatrix} 1 & 2 & -5 & 3 & 6 & 14 \\ 0 & 0 & 1 & 0 & -7/2 & -6 \\ 0 & 0 & 5 & 0 & -17 & -29 \end{bmatrix}$$

(now done with 2nd row) $$\xrightarrow{r_3 + (-5) r_2} \begin{bmatrix} 1 & 2 & -5 & 3 & 6 & 14 \\ 0 & 0 & 1 & 0 & -7/2 & -6 \\ 0 & 0 & 0 & 0 & 1/2 & 1 \end{bmatrix}$$

$$\xrightarrow{2r_3} \begin{bmatrix} \boxed{1} & 2 & -5 & 3 & 6 & 14 \\ 0 & 0 & \boxed{1} & 0 & -7/2 & -6 \\ 0 & 0 & 0 & 0 & \boxed{1} & 2 \end{bmatrix}$$

Gauss-Jordan elimination

The procedure for reducing a matrix all the way to reduced row echelon is called **Gauss-Jordan elimination**. To do this, first perform Gaussian elimination to reduce A to row echelon form, then use row operations to clear the entries above leading 1's, starting with the rightmost and working backward.

Continuing our previous example:

$$\begin{bmatrix} \boxed{1} & 2 & -5 & 3 & 6 & 14 \\ 0 & 0 & \boxed{1} & 0 & -7/2 & -6 \\ 0 & 0 & 0 & 0 & \boxed{1} & 2 \end{bmatrix}. \xrightarrow{r_2+7/2r_3} \begin{bmatrix} \boxed{1} & 2 & -5 & 3 & 6 & 14 \\ 0 & 0 & \boxed{1} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & \boxed{1} & 2 \end{bmatrix}.$$

$$\xrightarrow{r_1-6r_3} \begin{bmatrix} \boxed{1} & 2 & -5 & 3 & 0 & 2 \\ 0 & 0 & \boxed{1} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & \boxed{1} & 2 \end{bmatrix}.$$

$$\xrightarrow{r_1+5r_2} \begin{bmatrix} \boxed{1} & 2 & 0 & 3 & 0 & 7 \\ 0 & 0 & \boxed{1} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & \boxed{1} & 2 \end{bmatrix}.$$

Solving a reduced system

It remains now to solve the resulting system corresponding to our matrix in row echelon (or reduced row echelon) form.

Since all reduced row echelon matrices are row echelon matrices, it will suffice to outline how to solve the latter type of systems.

Let's continue with our example:

$$\begin{aligned}
-2x_3 + 7x_5 &= 12 \\
2x_1 + 4x_2 - 10x_3 + 6x_4 + 12x_5 &= 28 \\
2x_1 + 4x_2 - 5x_3 + 6x_4 - 5x_5 &= -1
\end{aligned}$$

$$\xrightarrow{\text{aug. mat.}} \begin{bmatrix} 0 & 0 & -2 & 0 & 7 & 12 \\ 2 & 4 & -10 & 6 & 12 & 28 \\ 2 & 4 & -5 & 6 & -5 & -1 \end{bmatrix}$$

$$\xrightarrow{\text{row op.'s}} \begin{bmatrix} \boxed{1} & 2 & -5 & 3 & 6 & 14 \\ 0 & 0 & \boxed{1} & 0 & -7/2 & -6 \\ 0 & 0 & 0 & 0 & \boxed{1} & 2 \end{bmatrix}$$

$$\xrightarrow{\text{new sys}} \begin{aligned}
\boxed{x_1} + 2x_2 - 5x_3 + 3x_4 + 6x_5 &= 14 \\
\boxed{x_3} - 7/2x_5 &= -6 \\
\boxed{x_5} &= 2
\end{aligned}$$

Solving a reduced system

$$\begin{array}{rcrcrcrcrcr} \boxed{x_1} & + & 2x_2 & - & 5x_3 & + & 3x_4 & + & 6x_5 & = & 14 \\ & & & & \boxed{x_3} & & & - & 7/2x_5 & = & -6 \\ & & & & & & & & \boxed{x_5} & = & 2 \end{array}$$

So how do we get ALL solutions, and describe them in a useful way? Here's how

1. Divide the variables $x_1, x_2, \ldots, x_5$ into **leading variables** and **free variables**: a leading variable is one corresponding to a column of the row reduced matrix that contains a leading 1; a free variable is any variable that is not a leading one.

   In our case, x_1, x_3, and x_5 are leading, and the rest, x_2, x_4 are free.

2. The free variables act as **parameters** for our solutions. They range independently over all reals. Give them parameter names: $x_2 = s$, $x_4 = t$.

3. Solve for the remaining leading variables in terms of the parameters s, t, starting from the rightmost leading variable and working backwards ("backwards substitution"). We find $x_5 = 2$, $x_3 = -6 + 7 = 1$, $x_1 = 7 - 2s - 3t$.

Thus the **general solution** of the system is $(x_1, x_2, \ldots, x_5) = (7 - 2s - 3t, s, 1, t, 2)$, where s, t can be any real numbers.

Solving a reduced system

$$\begin{aligned}
\boxed{x_1} + 2x_2 - 5x_3 + 3x_4 + 6x_5 &= 14 \\
\boxed{x_3} - 7/2x_5 &= -6 \\
\boxed{x_5} &= 2
\end{aligned}$$

Some comments about how we express the solutions to a system.

I described the general solution in tuple form:

$$(x_1, x_2, \ldots, x_5) = (5 - 2s - 3t, s, 1, t, 2), \quad s, t \text{ any real numbers.}$$

Alternatively we can give parametric equations for each variable separately:

$$\begin{aligned}
x_1 &= 7 - 2s - 3t \\
x_2 &= s \\
x_3 &= 1 \qquad\qquad\qquad s, t \in \mathbb{R} \\
x_4 &= t \\
x_5 &= 2
\end{aligned}$$

Of course we can also just write down the set of all solutions:

$$S = \Big\{(7 - 2s - 3t, s, 1, t, 2) \colon s, t \in \mathbb{R}\Big\}.$$

Get used to using all three forms of answers.

Inconsistent system

It seems we have a surefire way of writing down general solution of any linear system.

However, we've glossed over the situation where a linear system has no solutions. This is called an **inconsistent** system.

When can this happen? As always, it all depends on the shape of the row echelon matrix we get after Gaussian elimination. Here is a row echelon matrix whose corresponding linear system has no solutions:

$$\begin{bmatrix} \boxed{1} & 0 & 2 & 3 \\ 0 & 0 & \boxed{1} & 1 \\ 0 & 0 & 0 & \boxed{1} \end{bmatrix}$$

The last equation of the corresponding linear system would read $0x_1 + 0x_2 + 0x_3 = 1$, or $0 = 1$. Since this is impossible, there is no solution to the system.

We can express this succinctly in terms of leading 1's.

Theorem 2.1

A linear system is inconsistent if and only if its augmented matrix reduces to a row echelon matrix with a leading 1 in the last column.

Solutions to linear systems

We are now in a position to fully describe what solution sets to linear systems look like qualitatively.

Theorem 2.2 (Gaussian elimination theorem)

Fix a linear system in n unknowns $x_1, x_2, \ldots, x_n$, let A be its corresponding augmented matrix, and let U be the row echelon matrix we get after applying Gaussian elimination to A.

1. The system is inconsistent if and only if the last column of U has a leading 1. In this case there are $\boxed{0}$ solutions.
2. Assume the system is consistent.
   - 2.1 If all variables are leading variables, then after back substituting, we find there is a unique solution. That is, in this case there is $\boxed{1}$ solution.
   - 2.2 If there is a free variable, say x_i, then since we can set $x_i = t$ for any t, there are $\boxed{\infty}$-many solutions

In particular, we see there are only 3 choices for the number of solutions to a linear system: 0, 1, or ∞-many!

Solutions to homogenous systems

Consider the special case of a homogenous system

$$\begin{array}{ccccccc}
a_{11}x_1 & + & a_{12}x_2 & +\cdots+ & a_{1n}x_n & = & 0 \\
a_{21}x_1 & + & a_{22}x_2 & +\cdots+ & a_{2n}x_n & = & 0 \\
 & \vdots & & \vdots & & \vdots & \vdots \\
a_{m1}x_1 & + & a_{m2}x_2 & +\cdots+ & a_{mn}x_n & = & 0
\end{array}$$

Observe that $(x_1, x_2, \ldots, x_n) = (0, 0, \ldots, 0)$ is a solution to this system. Thus a homogenous system is always consistent!

(Alternatively, convince your self that the corresponding row echelon matrix U for the system will have no leading 1's in the last column.)

Solutions to homogenous systems

Since a homogenous system is always consistent, the theorem from before boils down to the following:

Corollary 2.2.1

Fix a homogenous linear system in n variables. There are two possibilities:

1. if all the variables are leading variables, then the system has a unique solution (i.e., $\boxed{1}$ solution);
2. if there is a free variable, then the system has $\boxed{\infty}$-many solutions.

Solutions to homogenous systems

Furthermore, we have:

Corollary 2.2.2

Fix a homogenous linear system. If the system has more variables than equations, then there are ∞-many solutions.

Proof.

Since any homogeneous system is consistent. We need only show there is a free variable.

Let m be the number of equations, or equivalently, the number of rows of the augmented matrix. By assumption $m < n$.

Now the definition of a leading 1 implies that there can be at most m leading 1's, since there is at most one leading 1 per row.

This implies there are at most m leading variables, and thus at least $n - m$ free variables. Since $n - m > 0$ there is at least one free variable, and thus ∞-many solutions. $\square$

1.3: executive summary

Definitions: matrix, matrix dimension (size), matrix equality, sum/difference, scalar multiplication, linear combinations, matrix multiplication, transpose.

Procedures: row method of matrix multiplication, column method of matrix multiplication.

Theorems: none yet!

Matrices

Definition 3.1

A **matrix** is a rectangular array of numbers.

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

The **size** (or **dimension**) of a matrix is given by the pair $m \times n$, where m is the number of rows, and n is the number of columns. The matrix A above is an $m \times n$ matrix.

Notation

We use the notation $[a_{ij}]_{m \times n}$ to define the $m \times n$ matrix whose ij-th entry (i-th row, j-th column) is a_{ij}.

Similarly, given a matrix A, the notation $(A)_{ij}$ denotes the ij-th entry of A.

Specially sized matrices

An $n \times n$ matrix is called a **square matrix of order** n.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}.$$

A $1 \times n$ matrix is called a **row vector**:

$$\mathbf{a} = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix}.$$

An $m \times 1$ matrix is called a **column vector**:

$$\mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

Equality, sum, difference

Definition 3.2

Two matrices A and B are **equal** when

1. they have the same size, and
2. their corresponding entries are equal.

In other words, A and B must both be $m \times n$ matrices, and $(A)_{ij} = (B)_{ij}$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$.

Definition 3.3

Suppose $A = [a_{ij}]$ and $B = [b_{ij}]$ are both $m \times n$ matrices. We define

- their **sum** $A + B$ to be the matrix $C = [a_{ij} + b_{ij}]$;
- their **difference** $A - B$ to be the matrix $D = [a_{ij} - b_{ij}]$.

Equivalently, we $A + B$ and $A - B$ are defined by declaring:

$$\begin{aligned} (A+B)_{ij} &= (A)_{ij} + (B)_{ij} \\ (A-B)_{ij} &= (A)_{ij} - B_{ij} \end{aligned}$$

Scalar multiplication

Definition 3.4 (Scalar multiplication)

Given any matrix $A = [a_{ij}]_{m \times n}$ and any constant c, we define

$$cA = [ca_{ij}].$$

We call cA a **scalar multiple** of A.

Comment

It is best to think of scalar multiplication as a sort of hybrid operation that takes two different types of object, a constant (or **scalar**) c and a matrix A, and spits back a matrix.

In particular it is important to keep straight the difference between scalar multiplication and matrix multiplication, which we consider next.

Matrix multiplication

Warning: after all this, you might guess that we would define multiplication of two $m \times n$ matrices A and B by taking the product of the corresponding entries. NOT SO!

Definition 3.5

Let $A = [a_{ij}]_{m \times r}$ be an $m \times r$ matrix, and $B = [b_{ij}]_{r \times n}$ be an $r \times n$ matrix.

We define their **product**, $A \cdot B$ to be the $m \times n$ matrix $C = [c_{ij}]_{m \times n}$, where

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots a_{ir}b_{rj} = \sum_{\ell=1}^{r} a_{i\ell}b_{\ell j}.$$

Note the many peculiarities of this definition:

1. In general $A_{m \times r}$, $B_{r \times n}$ and $C_{m \times n}$ all have different sizes!
2. The rule for getting the entries of $A \cdot B$ is nowhere near as simple as we may have hoped!

Matrix multiplication

For the product of A and B to be defined, we need the number of columns of A to be equal to the number of rows of B. That is, the "inside" dimensions in the product below must be equal.

$$A_{m\times r}\cdot B_{r\times n}=C_{m\times n}$$

The "outside" dimensions tells us the dimension of the resulting matrix.

All of this will make more sense once we begin thinking of matrices A as defining certain functions T_A. It turns out that the product of two matrices $A\cdot B$ will represent the composition of their corresponding functions: i.e., $T_A\circ T_B$.

The peculiar restriction on the dimensions of the matrices ensures that the two functions T_A and T_B can be composed: that is, that the range of T_B lies within the domain of T_A. More on this later!

Alternative methods of multiplication

In addition to the straightforward definition of matrix multiplication, we will make heavy use of a couple of alternative methods to computing products.

To articulate these other methods, we need the following notion.

Definition 3.6 (Linear combination of matrices)

Let $A_1, A_2, \ldots, A_r$ be matrices of the same size, and let $c_1, c_2, \ldots, c_r$ be scalars. The matrix

$$c_1A_1 + c_2A_2 \cdots + c_rA_r$$

is called a **linear combination** of the A_i, with **coefficients** c_i.

Column method of AB

Given a matrix $A_{m\times n}$, we will think of A as a sequence of n column vectors:

$$\left[\begin{array}{c|c|c|c} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{array}\right] = \begin{bmatrix} | & | & & | \\ \mathbf{a}_1 & \mathbf{a}_2 & \cdots & \mathbf{a}_n \\ | & | & & | \end{bmatrix}$$

Then for any column vector $\mathbf{b} = [b_i]$ we have

$$A\mathbf{b} = A \cdot \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = b_1\mathbf{a}_1 + b_2\mathbf{a}_2 + \cdots + b_n\mathbf{a}_n.$$

Next, we treat any $n \times r$ matrix $B_{n\times r}$ as a sequence of column vectors $B = \begin{bmatrix} | & | & & | \\ \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_r \\ | & | & & | \end{bmatrix}$. Then we have

$$AB = A\begin{bmatrix} | & | & & | \\ \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_r \\ | & | & & | \end{bmatrix} = \begin{bmatrix} | & | & & | \\ A\mathbf{b}_1 & A\mathbf{b}_2 & \cdots & A\mathbf{b}_r \\ | & | & & | \end{bmatrix}.$$

Row method of AB

Given a matrix $B_{n\times r}$, we will think of B as a sequence of m row vectors:

$$\left[\begin{array}{cccc} b_{11} & b_{12} & \cdots & b_{1r} \\ \hline b_{21} & b_{22} & \cdots & b_{2r} \\ \hline \vdots & \vdots & \ldots & \vdots \\ \hline b_{n1} & b_{n2} & \cdots & b_{nr} \end{array}\right] = \begin{bmatrix} -\mathbf{b}_1- \\ -\mathbf{b}_2- \\ \vdots \\ -\mathbf{b}_n- \end{bmatrix}$$

Then for any row vector $\mathbf{a} = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix}$ we have

$$\mathbf{a}B = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix} B = a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n.$$

Next, we treat any $m \times n$ matrix $A_{m\times n}$ as a sequence of row vectors and compute

$$AB = \begin{bmatrix} -\mathbf{a}_1- \\ -\mathbf{a}_2- \\ \vdots \\ -\mathbf{a}_m- \end{bmatrix} B = \begin{bmatrix} -\mathbf{a}_1 B- \\ -\mathbf{a}_2 B- \\ \vdots \\ -\mathbf{a}_m B- \end{bmatrix}$$

Transpose of a matrix

Definition 3.7

Given an $m \times n$ matrix $A = [a_{ij}]$ its transpose A^T is the matrix whose ij-entry is the ji-th entry of A.

Using notation we have $A^T = [b_{ij}]_{n \times m}$, where $b_{ij} = a_{ji}$.

Note in particular that A^T is $n \times m$.

Examples: let $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$; then $A^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$.

Let $B = \begin{bmatrix} 1 \\ 0 \\ 3 \end{bmatrix}$, then $B^T = \begin{bmatrix} 1 & 0 & 3 \end{bmatrix}$.

Comment: there are a couple of equivalent ways of describing A^T that may be more helpful depending on the situation:

- A^T is the matrix whose columns are the rows of A.
- A^T is the matrix whose rows are the columns of A.

1.4: executive summary

Definitions: zero matrix $\mathbf{0}_{m\times n}$, identity matrix I_n, inverse matrix A^{-1}, invertibility, A^r and A^{-r} for nonnegative integer $r \geq 0$.

Procedures: none!

Theorems: Many! Lots of familiar rules of real number algebra (associativity, distributivity, etc.) also hold for matrix algebra. However some important properties fail: e.g., commutativity and multiplicative cancellation. We also learn some properties about taking the transpose ($A \mapsto A^T$) and its relation with taking the inverse ($A \mapsto A^{-1}$).

1.4: algebraic properties of matrices

For the most part, the matrix operations of $\cdot$ and $+$ behave in much the same manner as their corresponding real number operations.

Theorem 4.1 (Properties of matrix arithmetic)

The following properties hold for all matrices A, B, C and scalars a, b, c for which the given expression makes sense.

(a) $A+B=B+A$

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

(c) $A(BC)=(AB)C$

(d) $A(B+C)=AB+AC$

(e) $(B+C)A=BA+CA$

(f) $A(B-C)=AB-AC$

(g) $(B-C)A=BA-CA$

(h) $a(B+C)=aB+aC$

(i) $a(B-C)=aB-aC$

(j) $(a+b)C=aC+bC$

(k) $(a-b)C=aC-bC$

(l) $a(bC)=(ab)C$

(m) $a(BC)=(aB)C=B(aC)$.

How does one actually prove one of these properties?

These are all matrix equalities. Using the definition of matrix equality, we must show (1) the LHS and RHS matrices are of the same size, and (2) that for each (i,j), the (i,j)-th entry of the LHS is equal to the (i,j)-th entry of the RHS. Let's see how this works on an example.

Proof of Theorem 4.1 (c).

Let $A = [a_{ij}]_{m\times r}$, $B = [b_{ij}]_{r\times s}$, $C = [c_{ij}]_{s\times n}$. Then

$$A(BC) = (AB)C.$$

(1) One checks easily that the matrices on the LHS and RHS are both of size $m \times n$, so we move straight to (2) using our index notation:

$$\begin{aligned}
\Big(A(BC)\Big)_{ij} &= \sum_{\ell=1}^{r} a_{i\ell}(BC)_{\ell j} = \sum_{\ell=1}^{r} a_{i\ell}\left(\sum_{k=1}^{s} b_{\ell k}c_{kj}\right) \\
&= \sum_{\ell=1}^{r}\sum_{k=1}^{s} a_{i\ell}(b_{\ell k}c_{kj}) \quad \text{(dist. prop.)} \\
&= \sum_{k=1}^{s}\sum_{\ell=1}^{r} (a_{i\ell}b_{\ell k})c_{kj} \quad \text{(comm.+assoc. prop.)} \\
&= \sum_{k=1}^{s}\left(\sum_{\ell=1}^{r} a_{i\ell}b_{\ell k}\right)c_{kj} \quad \text{(dist. prop.)} \\
&= \sum_{k=1}^{s}(AB)_{ik}c_{kj} = \Big((AB)C\Big)_{ij}
\end{aligned}$$

This proves their ij-th entries are equal, and hence $A(BC) = (AB)C$. $\square$

Zero matrix and additive inverses

Another similarity between matrix algebra and real number algebra is the existence of additive inverses.

Definition: the $m \times n$ **zero matrix** is the matrix $\mathbf{0}_{m\times n}$ all of whose entries are 0. Note we have a different zero matrix for every possible size of matrix.

Theorem 4.2

Let $A = [a_{ij}]$ be $m \times n$. Then the matrix $-A := (-1)A = [-a_{ij}]$ is an **additive inverse** of A in the sense that

$$A + (-A) = (-A) + A = \mathbf{0}_{m\times n}.$$

Comment: thus every $m \times n$ matrix has an additive inverse. This allows us to "cancel" matrices additively. Example: solve the following equation for B.

$$\begin{aligned} A + B &= 3A \\ (-A) + A + B &= (-A) + 3A \\ \mathbf{0}_{m\times n} + B &= (-1)A + 3A \\ B &= 2A \end{aligned}$$

I give all the gory details, but now the point should be clear; we can cancel a multiple of A on both sides, just as we do in normal algebra!

Abnormalities

There are two very important properties that matrix algebra fails to enjoy.

Theorem 4.3

Matrix multiplication is NOT commutative, and there are nontrivial zero divisors. That is:

1. Fix n. There are (many) $n \times n$ matrices A, B such that
$$AB \neq BA.$$
Example: verify that $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.
2. Given matrices $A_{m \times n}, B_{n \times r}$,
$$AB = 0_{m \times r} \not\Rightarrow A = 0_{m \times n} \text{ or } B = 0_{n \times r}.$$
In English: if the product of two matrices is the zero matrix, we CANNOT conclude that one of them is the zero matrix.

   Example: verify that $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

It is worth pointing out how important the second failed property is to matrix algebra.

In normal real number algebra, if $a \neq 0$ and $ab = ac$, we may "cancel" the a and conclude $b = c$. Not so in matrix algebra!

Theorem 4.4 (Failure of cancellation)

$$\begin{array}{lcl} \text{Suppose } A \neq 0_{m\times n}, \text{ then } AB = AC & \not\Rightarrow & B = C \\ \text{Suppose } D \neq 0_{s\times t}, \text{ then } BD = CD & \not\Rightarrow & B = D \end{array}$$

Let that sink in. Cancellation is one of the most used properties in normal algebra. It is in general no longer available to us when doing matrix algebra.

Examples: (you should verify).

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

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

Invertibility

What allows cancellation of a nonzero a in the reals is the existence of its multiplicative inverse, the element $a^{-1} = \frac{1}{a}$, which satisfies $a^{-1}a = 1$.

Not all nonzero matrices A have a multiplicative inverse. The ones that do are called invertible. In order to define this properly, we need to identify a matrix that acts as the number one does: i.e., a multiplicative identity.

Definition 4.1

The **identity matrix of size** $n \times n$ is the $n \times n$ matrix I_n with 1's along the diagonal (i.e., $a_{ii} = 1$) and 0's everywhere else (i.e., $a_{ij} = 0$ for $i \neq j$). For example:

$$I_1 = \begin{bmatrix} 1 \end{bmatrix}, I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \text{ etc.}$$

Theorem 4.5 (Multiplicative identity)

For any $A_{m\times n}$ we have

$$\begin{aligned} I_m A &= A \\ A I_n &= A. \end{aligned}$$

Proof.

Use either column or row method to perform the multiplications involved! $\square$

Invertibility

Definition 4.2

A square matrix $A_{n\times n}$ is **invertible** if there is a matrix $B_{n\times n}$ such that

$$\begin{aligned} AB &= I_n, \text{ and} \\ BA &= I_n \end{aligned}$$

In this case we call B an **inverse** of A, and we say that A and B are **inverses** of one another.

Theorem (uniqueness of inverses): an invertible matrix A has exactly one inverse. That is, if

$$AB = BA = I_n$$

and

$$AC = CA = I_n,$$

then $B = C$.
We denote by A^{-1} the inverse of A.

Proof.

Suppose we have such matrices B and C.
Then $I_n = AB = AC \Rightarrow BAB = BAC \Rightarrow I_n B = I_n C \Rightarrow B = C$. $\square$

2×2 matrices

When is a 2×2 matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ invertible?

If $ad - cb \neq 0$, then we can easily show that

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

is the inverse.

Thus

$$ad - bc \neq 0 \Rightarrow A \text{ invertible.}$$

It turns out that the converse is also true, that is

$$ad - bc \neq 0 \Leftrightarrow A \text{ invertible.}$$

We will prove this a littler further down the line.

Theorem 4.6

Let A, B be $n \times n$ matrices.

$$A \text{ and } B \text{ invertible} \Rightarrow AB \text{ invertible},$$

and in fact $(AB)^{-1} = B^{-1}A^{-1}$.

Proof.

In the absence of more theory, we can only prove invertibility by providing an inverse. The last statement offers up a candidate: viz., $C = B^{-1}A^{-1}$. We need only show that C satisfies the relevant properties:

$$\begin{aligned} C(AB) &= (B^{-1}A^{-1})AB = B^{-1}A^{-1}AB = B^{-1}IB = B^{-1}B = I \\ (AB)C &= (AB)B^{-1}A^{-1} = ABB^{-1}A^{-1} = AIA^{-1} = AA^{-1} = I. \end{aligned}$$

$\square$

Corollary 4.6.1

More generally,

$$A_1, A_2, \ldots A_r \text{ invertible} \Rightarrow (A_1A_2 \cdots A_r) \text{ invertible},$$

and in fact $(A_1A_2 \cdots A_r)^{-1} = A_r^{-1}A_{r-1}^{-1} \cdots A_1^{-1}$.

Question: do the implication arrows above go the other way?

Answer: we shall see.

Powers of matrices

Definition 4.3

Let A be any $n \times n$ matrix. For any integer $r \geq 0$ we define the r-th power of A, A^r, as follows:

i $A^0 = I_n$.

ii $A^r = \underbrace{A \cdot A \cdots A}_{r \text{ times}}$ for $r > 0$.

Furthermore, if A is invertible, we define

$$A^{-r} = \left(A^{-1}\right)^r,$$

for any positive integer $r > 0$.

Theorem 4.7 (Power rules)

(a) $A^r A^s = A^{r+s}$

(b) $(A^r)^s = A^{rs}$

(c) $\left(A^{-1}\right)^{-1} = A$

(d) $(A^n)^{-1} = A^{-n}$

(e) $(kA)^n = k^n A^n$ for any scalar k.

Question: $A^r B^r \stackrel{?}{=} (AB)^r$

Transposes and inverses

Theorem 4.8

(a) $\left(A^T\right)^T = A$

(b) $(A + B)^T = A^T + B^T$

(c) $(A - B)^T = A^T - B^T$

(d) $(kA)^T = kA^T$

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

Theorem 4.9

Let $A_{n \times n}$ be invertible. Then A^T is invertible, and $\left(A^T\right)^{-1} = \left(A^{-1}\right)^T$.

More sample proofs

Let's prove some of the last two theorems.

Proof that $(A+B)^T = A^T + B^T$.

$$\begin{aligned}
\left((A+B)^T\right)_{ij} &= (A+B)_{ji} \ \ \text{(def. of transp.)} \\
&= A_{ji} + B_{ji} \ \ \text{(def. of +)} \\
&= (A^T)_{ij} + (B^T)_{ij} \ \ \text{(def. of transp.)} \\
&= (A^T + B^T)_{ij} \ \ \text{(def. of +)}
\end{aligned}$$

Since ij-entry of LHS and RHS is same for each (i, j), it follows that $(A+B)^T = A^T + B^T$. $\square$

More sample proofs

Proof that $\left(A^T\right)^{-1} = \left(A^{-1}\right)^T$.

Suppose A is invertible, and let A^{-1} be its inverse. The claim above is that $B = \left(A^{-1}\right)^T$ is the inverse of A^T. To prove this claim we need only show that $BA^T = A^T B = I_n$:

$$
\begin{aligned}
BA^T = \left(A^{-1}\right)^T A^T &= \left(AA^{-1}\right)^T \text{ (since } (CD)^T = D^T C^T\text{)} \\
&= I_n^T = I_n \checkmark
\end{aligned}
$$

$$
\begin{aligned}
A^T B = A^T \left(A^{-1}\right)^T &= \left(A^{-1}A\right)^T \text{ (since } (CD)^T = D^T C^T\text{)} \\
&= I_n^T = I_n \checkmark
\end{aligned}
$$

$\square$

1:5 executive summary

Definitions:elementary matrices

Procedures: finding A^{-1} using row reduction, writing A as a product of elementary matrices.

Theorems: elementary matrices are invertible, and their inverses are themselves elementary; the invertibility theorem.

1:5: computing inverses with row reduction

Surprisingly row reduction provides a tool for both deciding whether a matrix is invertible, and computing this inverse if it exists.

First we will construe row operations as certain matrix multiplications.

Definition 5.1

A square matrix $E_{m\times m}$ is an **elementary matrix** if multiplying any matrix $A_{m\times n}$ on the left by E performs one of our row operations on A.

Comment

Equivalently, a matrix $E_{m\times m}$ is elementary if it is the result of applying a single row operation on I_m.

The row method of multiplication is the key to matching up a row operation with a particular elementary matrix.
Suppose the multiplication

$$\underset{m \times m}{E} \cdot \underset{m \times n}{A} = \underset{m \times n}{A'}$$

performs a single row operation on A. What must E be? In what follows let $\mathbf{r}_i$ be the i-th row of A for $1 \leq i \leq m$.

Scale. Suppose E replaces $\mathbf{r}_i$ of A with $c \cdot \mathbf{r}_i$ for $c \neq 0$. Then E is the identity matrix except for the i-th row, where the 1 is replaced with c.

$$\underset{cr_i}{E} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & \\ \vdots & & \vdots & & \vdots & \\ 0 & \cdots & 0 & c & 0 & \cdots \\ \vdots & & \vdots & & \vdots & \\ 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$$

The row method of multiplication is the key to matching up a row operation with a particular elementary matrix.

Suppose the multiplication

$$\underset{m\times m}{E} \cdot \underset{m\times n}{A} = \underset{m\times n}{A'}$$

performs a single row operation on A. What must E be? In what follows let $\mathbf{r}_i$ be the i-th row of A for $1 \leq i \leq m$.

Swap. Suppose E swaps rows i and j of A. Then E is the identity matrix with the i-th row and j-th rows swapped.

$$\underset{r_i \leftrightarrow r_j}{E} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & & \vdots & \\ 0 & 0 & 0 & 0 & 1 & \cdots \\ \vdots & & \vdots & & \vdots & \\ 0 & \cdots & 1 & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \\ 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$$

The row method of multiplication is the key to matching up a row operation with a particular elementary matrix.
Suppose the multiplication

$$\underset{m\times m}{E} \cdot \underset{m\times n}{A} = \underset{m\times n}{A'}$$

performs a single row operation on A. What must E be? In what follows let $\mathbf{r}_i$ be the i-th row of A for $1 \leq i \leq m$.

Row addition. Suppose E replaces $\mathbf{r}_i$ of A with $\mathbf{r}_i + c\mathbf{r}_j$. Then E is the identity matrix except for its i-th row.

$$\underset{r_i+cr_j}{E} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & & \vdots & \\ \cdots & c & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \\ 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$$

Row reduction as matrix multiplication

Suppose we perform a sequence of row operations on a matrix A. Denote the i-th row operation ρ_i, and denote by $\rho_i(B)$ the result of applying ρ_i to a matrix B.

Our sequence of operations ρ_i would produce the following sequence of matrices:

$$\begin{gathered} A \\ \rho_1(A) \\ \rho_2(\rho_1(A)) \\ \vdots \\ \rho_r(\rho_{r-1}(\dots\rho_2(\rho_1(A)))) \end{gathered}$$

Let ρ_i corresponds to the elementary matrix E_i. Then we represent this same sequence using matrix multiplication:

$$\begin{gathered} A \\ E_1 A \\ E_2 E_1 A \\ \vdots \\ E_r E_{r-1} \cdots E_2 E_1 A \end{gathered}$$

Elementary matrices are invertible

We will use our row operation notation to denote the different types of elementary matrices:

$$\underset{cr_i}{E}, \underset{r_i \leftrightarrow r_j}{E}, \underset{r_i + cr_j}{E}.$$

Theorem 5.1 (Elementary matrix theorem)

Fix n. All elementary matrices are invertible, and their inverses are elementary matrices. In fact:

$$\begin{aligned}
\underset{cr_i}{E}^{-1} &= \underset{\frac{1}{c} r_i}{E} \\
\underset{r_i \leftrightarrow r_j}{E}^{-1} &= \underset{r_i \leftrightarrow r_j}{E} \\
\underset{r_i + cr_j}{E}^{-1} &= \underset{r_i - cr_j}{E}
\end{aligned}$$

Proof.

These are formulas that you can easily check for each type of elementary matrix directly. □

Examples

Fix $n = 3$. Verify that the pairs below are indeed inverses.

We have $\underset{r_1+3r_3}{E} = \begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and thus $\left(\underset{r_1+3r_3}{E}\right)^{-1} = \begin{bmatrix} 1 & 0 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

We have $\underset{2r_3}{E} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$ and thus $\left(\underset{2r_3}{E}\right)^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{2} \end{bmatrix}$

We have $\underset{r_1 \leftrightarrow r_3}{E} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ and thus $\left(\underset{r_1 \leftrightarrow r_3}{E}\right)^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

Interlude on matrix equations

We take a moment to make the following simple, somewhat overdo observation. Namely, we can represent a system of linear equations

$$\begin{array}{ccccccc} a_{11}x_1 & + & a_{12}x_2 & +\cdots+ & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & +\cdots+ & a_{2n}x_n & = & b_2 \\ & \vdots & & \vdots & & \vdots & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & +\cdots+ & a_{mn}x_n & = & b_m \end{array} \qquad (*)$$

as a single matrix equation

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}, \qquad (**)$$

or $A\mathbf{x} = \mathbf{b}$,where $A = [a_{ij}]$, $\mathbf{x} = [x_i]$, $\mathbf{b} = [b_i]$.

Indeed if you expand out the left-hand side of $(**)$ into an $m \times 1$ column vector, using the definition of matrix multiplication, and then invoke the definition of matrix equality, then you obtain the linear system $(*)$.

By the same token, an n-tuple $(s_1, s_2, \ldots, s_n)$ is a solution to the system of equations $(*)$ if and only if its corresponding column vector $\underset{n\times 1}{\mathbf{s}} = [s_i]$ is a solution to the matrix equation $A\mathbf{x} = \mathbf{b}$.

Interlude on matrix equations

In particular, a homogeneous linear system

$$\begin{array}{ccccccc} a_{11}x_1 & + & a_{12}x_2 & +\cdots+ & a_{1n}x_n & = & 0 \\ a_{21}x_1 & + & a_{22}x_2 & +\cdots+ & a_{2n}x_n & = & 0 \\ & \vdots & & \vdots & & \vdots & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & +\cdots+ & a_{mn}x_n & = & 0 \end{array}$$

can be represented as the single matrix equation

$$A\mathbf{x} = \underset{m\times 1}{\mathbf{0}},$$

where $A = [a_{ij}]$ and $\mathbf{x} = [x_i]$; and $(s_1, s_2, \ldots, s_n)$ is a solution to the homogenous system if and only if its corresponding column vector $\underset{n\times 1}{\mathbf{s}} = [s_i]$ is a solution to the matrix equation $A\mathbf{x} = \underset{m\times 1}{\mathbf{0}}$.

We are now ready to state a major theorem about invertibility.

Theorem 5.2 (Invertibility theorem)

Let $A = [a_{ij}]$ be a square $n \times n$ matrix. The following statements are equivalent.

(a) A is invertible.

(b) $A\mathbf{x} = \mathbf{0}$ has a unique solution (the trivial one).

(c) A is row equivalent to I_n, the $n \times n$ identity matrix.

(d) A is a product of elementary matrices.

Proof.

Recall that two show two statements P and Q are equivalent, we must show two implications: $P \Rightarrow Q$, and $Q \Rightarrow P$.

We must show this for each pair of statements above. That would be 6 different pairs and a total of 12 different implications to show!

We ease our work load by showing the following cycle of implications:

$$(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (d) \Rightarrow (a)$$

and using the fact that implication is transitive!

We will complete the proof in class. $\square$

Algorithm for inverses

The proof of the invertibility theorem (IT) provides an algorithm for (1) deciding whether A is invertible, and (2) computing A^{-1} if it exists.

The algorithm:

1. Row reduce A to row echelon form U (keeping track of the elementary matrices you use). The theorem tells us that A is invertible if and only if U has n leading 1's.
2. If this is so, we can keep row reducing to the identity matrix. In terms of matrices we have
$$E_r E_{r-1} \cdots E_1 A = I_n.$$
This means $A^{-1} = E_r E_{r-1} \cdots E_1$.
3. As an added bonus we also have $A = E_1^{-1} E_2^{-1} \cdots E_r^{-1}$, expressing A as a product of elementary matrices.

Inverses with augmented matrix

It can be bothersome to keep track of those E_i, and the order of their multiplication. Instead, we use an augmented matrix method, beginning with the augmented matrix

$$\left[A \;\middle|\; I_n\right],$$

and simply applying row reductions until A on the left becomes I_n, at which point I_n on the right has become A^{-1}.

Why does this work? In terms of the E_i, we have the sequence:

$$\begin{gathered}
\left[A \;\middle|\; I_n\right] \\
\left[E_1 A \;\middle|\; E_1\right] \\
\left[E_2 E_1 A \;\middle|\; E_2 E_1\right] \\
\vdots \\
\left[E_r E_{r-1} \cdots E_1 A \;\middle|\; E_r E_{r-1} \cdots E_1\right] = \left[I_n \;\middle|\; A^{-1}\right]
\end{gathered}$$

Thus when we are done, the RHS of our augmented matrix magically becomes A^{-1}.

Example: take $A = \begin{bmatrix} 1 & 2 & 0 \\ 1 & 2 & 1 \\ -1 & -1 & 3 \end{bmatrix}$.

$$\left[\begin{array}{rrr|rrr} 1 & 2 & 0 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ -1 & -1 & 3 & 0 & 0 & 1 \end{array}\right] \xrightarrow{r_2 - r_1} \left[\begin{array}{rrr|rrr} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 1 & 0 \\ -1 & -1 & 3 & 0 & 0 & 1 \end{array}\right]$$

$$\xrightarrow{r_3 + r_1} \left[\begin{array}{rrr|rrr} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 1 & 0 \\ 0 & 1 & 3 & 1 & 0 & 1 \end{array}\right]$$

(3 leading 1's, thus invertible!)

$$\xrightarrow{r_2 \leftrightarrow r_3} \left[\begin{array}{rrr|rrr} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{array}\right]$$

$$\xrightarrow{r_2 - 3r_3} \left[\begin{array}{rrr|rrr} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & -3 & 1 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{array}\right]$$

$$\xrightarrow{r_1 - 2r_2} \left[\begin{array}{rrr|rrr} 1 & 0 & 0 & -7 & 6 & -2 \\ 0 & 1 & 0 & 4 & -3 & 1 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{array}\right]$$

We conclude that $A^{-1} = \begin{bmatrix} -7 & 6 & -2 \\ 4 & -3 & 1 \\ -1 & 1 & 0 \end{bmatrix}$. On the next slide I show how A^{-1} and A can be written as products of elementary matrices.

Example (contd): in terms of elementary matrices we have

$$E_5 E_4 E_3 E_2 E_1 A = I,$$

where

$$E_1 = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad E_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$E_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad E_4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix}$$

$$E_5 = \begin{bmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Thus we have $A^{-1} = E_5 E_4 E_3 E_2 E_1$ and $A = E_1^{-1} E_2^{-1} E_3^{-1} E_4^{-1} E_5^{-1}$.

This shows how both of these matrices can be written as products of elementary matrices (recall that each E_i^{-1} is also elementary).

1:6: executive summary

Definitions: none.

Procedures: deciding when a linear system $A\mathbf{x} = \mathbf{b}$ is consistent.

Theorems: invertibility theorem (expanded), AB invertible if and only if A and B are invertible, A is a left inverse of B if and only if A is a right inverse of B.

1:6: expanded invertibility theorem

We add two more equivalent statements of invertibility to our invertibility theorem (IT).

Theorem 6.1 (Expanded invertibility theorem)

Let $A = [a_{ij}]$ be a square $n \times n$ matrix. The following statements are equivalent.

(a) A is invertible.

(b) $A\mathbf{x} = \mathbf{0}$ has a unique solution (the trivial one).

(c) A is row equivalent to I_n, the $n \times n$ identity matrix.

(d) A is a product of elementary matrices.

(e) $A\mathbf{x} = \mathbf{b}$ has a *unique* solution for every $n \times 1$ column vector $\mathbf{b}$.

(f) $A\mathbf{x} = \mathbf{b}$ has a solution for every $n \times 1$ column vector $\mathbf{b}$.

Proof.

We already know statements (a)-(d) are equivalent. Adding (e) and (f) to this list is left as an exercise. $\square$

Corollary 6.1.1

Let A and B be $n \times n$. Then AB is invertible if and only if A and B are both invertible.

Proof.

We have already proved the $\Leftarrow$ direction of this equivalnce.

For the $\Rightarrow$ direction, assume AB is invertible and let C be its inverse, so that $C(AB) = (AB)C = I_n$.
We first prove B is invertible, using equivalent statement (b) of IT; that is we will prove the implication $B\mathbf{x} = \mathbf{0} \Rightarrow \mathbf{x} = \mathbf{0}$.

$$\begin{aligned} B\mathbf{x} = \mathbf{0} \quad &\Rightarrow \quad AB\mathbf{x} = \mathbf{0} \\ &\Rightarrow \quad \mathbf{x} = \mathbf{0} \ \text{ (since } AB \text{ invertible).} \end{aligned}$$

This proves B is invertible, and hence that B^{-1} exists.

Next we prove A is invertible, by explicitly exhibiting an inverse: namely, $A^{-1} = BC$.

Indeed we have $A(BC) = (AB)C = I_n$, from above. For the other direction we have

$$\begin{aligned} C(AB) = I \quad &\Leftrightarrow \quad CA = B^{-1} \ \text{ (mult. both sides on right by } B^{-1}\text{)} \\ &\Leftrightarrow \quad (BC)A = I_n \ \text{(mult. both sides on left by } B\text{).} \end{aligned}$$

This proves A and B are both invertible, and completes our proof. $\square$

Corollary 6.1.2

Let A and B be $n \times n$.

(i) $BA = I_n \Rightarrow AB = I_n$.

(ii) $AB = I_n \Rightarrow BA = I_n$.

In other words, to show B is the inverse of A it is enough to show either that it is a left-inverse ($BA = I_n$), or a right-inverse ($AB = I_n$).

Proof.

It is enough to prove the first implication: the second then follows by exchanging the roles of A and B!

Suppose $BA = I_n$. I will first show that A is invertible. Indeed, suppose $A\mathbf{x} = \mathbf{0}$. Then $BA\mathbf{x} = \mathbf{0}$. But $BA = I_n$, and $I\mathbf{x} = \mathbf{0}$ implies $\mathbf{x} = \mathbf{0}$. It follows from statement (b) of IT that A is invertible.

Now that we know A^{-1} exists we have

$$\begin{aligned} BA = I_n \quad &\Rightarrow \quad B = A^{-1} \ \text{(mult. both sides on right by } A^{-1}\text{)} \\ &\Rightarrow \quad AB = I_n \ \text{(mult. both sides on left by } A\text{)} \end{aligned}$$

□

When is a linear system consistent

Consider a general linear equation

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

which we represent as a matrix equation

$$\underset{m\times n}{A} \cdot \underset{n\times 1}{\mathbf{x}} = \underset{m\times 1}{\mathbf{b}}.$$

Question: what conditions on A and $\mathbf{b}$ guarantee the system is consistent; equivalently, when we can solve the matrix equation above?

Partial answer: the preceding discussion gives us a partial answer. If A happens to be an invertible matrix (in particular, it must be square!), then the equation is guaranteed to have a (unique) solution. We just solve for $\mathbf{x}$ directly in this case: $\mathbf{x} = A^{-1}\mathbf{b}$.

Otherwise: if A is not invertible, then we resort to the theory of Gaussian elimination to answer the question. Take the augmented matrix $[A|\mathbf{b}]$, row reduce to row echelon form $[U|\mathbf{b}']$ and reason from there. The example that follows illustrates this.

Example

Find all b_1, b_2, b_3 for which the following system is consistent:

$$\begin{aligned} x_1 + x_2 + 2x_3 &= b_1 \\ x_1 \phantom{{}+x_2} + x_3 &= b_2 \\ 2x_1 + x_2 + 3x_3 &= b_3 \end{aligned}$$

Solution: We consider the augmented matrix $[A|\mathbf{b}]$ and row reduce

$$\left[\begin{array}{ccc|c} 1 & 1 & 2 & b_1 \\ 1 & 0 & 1 & b_2 \\ 2 & 1 & 3 & b_3 \end{array}\right] \xrightarrow{\text{row red.}} \left[\begin{array}{ccc|r} \boxed{1} & 1 & 2 & b_1 \\ 0 & \boxed{1} & 1 & b_2 - b_1 \\ 0 & 0 & 0 & b_3 - b_2 - b_1 \end{array}\right]$$

Note: since the 3×3 matrix on the left only 2 leading 1's, we know A is not invertible. But of course that doesn't mean that the given system is necessarily inconsistent! Indeed, the theory of Gaussian elimination tells us that the system will be consistent if and only if $b_3 - b_2 - b_1 = 0$.

We conclude the original system is consistent if and only if $b_3 = b_2 + b_1$: equivalently, iff

$$\mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ b_1 + b_2 \end{bmatrix}.$$

Diagonal, triangular and symmetric matrices

Lastly, we officially introduce some special families of square matrices, as well as a corresponding invertibility theorem. The proof of the latter will be done in class.

Definition 6.1

Let $A = [a_{ij}]$ be $n \times n$. We say

(i) A is **diagonal** if $a_{ij} = 0$ for all (i, j) with $i \neq j$. ("A is zero off the diagonal.")

(ii) A is **upper triangular** if $a_{ij} = 0$ for all (i, j) with $j > i$. ("A is zero below the diagonal.")

(iii) A is **lower triangular** if $a_{ij} = 0$ for all (i, j) with $i > j$. ("A is zero above the diagonal.")

(iv) A is **triangular** if A is upper triangular or lower triangular.

(v) A is **symmetric** if $A^T = A$. (Equivalently, $a_{ij} = a_{ji}$ for all $1 \leq i, j \leq n$.)

Theorem 6.2 (Invertibility of triangular matrices)

Let $A = [a_{ij}]$ be a triangular $n \times n$ matrix. Then A is invertible if and only if $a_{ii} \neq 0$ for all $1 \leq i \leq n$.
In other words, A is invertible if and only if the diagonal entries of A are all nonzero.

2.1-2.3: executive summary

Definitions: determinant, minors, cofactors.

Procedures: determinant.

Theorems: $\det(A) \neq 0$ iff A invertible; $\det(AB) = \det(A)\det(B)$, how row reduction affects determinant, some other determinant properties.

2.1: determinants

The determinant is a map that assigns to a square matrix A a scalar, called $\det(A)$:

$$A \mapsto \det(A).$$

As you will see, the definition of the determinant is far from intuitive; nonetheless the determinant will be very useful to us. In particular we shall see that

$$A \text{ is invertible } \Leftrightarrow \det(A) \neq 0.$$

We will define the determinant *recursively*; this means that when computing $\det A$ for an $n \times n$ matrix will have to compute the determinant of certain smaller matrices. We begin with the smallest cases: $n = 1$ and $n = 2$.

Definition 1.1 (Small cases)

Let $A = [a]$ be a 1×1 matrix. Then $\det(A) = a$.

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then $\det(A) = ad - bc$.

Definition 1.2

Let A be $n \times n$.

The ij**-th minor of** A, denoted M_{ij}, is the determinant of the submatrix of A obtained by deleting the i-th row and j-th column.

The ij**-th cofactor of** A, denoted C_{ij}, is defined as

$$C_{ij} = (-1)^{i+j} M_{ij}.$$

Definition 1.3

Let $A = [a_{ij}]_{n \times n}$.

Expansion along row. Pick any i. Then we define

$$\det(A) = \sum_{j=1}^{n} a_{ij} C_{ij} = a_{i1} C_{i1} + a_{i2} C_{i2} \cdots + a_{in} C_{in}$$

Expansion along column. Pick any j. Then we define

$$\det(A) = \sum_{i=1}^{n} a_{ij} C_{ij} = a_{1j} C_{1j} + a_{2j} C_{2j} \cdots + a_{nj} C_{nj}.$$

Let $A = [a_{ij}]_{n \times n}$.
Expansion along row. Pick any i. Then we define

$$\det(A) = \sum_{j=1}^{n} a_{ij} C_{ij} = a_{i1} C_{i1} + a_{i2} C_{i2} \cdots + a_{in} C_{in}$$

Expansion along column. Pick any j. Then we define

$$\det(A) = \sum_{i=1}^{n} a_{ij} C_{ij} = a_{1j} C_{1j} + a_{2j} C_{2j} \cdots + a_{nj} C_{nj}.$$

Comments

1. For this to be well-defined, we should get the same value no matter which column or row we decide to use in order to compute the determinant. This is not at all obvious and technically needs to be proved!
2. The definition $\det(A)$ involves cofactors, which themselves are computed by invoking the definition of the determinant on a smaller submatrix. This means we keep invoking the recursive definition until we get down to 2×2 matrices, where the determinant is given by a formula.
3. When A is written as a rectangular array, we use vertical lines to denote determinant: e.g., $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$.

Example

Compute $\det(A)$ for

$$A = \begin{bmatrix} 2 & 1 & 0 & 3 \\ 0 & 2 & 1 & 0 \\ 4 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Choose the row/column along which you wish to expand wisely! I pick the third column for its preponderance of 0's and 1's:

$$\begin{aligned}
\det(A) &= 0M_{13} - M_{23} + M_{33} - 0M_{43} \\
&= -\begin{vmatrix} 2 & 1 & 3 \\ 4 & 2 & 0 \\ 0 & 0 & 2 \end{vmatrix} + \begin{vmatrix} 2 & 1 & 3 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{vmatrix} \\
&= -2\begin{vmatrix} 2 & 1 \\ 4 & 2 \end{vmatrix} + 2\begin{vmatrix} 2 & 1 \\ 0 & 2 \end{vmatrix} \\
&= -0 + 8 = \boxed{8}.
\end{aligned}$$

What was I thinking? I should have picked the last row!

The freedom to compute the determinant using any row or column leads to two important, if obvious, properties.

Theorem 1.1

Let A be $n \times n$. If A has a row or column of zeros, then $\det(A) = 0$.

Proof.

Expand along the row (or column) of zeros. $\square$

Theorem 1.2

For any $n \times n$ matrix A we have $\det(A^T) = \det(A)$.

Proof.

Expanding along the i-th row of A is the same as expanding along the i-th column of A^T. $\square$

Because of its recursive definition, we often resort to a proof by induction to show some property of determinants holds.

Theorem 1.3

The determinant of a triangular matrix is the the product of its diagonal entries; that is, if $A = [a_{ij}]$ is triangular, then $\det(A) = a_{11} \cdot a_{22} \cdots a_{nn}$.

Proof.

We will prove this for lower triangular matrices, the proof for upper triangular matrices being exactly similar.
We proceed by induction on the size n of the matrix.

Base case: n=1. If $A = [a]$ is 1×1, then $\det(A) = a$, which is the product of its diagonal entries.

Induction step. We assume that the proposition is true for all lower triangular matrices of size $n - 1$.
Let $A = [a_{ij}]_{n \times n}$. We compute $\det(A)$ by expanding along the top row. Since A is lower triangular all the entries are 0 except a_{11} and we get $\det(A) = a_{11} M_{11}$.
Now $M_{11} = \det(\tilde{A})$, where $\tilde{A}$ is the submatrix of A obtained by deleting the first row and column. This matrix is also lower triangular with diagonal entries $a_{22}, a_{33}, \ldots, a_{nn}$. By the induction hypothesis $\det(\tilde{A}) = a_{22} \cdot a_{33} \cdots a_{nn}$.
Thus $\det(A) = a_{11} \det(\tilde{A}) = a_{11} \cdot a_{22} \cdots a_{nn}$, as claimed. $\square$

Theorem 1.4

Let A be $n \times n$, with $n \geq 2$, and let $\tilde{A}$ be the matrix obtained by swapping two rows of A. Then $\det(A) = -\det(\tilde{A})$.
The same is true if $\tilde{A}$ is the result of swapping two columns of A.

Proof.

The second statement about swapping columns follows from the first and the fact that $\det A = \det A^T$. I leave the details to you.
To prove the first statement we proceed by induction on n.

Base case: $n = 2$. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then $\tilde{A} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$. We have $\det(A) = ad - cb = -(cb - ad) = -\det(\tilde{A})$, as claimed.

Induction step. Assume $n \geq 3$. We assume by induction that the result holds for any square matrices of size $n-1$.

Suppose $\tilde{A}$ is the result of swapping the i-th and j-th rows of A. Compute the determinants of A and $\tilde{A}$ by expanding along any row other than the i-th or j-th rows. This is possible since $n \geq 3$. Call this the k-th row.

The expansions for $\det(A)$ and $\det(\tilde{A})$ differ only in terms of their minors, $M_{k\ell}$ and $\tilde{M}_{k\ell}$, and these differ only in that the square matrices of size $n-1$ involved have two rows swapped: the ones corresponding the i-th and j-th rows of A!

By induction the determinants of these matrices differ by a factor of (-1). Thus $M_{k\ell} = -\tilde{M}_{k\ell}$ for all (k, ℓ), from which it follows that $\det(A) = -\det(\tilde{A})$. $\square$

2.2: row operations and the determinant

We denote our various elementary row operations as

$$\rho_{c\cdot r_i}, \rho_{r_i \leftrightarrow r_j}, \text{ and } \rho_{r_i + cr_j},$$

as usual.

Theorem 2.1

Let A be $n \times n$. Then:

(i) $\det(\rho_{c\cdot r_i}(A)) = c\det(A)$,

(ii) $\det(\rho_{r_i \leftrightarrow r_j}(A)) = -\det(A)$,

(iii) $\det(\rho_{r_i + cr_j}(A)) = \det(A)$.

Equivalently, we have:

(i) $\det(\underset{c\cdot r_i}{E} \cdot A) = c\det(A)$,

(ii) $\det(\underset{r_i \leftrightarrow r_j}{E} \cdot A) = -\det(A)$,

(iii) $\det(\underset{r_i + cr_j}{E} \cdot A) = \det(A)$.

Theorem 2.2

Let A be $n \times n$. Then:

(i) $\det(\underset{c \cdot r_i}{E} \cdot A) = c \det(A)$,

(ii) $\det(\underset{r_i \leftrightarrow r_j}{E} \cdot A) = -\det(A)$,

(iii) $\det(\underset{r_i + cr_j}{E} \cdot A) = \det(A)$.

Setting $A = I_n$ in the last theorem, we get formulas for the determinant of an elementary matrix.

Corollary 2.2.1

(i) $\det(\underset{c \cdot r_i}{E}) = c$,

(ii) $\det(\underset{r_i \leftrightarrow r_j}{E}) = -1$,

(iii) $\det(\underset{r_i + cr_j}{E}) = 1$.

We can now use row operations to simplify the computation of $\det(A)$ as follows. We row reduce A to some simpler matrix B, yielding a matrix equation of the form

$$E_r E_{r-1} \cdots E_1 A = B.$$

From our theorem above, it follows that

$$\begin{aligned}
\det(B) &= \det(E_r)\det(E_{r-1}\cdots E_1 A) \\
&= \det(E_r)\det(E_{r-1})\det(E_{r-2}\cdots E_1 A) \\
&= \vdots \\
&= \det(E_r)\det(E_r - 1)\cdots\det(E_1)\det(A)
\end{aligned}$$

and thus that

$$\det(A) = \frac{\det(B)}{\det(E_r)\det(E_{r-1})\cdots\det(E_1)}.$$

As an example of this method we can easily prove the following corollary.

Corollary 2.2.2

Let A be $n \times n$, and denote the rows of A by $\mathbf{r}_i$. If $\mathbf{r}_i = c\mathbf{r}_j$ for some $i \neq j$ and some scalar c, then $\det(A) = 0$.
Similarly if A has two columns that are scalar multiples of one another, then $\det(A) = 0$.

Proof.

We assume $\mathbf{r}_i = c\mathbf{r}_j$ for some $i \neq j$ and some scalar c.
Using the row method of matrix multiplication, we see that the matrix

$$\tilde{A} = \underset{\mathbf{r}_i - cr_j}{E} \cdot A$$

has a row of zeros in the i-th row. We conclude that $\det(\tilde{A}) = 0$.
It follows that $0 = \det(\underset{\mathbf{r}_i - cr_j}{E} \cdot A) = \det \underset{\mathbf{r}_i - cr_j}{E} \det A$. Since $\det \underset{\mathbf{r}_i - cr_j}{E} \neq 0$, we must have $\det A = 0$.
The statement about columns follows from the statement about rows and the fact that $\det(A^T) = \det(A)$. $\square$

2.3: further properties of the determinant

Our analysis of how the determinant changes with row operations leads to a number of very important theorems.

Theorem 3.1 (Determinant is multiplicative)

Let A, B be $n \times n$. Then

$$\det(AB) = \det(A)\det(B).$$

Comment: please observe, the same is NOT true of addition!

$$\det(A+B) \neq \det(A) + \det(B).$$

Proof.

Your instructor will do this in class. $\square$

Theorem 3.2 (Determinant and invertibility)

Let A be $n \times n$. Then A is invertible if and only if $\det(A) \neq 0$.

Proof.

($\Rightarrow$) I'll prove this direction as a chain of implications.

$$
\begin{aligned}
A \text{ invertible} &\Rightarrow AA^{-1} = I_n \text{ for some matrix } A^{-1} \\
&\Rightarrow \det(AA^{-1}) = \det I_n \\
&\Rightarrow \det(AA^{-1}) = 1 && (\text{since } \det I_n = 1) \\
&\Rightarrow \det A \ \det A^{-1} = 1 && (\text{by Th. } 3.1) \\
&\Rightarrow \det A \neq 0 && (\text{otherwise product would be } 0)
\end{aligned}
$$

($\Leftarrow$) I'll prove the contrapositive of this direction: that is, if A is not invertible, then $\det A = 0$. Suppose A is not invertible, and suppose A reduces to the reduced row echelon matrix U. By the invertibility theorem, U is not the identity matrix. Thus one of its diagonal entries must be 0, and hence $\det U = 0$.

This means we have $E_r E_{r-1} \cdots E_1 A = U$, for some elementary matrices E_i, in which case $\det E_r \det E_{r-1} \cdots \det E_1 \det A = \det U = 0$, since det is multiplicative. Since the E_i are invertible, $\det E_i \neq 0$ (as shown above). It follows that $\det A = 0$. $\square$

Adjoint formula for A^{-1}

Its worth recording also that we can use the determinant to give an actual formula for computing the inverse of a matrix!
We all love formulas, but keep in mind that it is faster to use our Gaussian elimination algorithm for computing A^{-1}.

Theorem 3.3 (Adjoint formula)

Let A be $n \times n$, and suppose $\det(A) \neq 0$.
We define the **adjoint matrix** of A as

$$\operatorname{adj}(A) = ([C_{ij}])^T ;$$

that is, the ij-th entry of the adjoint matrix is the ji-th cofactor of A.
Then

$$A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A).$$

Proof sketch.

Let $B = \operatorname{adj} A$, and let $c = \det A$. Using the definition of $\operatorname{adj} A$ and properties of the determinant, you can in fact show directly that

$$AB = cI_n.$$

It follows that $A^{-1} = \frac{1}{c} B = \frac{1}{\det A} \operatorname{adj} A$. $\square$

Our growing invertibility theorem

Thanks to Theorem 3.2, our invertibility theorem has grown by one statement.

Theorem 3.4 (Invertibility theorem)

Let A be $n \times n$. The following statements are equivalent.

(a) A is invertible.

(b) $A\mathbf{x} = \mathbf{0}$ has a unique solution (the trivial one).

(c) A is row equivalent to I_n, the $n \times n$ identity matrix.

(d) A is a product of elementary matrices.

(e) $A\mathbf{x} = \mathbf{b}$ has a solution for every $n \times 1$ column vector $\mathbf{b}$.

(f) $A\mathbf{x} = \mathbf{b}$ has a *unique* solution for every $n \times 1$ column vector $\mathbf{b}$.

(g) $\det(A) \neq 0$.

3.1: executive summary

Definitions: general vector space.

Procedures: deciding whether something is a vector space

Theorems: no theorems, but a list of familiar examples to get acquainted with.

Interlude on abstraction

In our study of matrices, we have seen that operations from real number arithmetic (addition, subtraction, multiplication) have “analogues” in the world of matrices (matrix addition, matrix subtraction, matrix multiplication).

The question naturally arises as to what other types of mathematical objects (besides real numbers or matrices) admit analogous operations, and further, what we can say about these analogous systems.

A common technique in mathematics to help investigate such questions, is to distill the important properties of the motivating operations into a list of axioms, and then attempt to prove statements about any system of operations that satisfies these axioms.

We now embark on just such an endeavor. In the current setting we are concerned with two important operations defined on matrices: matrix addition ($A + B$) and scalar multiplication (cA). As you recall from 1.3, these two operations satisfy many useful properties: e.g, commutativity, associativity, distributivity, etc.

We axiomatize this setting by considering *any* system admitting two operations like this: our axioms will stipulate the existence of these two operations, as well as the fact that the operations satisfy the relevant properties (commutativity, associativity, etc.). A system satisfying these axioms is called a vector space.

3.1: vector spaces

Definition 1.1

A **(real)**[1] **vector space**is a set V together with two operations defined on V: a multiplication by (real) scalars

$$\begin{aligned} \mathbb{R} \times V &\to V \\ (r, \mathbf{v}) &\mapsto r\mathbf{v}, \end{aligned}$$

called **scalar multiplication**, and an addition of elements of V

$$\begin{aligned} V \times V &\to V \\ (\mathbf{v}, \mathbf{w}) &\mapsto \mathbf{v} + \mathbf{w}, \end{aligned}$$

called **vector addition**.

Furthermore, these two operations must satisfy the axioms listed on the next slide!

[1] There is a notion of *complex* vector space as well. In this course it is assumed the vector space is real. As such, we will often drop this modifier.

Definition contd.

(a) $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$ (addition is commutative)

(b) $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ (addition is associative)

(c) There is an element $\mathbf{0} \in V$ satisfying
$\mathbf{0} + \mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$. (V has an additive identity)

(d) For all $\mathbf{v} \in V$, there is an element $-\mathbf{v} \in V$
s.t. $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$. ($V$ has additive inverses)

(e) $r(\mathbf{u} + \mathbf{v}) = r\mathbf{u} + r\mathbf{v}$ (scal. mult. distributes over vector sums)

(f) $(r + s)\mathbf{v} = r\mathbf{v} + s\mathbf{v}$ (sum of scalars distributes)

(g) $r(s\mathbf{v}) = (rs)\mathbf{v}$ (scal. mult. is assoc.)

(h) $1\mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$ (scalar 1 acts as identity)

Elements of a vector space V are called **vectors**.

A **linear combination** in a vector space is any expression of the form
$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_r\mathbf{v}_r$, where $c_i \in \mathbb{R}$ and $\mathbf{v}_i \in V$ for all $1 \leq i \leq r$.

Examples: M_{mn}

As mentioned above, our inspiration for the abstract notion of a vector space comes from matrices. Let's make explicit how they constitute an example.

Fix an m and n and let $V = M_{mn}$ be the set of all $m \times n$ matrices.

Addition and scalar multiplication. Given any $A = [a_{ij}]$, $B = [b_{ij}]$, define:

$$\begin{aligned} rA &:= [ra_{ij}], \text{ (the usual scalar multiplication)} \\ A + B &:= [a_{ij} + b_{ij}], \text{ (the usual matrix addition)} \end{aligned}$$

Additive identity and inverses. Set:

$$\begin{aligned} \mathbf{0} &:= 0_{mn}, \text{ the } m \times n \text{ zero matrix} \\ -A &:= [-a_{ij}]. \end{aligned}$$

We have already seen in 1.3 that these operations, along with our choices of zero vector and additive inverses, satisfy all the axioms of our vector space definition. Thus M_{mn}, along with these operations, constitutes a vector space.

Examples: $\mathbb{R}^n$

We define $\mathbb{R}^n$ to be the set of all n-tuples: i.e., $\mathbb{R}^n = \{(t_1, t_2, \ldots t_n) : t_i \in \mathbb{R}\}$. We call $\mathbb{R}^n$ n-**space**, call elements of $\mathbb{R}^n$ n-**vectors**, and denote elements of $\mathbb{R}^n$ with bold, lowercase letters: typically, $\mathbf{v}$, $\mathbf{w}$, and $\mathbf{u}$.

Define a vector space structure on $\mathbb{R}^n$ as follows.
Addition and scalar multiplication. Given any $\mathbf{v} = (v_1, \ldots, v_n)$ and $\mathbf{w} = (w_1, \ldots, w_n)$ in $\mathbb{R}^n$ define:

$$\begin{aligned} r\mathbf{v} &:= (rv_1, rv_2, \ldots, rv_n) \text{ for all } r \in \mathbb{R}, \\ \mathbf{v} + \mathbf{w} &:= (v_1 + w_1, \ldots, v_n + w_n) \end{aligned}$$

Additive identity and inverses. Set:

$$\begin{aligned} \mathbf{0} &:= (0, 0, \ldots, 0) \\ -\mathbf{v} &:= (-v_1, -v_2, \ldots, -v_n). \end{aligned}$$

The difference between $\mathbb{R}^n$ and M_{1n} (row vectors) is simply one of notation (parenthesis instead of bracket). In particular, it follows immediately from the last example that $\mathbb{R}^n$ with these operations is a vector space.
Furthermore I reserve the right to identify $\mathbb{R}^n$ with M_{1n}, as well as M_{n1} (column vectors), in any given example. I will always make my choice explicit: e.g. "Let $V = \mathbb{R}^n$, with elements treated as column vectors".

Examples: the trivial vector space

Vector spaces of the form $\mathbb{R}^n$ will be our main object of study. It is important to observe, however, that there are many other, more exotic vector spaces. In other words, you cannot always assume that a vector is an n-vector. We now introduce some of these more exotic examples, starting with the trivial vector space.

Let $V = \{\mathbf{v}\}$ be a set containing exactly one element.

Addition and scalar multiplication. Define:

$$\begin{aligned} r\mathbf{v} &:= \mathbf{v} \text{ for all } r \in \mathbb{R}, \\ \mathbf{v} + \mathbf{v} &:= \mathbf{v} \end{aligned}$$

Additive identity and inverses. Set:

$$\begin{aligned} \mathbf{0} &:= \mathbf{v} \\ -\mathbf{v} &:= \mathbf{v}. \end{aligned}$$

It follows easily that $V = \{\mathbf{v}\}$, along with these operations and choices of zero vector and additive inverses, satisfies the definition of a vector space.

We call V the **trivial (or zero) vector space**, and denote it $V = \{\mathbf{0}\}$. (Note that the single element of the trivial vector space is always the zero vector of the space. Hence the notation.)

Examples: $\mathbb{R}^\infty$

Definition 1.2

We define $\mathbb{R}^\infty$ to be the set of all infinite sequences of real numbers: i.e.,

$$\mathbb{R}^\infty = \{(t_1, t_2, t_3, \dots)\colon\, t_i \in \mathbb{R}\}.$$

Define a vector space structure on $\mathbb{R}^\infty$ as follows.
Addition and scalar multiplication. Given any $\mathbf{v} = (v_1, v_2, \dots)$ and $\mathbf{w} = (w_1, w_2, \dots)$ in $\mathbb{R}^n$ define:

$$\begin{aligned} r\mathbf{v} &:= (rv_1, rv_2, \dots) \text{ for all } r \in \mathbb{R}, \\ \mathbf{v} + \mathbf{w} &:= (v_1 + w_1, v_2 + w_2, \dots) \end{aligned}$$

Additive identity and inverses. Set:

$$\begin{aligned} \mathbf{0} &:= (0, 0, \dots) \\ -\mathbf{v} &:= (-v_1, -v_2, \dots). \end{aligned}$$

It is easy to show $\mathbb{R}^\infty$ with these operations forms a vector space.

Examples: $C^\infty(X)$

Let $X \subset \mathbb{R}$ be any interval of any sort: e.g. $X = [a, b]$, $X = (-\infty, \infty)$, $X = (-\infty, b]$, etc. Define $V = C^\infty(X)$ to be the set of all infinitely-differentiable real-valued functions with domain X.

Addition and scalar multiplication. Given any elements $f, g \in C^\infty(X)$, define:

$$\begin{aligned} rf &:= \text{the function defined as } (rf)(x) = rf(x) \text{ for all } r \in \mathbb{R}, \\ f + g &:= \text{the function defined as } (f+g)(x) = f(x) + g(x). \end{aligned}$$

In other words, vector scalar multiplication is defined to be scalar multiplication of functions, and vector addition is defined to be function addition.

Additive identity and inverses. Set:

$$\begin{aligned} \mathbf{0} &:= \text{the zero function } 0_X, \text{ defined as } 0_X(x) = 0 \text{ for all } x \in X. \\ -f &:= \text{the function defined as } (-f)(x) = -f(x) \text{ for all } x \in X. \end{aligned}$$

The fact that $C^\infty(X)$ with these operations forms a vector space follows from familiar properties of function arithmetic.

Take a moment to let the exotic quality of this example sink in. Our "vectors" in this example are functions! Whereas we can concretely describe the general element of $\mathbb{R}^3$ ((a, b, c)) or even $\mathbb{R}^n$ ($(r_1, r_2, \dots, r_n)$), this is not so in $C^\infty(X)$: the general element is just some infinitely differentiable function f. I can give you plenty of examples of elements (e.g., $f(x) = x^2$, $f(x) = \sin x - e^x$, etc.), but I cannot express the general element in any kind of finite way.

When proving a general fact about vector spaces we can only invoke the defining axioms the vector space satisfies; we cannot assume the vectors of the space are of any particular form. For example, we cannot assume vectors of V are n-tuples, or matrices, etc.

We end with an example of such an axiomatic proof.

Theorem 1.1

Let V be a vector space.

(a) $0\mathbf{v} = \mathbf{0}$ for all $\mathbf{v} \in V$.

(b) $k\mathbf{0} = \mathbf{0}$ for all $k \in \mathbb{R}$.

(c) $(-1)\mathbf{v} = -\mathbf{v}$ for all $\mathbf{v} \in V$.

(d) If $k\mathbf{u} = \mathbf{0}$, then $k = 0$ or $\mathbf{u} = \mathbf{0}$.

Proof.

We prove (a), leaving (b)-(d) as an exercise.
First observe that $0\mathbf{v} = (0+0)\mathbf{v}$, since $0 = 0+0$.

By Axiom (e) we have $(0+0)\mathbf{v} = 0\mathbf{v} + 0\mathbf{v}$. Thus $0\mathbf{v} = 0\mathbf{v} + 0\mathbf{v}$.

Add $-0\mathbf{v}$, the additive inverse of $0\mathbf{v}$, to both sides of the last equation:

$$-0\mathbf{v} + 0\mathbf{v} = -0\mathbf{v} + 0\mathbf{v} + 0\mathbf{v}. \tag{$*$}$$

The left-hand side of $(*)$ is $\mathbf{0}$, by Axiom (d). The right-hand side is $\mathbf{0} + 0\mathbf{v} = 0\mathbf{v}$, by Axiom (c). We conclude that $\mathbf{0} = 0\mathbf{v}$. □

3.3: executive summary

Definitions: subspace, linear combination, span, polynomial spaces P and P_n, null T, range T.

Procedures: proving something is/isn't a subspace; computing the span of a set of vectors, computing null T and range T for a linear transformation.

Theorems: intersection of subspaces is a subspace, span$(\{\mathbf{v}_1, \mathbf{v}_2, \dots\})$ is a subspace, null T is a subspace, range T is a subspace.

3.3: subspaces

Definition 3.1

Let V be a vector space. A subset $W \subseteq V$ is a **subspace** of V if

(i) $\mathbf{0} \in W$,

(ii) $\mathbf{w}_1, \mathbf{w}_2 \in W \Rightarrow \mathbf{w}_1 + \mathbf{w}_2 \in W$, (i.e., W is **closed under addition**),

(iii) $\mathbf{w} \in W \Rightarrow k\mathbf{w} \in W$ for all $k \in \mathbb{R}$ (i.e., W is **closed under scalar multiplication**).

Comments

(1) You may see slightly different definitions for subspace in the literature: e.g., some define a subspace to be a subset $W \subseteq V$ which, under the operations of addition and scalar multiplication of V, is itself a vector space. I prefer mine as it gives you a hands-on method of deciding whether a given subset of $W \subseteq V$ is in fact a sub*space* of V: namely, determine whether each of properties (i)-(iii) hold for W.

(2) Each of properties (ii) and (iii) is stated as an implication. Thus when verifying these, as always we assume the antecedent and prove the consequent.

Example

Let $V = \mathbb{R}^2$ and let $W \subseteq V$ be the subset $W = \{(t,t) \in \mathbb{R}^2 \colon t \in \mathbb{R}\}$. We claim W is a subspace.

Proof.

We must show properties (i)-(iii) hold for W.

(i) The zero element of V is $\mathbf{0} = (0,0)$, which is certainly of the form (t,t). Thus $\mathbf{0} \in W$.

(ii) We must prove the implication $\mathbf{w}_1, \mathbf{w}_2 \in W \Rightarrow \mathbf{w}_1 + \mathbf{w}_2 \in W$.

$$\begin{aligned}
\mathbf{w}_1, \mathbf{w}_2 \in W \quad &\Rightarrow \quad \mathbf{w}_1 = (t,t), \mathbf{w}_2 = (s,s) \text{ for some } t, s \in \mathbb{R} \\
&\Rightarrow \quad \mathbf{w}_1 + \mathbf{w}_2 = (t+s, t+s) \\
&\Rightarrow \quad \mathbf{w}_1 + \mathbf{w}_2 \in W.
\end{aligned}$$

(iii) We must prove the implication $\mathbf{w} \in W \Rightarrow k\mathbf{w} \in W$.

$$\begin{aligned}
\mathbf{w} \in W \quad &\Rightarrow \quad \mathbf{w} = (t,t) \\
&\Rightarrow \quad k\mathbf{w} = (kt, kt) \\
&\Rightarrow \quad k\mathbf{w} \in W
\end{aligned}$$

$\square$

Example

Let $V = \mathbb{R}^n$, and treat elements of V as column vectors. Fix a vector $\mathbf{v}_0 \in V$. Let $W \subseteq V$ be the subset $W = \{\mathbf{w} \in \mathbb{R}^n \colon \mathbf{v}_0^T \mathbf{w} = 0\}$. We claim W is a subspace.

Proof.

We must show properties (i)-(iii) hold for W.

(i) The zero element of V is $\mathbf{0} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$. Clearly $\mathbf{v}_0^T \mathbf{0} = 0$. Thus $\mathbf{0} \in W$.

(ii) We must prove the implication $\mathbf{w}_1, \mathbf{w}_2 \in W \Rightarrow \mathbf{w}_1 + \mathbf{w}_2 \in W$.

$$
\begin{aligned}
\mathbf{w}_1, \mathbf{w}_2 \in W \quad &\Rightarrow \quad \mathbf{v}_0^T \mathbf{w}_1 = 0, \mathbf{v}_0^T \mathbf{w}_2 = 0 \\
&\Rightarrow \quad \mathbf{v}_0^T (\mathbf{w}_1 + \mathbf{w}_2) = \mathbf{v}_0^T \mathbf{w}_1 + \mathbf{v}_0^T \mathbf{w}_2 = 0 + 0 = 0 \\
&\Rightarrow \quad \mathbf{w}_1 + \mathbf{w}_2 \in W.
\end{aligned}
$$

(iii) We must prove the implication $\mathbf{w} \in W \Rightarrow k\mathbf{w} \in W$.

$$
\begin{aligned}
\mathbf{w} \in W \quad &\Rightarrow \quad \mathbf{v}_0^T \mathbf{w} = 0 \\
&\Rightarrow \quad \mathbf{v}_0^T (k\mathbf{w}) = k\mathbf{v}_0^T \mathbf{w} = k0 = 0 \\
&\Rightarrow \quad k\mathbf{w} \in W
\end{aligned}
$$

$\square$

Lines and planes

Recall that a line in $\mathbb{R}^2$ containing the origin $(0,0)$ can be expressed as the set of solutions $(x_1, x_2) \in \mathbb{R}^2$ to an equation of the form

$$ax_1 + bx_2 = 0, \text{ or } \begin{bmatrix} a \\ b \end{bmatrix}^T \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = 0$$

Similarly, a plane in $\mathbb{R}^3$ containing the origin $(0,0,0)$ can be expressed as the the set of solutions (x_1, x_2, x_3) to an equation of the form

$$ax_1 + bx_2 + cx_3 = 0, \text{ or } \begin{bmatrix} a \\ b \\ c \end{bmatrix}^T \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = 0.$$

By the previous example we see that lines in $\mathbb{R}^2$ containing the origin are subspaces, as are planes in $\mathbb{R}^3$ containing the origin! Both can be expressed in the form $W = \left\{\mathbf{x} \colon \mathbf{v}_0^T\mathbf{x} = 0\right\}$: take $\mathbf{v}_0 = (a, b)$ in the first case, and $\mathbf{v}_0 = (a, b, c)$ in the second.

On the other hand, a line or place that does not contain the origin is not a subspace, since it does not contain $\mathbf{0}$.

We will revisit this example after defining the dot product on $\mathbb{R}^n$.

Polynomials

Recall that a **polynomial** is a function that can be written in the form $f(x) = a_n x^n + a_{n-1}x^{n-1} \cdots + a_1 x + a_0$, where $a_i \in \mathbb{R}$ are fixed constants and $a_n \neq 0$. We call n the **degree** of such a function, denoted $\deg f = n$.

Let P be the set of all polynomial functions, and let $P_n = \{f\colon f(x) = a_n x^n + a_{n-1}x^{n-1} \cdots + a_1 x + a_0, a_i \in \mathbb{R}\}$ be the set of all polynomials of degree at most n.
We have the set inclusions $P_n \subset P \subset C^\infty(X)$, where X is any nontrivial interval. (The second inclusion holds since any polynomial is infinitely differentiable on any interval.)

It is easy to see that in fact P_n is a subspace of P, and P is a subspace of $C^\infty(X)$. Indeed P_n and P both contain the zero polynomial $f(x) = 0 = 0x^n + 0x^{n-1} + \cdots 0x + 0$, which is the same thing as the zero function $0_X = \mathbf{0}$. Furthermore, sums and scalar multiples of polynomials (resp. of polynomials of at most degree n) are polynomials (resp. polynomials of at most degree n).

Important: a fact we will make use of all the time is that for two polynomials

$$
\begin{aligned}
f(x) &= a_n x^n + a_{n-1}x^{n-1} \cdots + a_1 x + a_0, \;\; a_n \neq 0\\
g(x) &= b_m x^m + b_{m-1}x^{m-1} \cdots + b_1 x + b_0, \;\; b_m \neq 0
\end{aligned}
$$

we have $f(x) = g(x)$ if and only if (1) n=m, and (2) $a_i = b_i$ for all $0 \leq i \leq n$.

Intersections and unions

Theorem 3.1

Let V be a vector space, and suppose $W_1, W_2, \ldots, W_r$ are each subspaces of V. Then the intersection $W = W_1 \cap W_2 \cdots \cap W_r$ is a subspace of V.

Comment. Thus intersections of subspaces are subspaces. The same is not true of unions.

For example, take $V = \mathbb{R}^2$, $W_1 = \{(t,t)\colon t \in \mathbb{R}\}$ and $W_2 = \{(t,-t)\colon t \in \mathbb{R}\}$. Then each W_i is a subspace, but their union $W_1 \cup W_2$ is not. Why?

We have $\mathbf{w}_1 = (1,1) \in W_1 \subset W_1 \cup W_2$ and $\mathbf{w}_2 = (1,-1) \in W_2 \subset W_1 \cup W_2$, but $\mathbf{w}_1 + \mathbf{w}_2 = (2,0) \notin W_1 \cup W_2$.

Note that $W_1 \cup W_2$ is in fact closed under scalar multiplication.

Linear combinations and span

Recall that a linear combination in a vector space V is a vector of the form

$$\mathbf{v} = k_1\mathbf{v}_1 + k_2\mathbf{v}_2 \cdots + k_r\mathbf{v}_r,$$

where $k_i \in \mathbb{R}$ are scalars.

We use this notion to define the span of a set of vectors.

Definition 3.2

Let V be a vector space, and let $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ be a set of vectors of V. The **span** of S is the set

$$\begin{aligned} \text{span}(\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}) \quad &:= \quad \begin{pmatrix} \text{the set of all linear} \\ \text{combinations of the } \mathbf{v}_i \end{pmatrix} \\ &= \quad \{\mathbf{v} \in V : \mathbf{v} = k_1\mathbf{v}_1 + k_2\mathbf{v}_2 \cdots + k_r\mathbf{v}_r, \text{ for some } k_i \in \mathbb{R}\}. \end{aligned}$$

Theorem 3.2

Let V be a vector space, $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ a set of vectors of V, and $W = \text{span}(S)$. Then

(i) W is a subspace of V;

(ii) if W' is a subspace containing all the vectors $\mathbf{v}_i$, then $W \subseteq W'$.

We paraphrase (ii) by saying $W = \text{span}(S)$ is the "smallest" subspace of V containing all the $\mathbf{v}_i$.

More terminology: in the spirit of the last theorem, given a set of vectors $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$, we call $W = \text{span}(S)$ the subspace of V **generated by** the vectors $\mathbf{v}_i$. Similarly, given a subspace W, a set $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ for which $W = \text{span}(S)$ is called a **spanning set** of W.

Examples

M_{mn}. Define E_{ij} to be the matrix whose (i,j)-th entry is 1, and whose every other entry is 0. Then the set

$$\{E_{ij} \colon 1 \leq i \leq m, 1 \leq j \leq n\}$$

is a spanning set for M_{mn}.

$\mathbb{R}^n$. In a similar vein, define $\mathbf{e}_i$ to be the n-tuple whose i-th entry is 1, and whose every other entry is 0.
Then $\{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n\}$ is a spanning set for $\mathbb{R}^n$.

P and P_n. The set $\{1, x, x^2, \dots,\}$ is a spanning set for P. The set $\{1, x, x^2, \dots, x^n\}$ is a spanning set for P_n.

$\mathbb{R}^\infty$. As above we can define $\mathbf{e}_i \in \mathbb{R}^\infty$ to be the infinite sequence whose i-th entry is 1, and whose every other entry is 0.
Note, however, that the set $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \dots\}$ is not a spanning set for $\mathbb{R}^\infty$.

Indeed, the sequence $(1, 1, 1, \dots)$ is not a (finite!) linear combination of the $\mathbf{e}_i$.

$\mathbb{R}_{>0}$ Any $a \neq 1 \in \mathbb{R}_{>0}$ forms a spanning set for $\mathbb{R}_{>0}$ as a vector space. This is because scalar multiplication by r in $\mathbb{R}_{>0}$ is defined as exponentiation. Thus $\text{span}(\{a\}) = \{a^r \colon r \in \mathbb{R}\} = \mathbb{R}_{>0}$. The last equality holds since the exponential function $f(x) = a^x$ has range all positive reals for any base $a \neq 1$.

Example

Let $V = P_2$ and let $S = \{p_1, p_2\}$, where $p_1(x) = x^2 - 1$ and $p_2(x) = x^2 - x$. Show that $W = \text{span}(S)$ is the subspace of all polynomials $p(x) = a_2x^2 + a_1x + a_0$ for which $p(1) = 0$. That is:

$$\text{span}(S) = \{p(x) \in P_2 \colon p(1) = 0\}$$

Proof.

We wish to prove a set equality. We do so by showing the $\subseteq$ and $\supseteq$ relations separately. (See my proof technique guide!)

$\subseteq$. Note first that $p_1(1) = p_2(1) = 0$. Given an element $q(x) \in \text{span}(\{p_1(x), p_2(x)\})$, we have $q(x) = ap_1(x) + bp_2(x)$ for some $a, b \in \mathbb{R}$. But then $q(1) = ap_1(1) + bp_2(1) = 0 + 0 = 0$. Thus $q(x) \in \{p(x) \colon p(1) = 0\}$.

$\supseteq$. Now take $p(x) = a_2x^2 + a_1x + a_0 \in \{p(x) \in P_2 \colon p(1) = 0\}$. We must find $a, b \in \mathbb{R}$ such that $p(x) = ap_1 + bp_2$.

Since $p(1) = 0$, we have $a_2 + a_1 + a_0 = 0$. I claim $p(x) = (-a_0)p_1 + (-a_1)p_2$. Indeed we have

$$-a_0p_1 - a_1p_2 = (-a_0 - a_1)x^2 + a_1x + a_0 = a_2x^2 + a_1x + a_0,$$

since $a_2 + a_1 + a_0 = 0$. This shows that $p(x) \in \text{span}(\{p_1, p_2\})$, as desired. $\square$

Example

Let $V = P_2$ and let $S = \{p_1, p_2, p_3\}$ where

$$p_1(x) = x^2 + x + 1, p_2(x) = x^2 + x, p_3(x) = x^2 + 1.$$

Show that $\text{span}(S) = P_2$.

Proof.

Again, we are tasked with showing a set equality.

It is clear that $\text{span}(S) = \{rp_1 + sp_2 + tp_3 \colon r, s, t \in \mathbb{R}\} \subseteq P_2$.

The harder direction is showing $P_2 \subseteq \text{span}(S)$: i.e., given *any* $p(x) = a_2x^2 + a_1x + a_0$ we must show there are $r, s, t \in \mathbb{R}$ such that $p(x) = rp_1 + sp_2 + tp_3$.

We do so by setting up a system of equations. Combining like terms and equating coefficients in the polynomial expression $p(x) = rp_1 + sp_2 + tp_3$ yields the linear system

$$\begin{aligned} r + s + t &= a_2 \\ r + s \phantom{{}+t} &= a_1 \\ r \phantom{{}+s} + t &= a_0 \end{aligned}$$

GE shows that the system has a solution for *any* choice of a_2, a_1, a_0: namely, $r = -a_2 + a_1 + a_0$, $s = a_2 - a_0$, $t = a_2 - a_1$. Thus given any $p(x) = a_2x^2 + a_1x + a_0$, we can find r, s, t such that $p = rp_1 + sp_2 + tp_3$, showing $P_2 \subseteq \text{span}(S)$. $\square$

Null space of a linear transformation

The notion of span is a useful tool for constructing subspaces inside a space V: given any collection $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$, we now know that the set $W = \text{span}(\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\})$ is guaranteed to be a subspace of V.

The notion of a null space of a linear transformation $T\colon V \to W$ provides another useful tool for constructing subspaces.

Definition 3.3

The **null space** of a linear transformation $T\colon V \to W$ is the set

$$\text{null}\, T\colon = \{\mathbf{v}\colon T(\mathbf{v}) = \mathbf{0}_W\}.$$

In the special case where $T\colon \mathbb{R}^n \to \mathbb{R}^m$ and $T = T_A$, we may write null A for null T_A: by definition this is the set

$$\text{null}\, A = \text{null}\, T_A = \{\mathbf{x} \in \mathbb{R}^n\colon A\mathbf{x} = \underset{m\times 1}{\mathbf{0}}\}.$$

In other words, null A is the set of solutions to the homogenous matrix equation $A\mathbf{x} = \mathbf{0}$, or equivalently, its associated homogenous system of equations.

As we see in the next theorem, given linear $T\colon V \to W$, its null space null T is always a subspace !!

Theorem 3.3 (Null space theorem)

Let $T\colon V \to W$. Then null T is a subspace of V.

Proof.

(i) Since $T(\mathbf{0}_V) = \mathbf{0}_W$, we see that $\mathbf{0}_V \in \operatorname{null} T$.

(ii) Suppose $\mathbf{v}_1, \mathbf{v}_2 \in \operatorname{null} T$. We have

$$\begin{aligned} T(\mathbf{v}_1 + \mathbf{v}_2) &= T(\mathbf{v}_1) + T(\mathbf{v}_2) && (T \text{ is linear}) \\ &= \mathbf{0}_W + \mathbf{0}_W && (\text{since } \mathbf{v}_1, \mathbf{v}_2 \in \operatorname{null} T) \\ &= \mathbf{0}_W. \end{aligned}$$

Thus $\mathbf{v}_1 + \mathbf{v}_2 \in \operatorname{null} T$, proving the implication
$\mathbf{v}_1, \mathbf{v}_2 \in \operatorname{null} T \Rightarrow \mathbf{v}_1 + \mathbf{v}_2 \in \operatorname{null} T$.

(iii) Suppose $\mathbf{v} \in \operatorname{null} T$. We have

$$\begin{aligned} T(c\mathbf{v}) &= cT(\mathbf{v}) && (T \text{ is linear}) \\ &= c\mathbf{0}_W && (\text{since } \mathbf{v} \in \operatorname{null} T) \\ &= \mathbf{0}_W. \end{aligned}$$

This shows $c\mathbf{v} \in \operatorname{null} T$, proving the implication $\mathbf{v} \in \operatorname{null} T \Rightarrow c\mathbf{v} \in \operatorname{null} T$.

Since null T satisfies the conditions (i)-(iii), we see that it is a subspace of V.

$\square$

Examples

The theorem gives us a clever, indirect way of proving a subset $V' \subseteq V$ is a subspace: namely, find a linear transformation $T\colon V \to W$ for which $V' = \operatorname{null} T$!!

Example 3.1

The set $W \subseteq \mathbb{R}^3$ of all vectors (x, y, z) satisfying $x + 2y + 3z = x - y - z = 0$ is a subspace of $\mathbb{R}^3$.

Indeed we have $W = \operatorname{null} A$ where $A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & -1 & -1 \end{bmatrix}$.

Example 3.2

The set $W = \{A \in M_{nn} \colon A^T = A\}$, consisting of all symmetric $n \times n$ matrices, is a subspace of M_{nn}.
Indeed, we have $W = \operatorname{null} T$, where $T\colon M_{nn} \to M_{nn}$ is the linear transformation defined as $T(A) = A^T - A$.
(I leave it to you to show T is linear.)

Example 3.3

The set W of all infinitely differentiable functions f satisfying the differential equation $f''(x) + xf'(x) = 3f(x)$ is a subspace of $C^\infty(\mathbb{R})$.
Indeed W is null T, where $T\colon C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R})$ is the linear transformation defined as $T(f) = f'' + xf' - 3f$.
(I leave it to you to show T is linear.)

Range

Definition 3.4

In general given a function $f\colon A \to B$ with domain A and codomain B, its **range** is the set

$$\operatorname{range} f = \{b \in B \colon b = f(a) \text{ for some } a \in A\} = f(A),$$

where the last equality makes use of our "image of a set" notation $f(A)$.

We will use the same notation for a linear transformation $T\colon V \to W$. The range of T is a subset of the codomain W. Not surprisingly, it is in fact a subspace of W.

Range

Theorem 3.4 (Range is a subspace)

Let $T\colon V \to W$ be a linear transformation. Then range T is a subspace of W.

Proof.

(i) We must show $\mathbf{0}_W \in \text{range}(T)$. But $\mathbf{0}_W = T(\mathbf{0}_V)$. Thus $\mathbf{0}_W \in \text{range}(T)$.

(ii) Suppose $\mathbf{w}_1, \mathbf{w}_2 \in \text{range}(T)$. This means there are $\mathbf{v}_1, \mathbf{v}_2 \in V$ such that $T(\mathbf{v}_i) = \mathbf{w}_i$ for $i = 1, 2$. We must show $\mathbf{w} = \mathbf{w}_1 + \mathbf{w}_2 \in \text{range}(T)$.

Set $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$. Then

$$
\begin{aligned}
T(\mathbf{v}) &= T(\mathbf{v}_1 + \mathbf{v}_2) \\
&= T(\mathbf{v}_1) + T(\mathbf{v}_2) \quad \text{(since } T \text{ is a linear transformation)} \\
&= \mathbf{w}_1 + \mathbf{w}_2 = \mathbf{w}.
\end{aligned}
$$

Since we have provided a $\mathbf{v}$ with $T(\mathbf{v}) = \mathbf{w}_1 + \mathbf{w}_2$, we see that $\mathbf{w}_1 + \mathbf{w}_2 \in \text{range}(T)$.

(iii) Suppose $\mathbf{w} \in \text{range}(T)$. Then there is a $\mathbf{v} \in V$ with $T(\mathbf{v}) = \mathbf{w}$. Then $T(k\mathbf{v}) = kT(\mathbf{v}) = k\mathbf{w}$, showing $k\mathbf{w} \in \text{range}(T)$.

$\square$

Example

Let $T = T_A\colon \mathbb{R}^2 \to \mathbb{R}^3$, where $A = \begin{bmatrix} 1 & 1 \\ 2 & 1 \\ 3 & 5 \end{bmatrix}$. According to the theorem, range T_A is a subspace of $\mathbb{R}^3$. Can we identify this subspace as a familiar geometric object?

By definition range T_A is the set

$$\{\mathbf{y} \in \mathbb{R}^3 \colon \mathbf{y} = T_A(\mathbf{x}) \text{ for some } \mathbf{x} \in \mathbb{R}^3\} = \left\{ \mathbf{y} = \begin{bmatrix} a \\ b \\ c \end{bmatrix} : \mathbf{y} = A\mathbf{x} \text{ for some } \mathbf{x} \in \mathbb{R}^2 \right\}.$$

Thus to compute range T_A we must determine which choice of $\mathbf{y} = (a, b, c)$ makes the system $A\mathbf{x} = \mathbf{y}$ consistent. We answer this using our good, old friend Gaussian elimination!

$$\left[\begin{array}{cc|c} 1 & 1 & a \\ 2 & 1 & b \\ 3 & 5 & c \end{array}\right] \xrightarrow{\text{row reduction}} \left[\begin{array}{cc|r} 1 & 1 & a \\ 0 & 1 & 2a - b \\ 0 & 0 & -7a + 2b + c \end{array}\right]$$

To be consistent we need $-7a + 2b + c = 0$. We conclude that range T is the set of all (a, b, c) satisfying $-7a + 2b + c = 0$. Geometrically this is the plane passing through O with normal vector $\mathbf{n} = (-7, 2, 1)$.

Example

Consider again the linear transformation $T\colon M_{nn} \to M_{nn}$, $T(A) = A^T - A$. We saw that null T was the space of symmetric matrices. The theorem above tells us that range T is also a subspace of M_{nn}. What is it?

Take $B \in \text{range } T$. By definition this means $B = T(A) = A^T - A$ for some A. So one, somewhat unsatisfying way of describing range T is as the set of all matrices of the form $A^T - A$.

Let's investigate further. Notice that if $B = A^T - A$, then $B^T = (A^T - A)^T = (A^T)^T - A^T = A - A^T = -B$. Thus every element $B \in \text{range } T$ satisfies $B^T = -B$. Such matrices are called **skew-symmetric**.

I claim further that in fact range T is the the set of all skew-symmetric matrices. To prove this, I need to show that given a skew-symmetric matrix B, there is a matrix A such that $T(A) = B$.

Suppose I have a B such that $B^T = -B$. Let $A = -\frac{1}{2}B$. Then

$$T(A) = T(-\frac{1}{2}B) = -\frac{1}{2}(B^T - B) = -\frac{1}{2}(-B - B) = B.$$

This shows that $B \in \text{range } T$, and concludes the proof that range T is the set of all skew-symmetric matrices.

3.4: executive summary

Definitions: linear independence, the Wronskian $W(f_1, f_2, \ldots, f_n)(x)$.

Procedures: how to determine whether a set of vectors is independent.

Theorems: if $f_1, f_2, \ldots, f_n$ are linearly dependent, then $W(f_1, f_2, \ldots, f_n)(x) = 0$ for all x.

3.4: linear independence

Definition 4.1

Let V be a vector space. A set $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ of elements of V is **linear independent** if

$$k_1\mathbf{v}_1 + k_2\mathbf{v}_2 + \cdots k_r\mathbf{v}_r = \mathbf{0} \Rightarrow k_i = 0 \text{ for all } i.$$

In other words, the only linear combination of the $\mathbf{v}_i$ yielding $\mathbf{0}$ is the **trivial linear combination** we get by setting $k_i = 0$ for all i.

The set S is **linearly dependent** if it is not linearly independent; i.e., if we can find a nontrivial linear combination of the $\mathbf{v}_i$ that yields $\mathbf{0}$.

Theorem 4.1

The set S is linearly independent if and only if no element $\mathbf{v}_i$ can be written as a linear combination of the other $\mathbf{v}_j$.

Similarly, S is linearly dependent if and only if one of the elements $\mathbf{v}_i$ can be written as a linear combination of the remaining $\mathbf{v}_j$.

Comment

Sometimes in the literature the statement in the theorem is taken to be the definition of linear dependence: i.e., that one vector can be written as a linear combination of the others. I prefer my definition, which leads to a straightforward procedure for determining linear independence.

Example in P_n

General procedure: all questions of linear dependence can be boiled down to deciding whether a certain linear system can be solved or not!

Let $S = \{x^2 + x - 2, 2x^2 + 1, x^2 - x\} \subset P_2$. Decide whether S is linearly independent.

Solution:

First observe that $\mathbf{0} = 0x^2 + 0x + 0$, the zero polynomial.
We ask whether there is a nontrivial combination

$$\begin{aligned} a(x^2 + x - 2) + b(2x^2 + 1) + c(x^2 - x) &= 0x^2 + 0x + 0 \\ (a + 2b + c)x^2 + (a - c)x + (-2a + b) &= 0x^2 + 0x + 0 \end{aligned}$$

Equating like terms gives us the linear system

$$\begin{aligned} a + 2b + c &= 0 \\ a \qquad\quad - c &= 0 \\ -2a + \ b \qquad &= 0 \end{aligned}$$

Row reduction shows this system only has the trivial solution $a = b = c = 0$.
Thus S is linearly independent. $\square$

Example in M_{mn}

General procedure: all questions of linear dependence can be boiled down to deciding whether a certain linear system can be solved or not!

Let $S = \left\{ A_1 = \begin{bmatrix} 3 & 1 \\ 2 & -3 \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 4 \\ 2 & 0 \end{bmatrix}, A_3 = \begin{bmatrix} -2 & -2 \\ -2 & 2 \end{bmatrix} \right\} \subset M_{22}$. Decide whether S is linearly independent.

Solution:

First observe that $\mathbf{0} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, the zero matrix.

We ask whether there is a nontrivial combination

$$\begin{aligned} a \begin{bmatrix} 3 & 1 \\ 2 & -3 \end{bmatrix} + b \begin{bmatrix} 0 & 4 \\ 2 & 0 \end{bmatrix} + c \begin{bmatrix} -2 & -2 \\ -2 & 2 \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 3a - 2c & a + 4b - 2c \\ 2a + 2b - 2c & -3a + 2c \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \end{aligned}$$

Equating like terms gives us the linear system

$$\begin{aligned} 3a \qquad\;\; - 2c &= 0 \\ a + 4b - 2c &= 0 \\ 2a + 2b - 2c &= 0 \\ -3a \qquad\;\; + 2c &= 0 \end{aligned}$$

Row reduction shows this system has a free variable, and hence a nontrivial solution–in fact infinitely many! One example is $a = 2$, $b = -1$, $c = 3$. Thus S is linearly dependent. □

Example in function space

General procedure: all questions of linear dependence can be boiled down to deciding whether a certain linear system can be solved or not!

Let $S = \{f(x) = x, g(x) = \cos(x), h(x) = \sin(x)\} \subseteq C^\infty(\mathbb{R})$.
Decide whether S is linearly independent.

Solution:

First observe that $\mathbf{0}$ is the zero function: the function that assigns 0 to all inputs x.
We ask whether there is a nontrivial combination $af + bg + ch = \mathbf{0}$.

Key observation: the equality above is an equality of functions. Thus this is true if and only if $af(x) + bg(x) + ch(x) = 0$ for all x.

To get a linear system, we evaluate the above at a few clever choices of x:

$$\begin{aligned} x = 0 \quad &: \quad a(0) + b\cos(0) + c\sin(0) = 0 \Rightarrow 0 + b + 0 = 0 \Rightarrow \boxed{b = 0} \\ x = \pi \quad &: \quad a(\pi) + c\sin(\pi) = 0 \Rightarrow \pi a + 0 = 0 \Rightarrow \boxed{a = 0} \end{aligned}$$

Having shown $a = b = 0$, we are left with the equation $c\sin(x) = 0$ for all x, which is true iff $\boxed{c = 0}$.

Thus the only linear combination yielding $\mathbf{0}$ is $a = b = c = 0$, the trivial one, showing S is linearly independent. $\square$

Linear independence in function spaces

As the last example illustrates, a set of functions $S = \{f_1, f_2, \ldots, f_r\}$ is linearly independent if
$k_1 f_1 + k_2 f_2 + \cdots k_r f_r = \mathbf{0}$ implies $k_i = 0$ for all i.

Recall $\mathbf{0}$ here stands for the zero function. Thus we must treat such a linear combination as a function identity! In other words to say

$$k_1 f_1 + k_2 f_2 + \cdots k_r f_r = \mathbf{0}$$

is simply to say that

$$k_1 f_1(x) + k_2 f_2(x) + \cdots k_r f_r(x) = 0$$

for all x in the given domain.

The beauty of this "for all x" is that by picking say r actual examples of x and evaluating above, we generate r linear equations in the unknowns k_i.

If this system has no nontrivial solutions, then we know the functions are independent.

However, if this system DOES have a nontrivial solution we CANNOT conclude the functions are linearly dependent. Why? We would have shown the identity above holds only for these r choices of x, but not necessarily all x!

$C^\infty(a, b)$ and the Wronskian

Let's consider this observation in the special example of differentiable functions.

Definition 4.2

Suppose $f_1, f_2, \ldots f_n$ are each $(n-1)$-differentiable functions on (a, b). We define the Wronskian of the f_i as the function

$$W(x) = \begin{vmatrix} f_1(x) & f_2(x) & \cdots & f_n(x) \\ f_1'(x) & f_2'(x) & \cdots & f_n'(x) \\ \vdots & \ldots & & \vdots \\ f_1^{(n-1)}(x) & f_2^{(n-1)}(x) & \cdots & f_n^{(n-1)}(x) \end{vmatrix}.$$

Theorem 4.2 (Wronskian)

Let $V = C^\infty(X)$, where X is a fixed interval (usually $X = \mathbb{R}$), and let $S = \{f_1, f_2, \ldots, f_n\}$ be a set of elements of V. Let $W(x)$ be the Wronskian of the f_i. Then

$$W \neq \mathbf{0} \Rightarrow \; S \text{ is linearly indendent.}$$

Comments

(1) Again $\mathbf{0}$ here is the zero function. So $W \neq \mathbf{0}$ means there is an x in (a, b) such that $W(x) \neq 0$.

(2) This implication only goes one way!! In other words, $W(x) = 0$ for all x does not imply S is dependent!!

3.5: executive summary

Definitions: basis.

Procedures: deciding whether a set is basis.

Theorems: B is a basis for V iff every vector in V can be written as a linear combination of the vectors in B in *a unique way*.

3.5: definition of basis

Definition 5.1

Let V be a vector a space. A set $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is called a (finite) **basis** for V if

(i) B spans V, and

(ii) B is linearly independent.

Comment

You should think of a basis B as a "minimal" set of vectors needed to generate the space V.

Condition (i) ensures all elements of V can be written as a linear combination of the $\mathbf{v}_i$. Thus B generates V.

Condition (ii) ensures we have no redundant elements in our set B. Thus B is minimal.

Some standard bases

1. Let $V = \mathbb{R}^n$, and let $\mathbf{e}_i$ be the the n-tuple whose i-th entry is 1, and whose every other entry is 0: e.g,

$$\mathbf{e}_1 = (1, 0, \ldots, 0), \mathbf{e}_2 = (0, 1, 0, \ldots, 0), \text{ etc.}$$

   Then the set $B = \{\mathbf{e}_1, \mathbf{e}_2, \ldots \mathbf{e}_n\}$ is a basis for $\mathbb{R}^n$, called the **standard basis** for $\mathbb{R}^n$.

2. Let $V = P_n$. Then the set $B = \{1, x, x^2, \ldots x^n\}$ is a basis for V, called the **standard basis** for P_n.
3. Let $V = M_{mn}$, and let E_{ij} be the $m \times n$ matrix whose ij-th entry is 1, and whose every other entry is 0. Then $B = \{E_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for V, called the **standard basis** for M_{mn}.

Some nonstandard bases

For each of the following choices of V and B, prove that B is a basis for V.

1. $V = \mathbb{R}^4$, $B = \{(1,1,1,1),(1,0,0,-1),(1,0,-1,0),(0,1,-1,0)\}$.
2. $V = P_2$, $B = \{1+x+x^2, -x+x^2, -1+x^2\}$.
3. $V = M_{22}$,

$$B = \left\{ \begin{bmatrix} 3 & 6 \\ 3 & -6 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -8 \\ -12 & -4 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} \right\}.$$

Nonexistence of a finite basis

A vector space need not have a finite basis.

For example, the space P_∞ of all polynomials does not have a finite basis.

Proof.

Suppose by contradiction that P_∞ did have a finite basis $B = \{p_1, p_2, \ldots, p_n\}$ for some polynomials $p_i(x)$.

Each polynomial p_i has a degree $m_i = \deg(p_i)$. Let m be the maximum of $m_1, m_2, \ldots, m_n$. Then $\mathrm{span}(S) \subset P_m$, the space of polynomials of degree at most m.

But then we have

$$\mathrm{span}(B) \subset P_m \subsetneq P_\infty.$$

Thus B doesn't span P_∞. A contradiction. $\square$

Since

$$P_\infty \subset C^\infty(a, b)$$

it follows that $C^\infty(a, b)$ also fails to have a finite basis.

Some funny spaces

1. Let $V = \{\mathbf{0}\}$. The only subsets of V are the empty set $S = \{\}$, and the set $S = \{\mathbf{0}\}$.

   The first set doesn't span V; the second set is not linearly independent. So technically the zero space has no basis!

   This turns out to be a significant inconvenience, so by executive order we declare the empty set $B = \{\}$ to be a basis of the zero space $V = \{\mathbf{0}\}$.

2. Let $V = \mathbb{R}_{>0}$. Recall that here vector addition is real number multiplication, and scalar multiplication is real number exponentiation.
   Let $r \neq 1$ be any element of $\mathbb{R}_{>0}$, not equal to 1. Claim: $B = \{r\}$ is a basis for $\mathbb{R}_{>0}$.

   Proof: homework exercise!

Theorem 5.1

A set $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis of V if and only if every vector $\mathbf{v} \in V$ can be written as a linear combination of $\mathbf{v}_i$ in a unique way: i.e., for every $\mathbf{v} \in V$ there is exactly one choice of scalars $c_1, c_2, \ldots c_n$ such that

$$\mathbf{v} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 \cdots + c_n\mathbf{v}_n.$$

Comment

The theorem allows us to prove a set B is a basis in one shot. No need to prove $\mathrm{span}(B) = V$ and linear independence in two separate steps.

Indeed, simply set up a linear combination of the given vectors equal to an arbitrary element of V, boil this vector equation down to a system of n linear equations in the n unknowns c_i, and use GE to determine the set of solutions.

3.6: executive summary

Definitions: dimension of a vector space.

Procedures: none, but many examples using "standard bases" for our familiar spaces.

Theorems: independent set can be extended to basis, spanning set can be contracted to basis; "street smarts" theorems; if $W \subset V$, then $\dim W \leq \dim V$, and $\dim W = \dim V$ iff $W = V$.

3.6: dimension

Theorem 6.1

Suppose $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis for the vector space V. Then every other basis S' for V contains exactly n elements.

In fact:

(a) if S' contains less than n elements, then it does not span V;

(b) if S' contains more than n elements, then it is linearly dependent.

Proof.

To be sketched in class. Boil everything down to a system of linear equations. $\square$

Thanks to the theorem, the following notion of dimension is well-defined.

Definition 6.1

Let V be a vector space.

If V does not have a finite basis, then we say V is **infinite dimensional** and write $\dim(V) = \infty$.

Otherwise we define the dimension of V to be the number n of vectors in a/any basis for V, and write $\dim(V) = n$.

Standard examples

To prove $\dim(V) = n$, we must EXHIBIT a basis of V containing n elements.

1. Since we have declared $S = \{\}$ to be a basis for $\{\mathbf{0}\}$, we have $\dim(\{\mathbf{0}\}) = 0$.
2. Since the standard basis $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ of $\mathbb{R}^n$ has n elements, we have $\dim(\mathbb{R}^n) = n$.
3. Since the standard basis $\{1, x, \dots, x^n\}$ of P_n has $n + 1$ elements, we have $\dim(P_n) = n + 1$.
4. Since the standard basis $\{E_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}$ of M_{mn} has mn elements, we have $\dim(M_{mn}) = mn$.

To prove $\dim(V) = \infty$, we must prove V has no finite basis.

We shown this already for
$P_\infty, C^\infty(-\infty, \infty), C^{(n)}(-\infty, \infty), C(-\infty, \infty), F(-\infty, \infty)$.
Thus for each of these spaces V we have $\dim(V) = \infty$.

Street smarts

For each pair V and S below, show super-super quickly that S is NOT a basis for V.

1. $V = M_{23}$.

$$S = \left\{ \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \right\}$$

Proof.

We have 5 vectors living in a 6-dimensional space. By Theorem 6.1, these vectors cannot span. □

2. $V = P_3$,

$$S = \{1 + \pi x - x^3, 1 + \sqrt{e}x^2 + x^3, 1 + x + x^2 + x^3, 1 - x^3, x + 17x^2 + x^3\}.$$

Proof.

We have 5 vectors living in a 4-dimensional space. By Theorem 6.1 they must be linearly dependent. □

Here are some more useful facts about bases, the proofs of which will be done in class and the exercises.

Theorem 6.2

Let V be finite dimensional.

1. If S spans V, then some subset of S is a basis of V. (Basically, throw out the redundant members!).
2. If S is linearly independent, then S can be extended to a basis of V. (Basically, add vectors to S one by one until it spans.)
3. Suppose $\dim V = n$, and let $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be any set of n vectors in V. Then
$$S \text{ spans } V \Leftrightarrow S \text{ is linearly independent.}$$
Thus if we know beforehand that $\dim V = n$, then to show a given set $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis it suffices to show either that is spans, or that it is linearly independent.

Dimension can be a useful tool for deciding whether a subspace W of V is in fact all of V.

Theorem 6.3

Suppose $\dim(V) = n$, and let $W \subset V$ be a subspace of V.

(a) $\dim(W) \leq \dim(V)$.

(b) $\dim(W) = \dim(V)$ if and only if $W = V$.

Proof of (a).

First we show W is finite-dimensional. Indeed, if not, we could find an infinite set S of linearly independent vectors, contradicting the fact that in an n-dimensional space there can be at most n linearly independent vectors.

Thus we have $\dim(W) = r$ for some finite r, which means we can find a basis $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ of W. Since these are linearly independent vectors in V, by the previous theorem we can extend S to a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_r, \mathbf{v}_{r+1}, \ldots, \mathbf{v}_n\}$ of V, showing $r \leq n$, and thus $\dim(W) \leq \dim(V)$. $\square$

Example

Describe all subspaces of $\mathbb{R}^3$.

Since $\dim(\mathbb{R}^3) = 3$, by the previous theorem a subspace $W \subset \mathbb{R}^3$ has dimension 0, 1, 2, or 3.

$\dim(W) = 0$. In this case $W = \{\mathbf{0}\}$ is the trivial subspace.

$\dim(W) = 1$. In this case $W = \text{span}\{\mathbf{v}\}$ of a single nonzero vector. We recognize this as a line in 3-space.

$\dim(W) = 2$. In this case $W = \text{span}\{\mathbf{v}, \mathbf{w}\}$ is the span of two linearly independent vectors. This means that they are not scalar multiples of one another, hence not colinear. It follows that W is a plane in 3-space.

$\dim(W) = 3$. Since $W \subset \mathbb{R}^3$ and $\dim(\mathbb{R}^3) = 3$, it follows from the previous theorem that $W = \mathbb{R}^3$.

We have shown that the only subspaces of $\mathbb{R}^3$ are lines, planes, the origin, and $\mathbb{R}^3$ itself.

Dimension theorem compendium

We collect here some of the most important results from this section.

Theorem 6.4

Dimension theorem compendium Let V be a vector space, and suppose $B = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ is a basis for V.

(a) (Street smarts) If S is a subset of V containing less than n elements, then S does not span V.

(b) (Street smarts) If S is a subset of V containing more than n elements, then S is linearly dependent.

(c) All bases of V contain exactly n elements.

(d) If S is linearly independent, then S can be extended to a basis of V.

(e) If S spans V, then some subset of S is a basis for V: i.e., S can be contracted to a basis.

(f) If $|S| = n$, then S is a basis if and only if S is linearly independent if and only if S spans V.

(g) (Dimension of subspaces I) Given subspace $W \subseteq V$, we have $\dim W \leq \dim V = n$.

(h) (Dimension of subspaces II) Given subspace $W \subseteq V$, we have

$$W = V \text{ if and only if } \dim W = \dim V.$$

Linear transformations and bases

As the next theorem articulates, a linear transformation $T\colon V \to W$ is uniquely determined by how it acts on the elements of a basis for V.

Theorem 1.1

Let $B = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis for V, and let W be any space.

(a) Given any choice of n elements $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n \in W$ there is a unique linear transformation $T\colon V \to W$ such that $T(\mathbf{v}_i) = \mathbf{w}_i$.

(b) Given linear transformations $T_1, T_2\colon V \to W$, $T_1 = T_2$ if and only if $T_1(\mathbf{v}_i) = T_2(\mathbf{v}_i)$ for $1 \leq i \leq n$.

This is an extremely useful theorem as it allows us, given a basis B of V, to

(i) easily define linear transformations simply by declaring where $\mathbf{v}_i$ gets sent for each i, and

(ii) easily check whether two linear transformations are equal simply by checking that they agree on the basis elements $\mathbf{v}_i$.

Proof of Theorem 1.1.

First observe that given any $\mathbf{v} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_n\mathbf{v}_n$, if T is a linear transformation satisfying $T(\mathbf{v}_i) = \mathbf{w}_i$ for all $\mathbf{v}_i \in B$, then we must have

$$\begin{aligned} T(\mathbf{v}) &= T(c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_n\mathbf{v}_n) \\ &= c_1 T(\mathbf{v}_1) + c_2 T(\mathbf{v}_2) + \cdots + c_n T(\mathbf{v}_n) \\ &= c_1\mathbf{w}_1 + c_2\mathbf{w}_2 + \cdots + c_n\mathbf{w}_n \end{aligned}$$

This shows that there is at most one such T, and furthermore that $T_1 = T_2$ if and only if $T_1(\mathbf{v}_i) = T_2(\mathbf{v}_i)$ for all $\mathbf{v}_i \in B$.
Thus we have proven (b), and the proof of (a) is completed by showing that the formula $T(\mathbf{v}) = c_1\mathbf{w}_1 + c_2\mathbf{w}_2 + \cdots + c_n\mathbf{w}_n$, where $\mathbf{v} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_n\mathbf{v}_n$, defines a linear transformation satisfying $T(\mathbf{v}_i) = \mathbf{w}_i$.
The latter property is obvious, since $\mathbf{v}_i = 1\mathbf{v}_i + \sum_{j\neq i} 0\mathbf{v}_j$ implies $T(\mathbf{v}_i) = 1\mathbf{w}_i + \sum_{i\neq j} 0\mathbf{w}_j = \mathbf{w}_i$.
Now let's show T is linear: given $\mathbf{v} = \sum_{i=1}^n c_i\mathbf{v}_i$ and $\mathbf{v}' = \sum_{i=1}^n c_i'\mathbf{v}_i$, we have $r\mathbf{v} + s\mathbf{v}' = \sum_{i=1}^n (rc_i + sc_i')\mathbf{v}_i$, in which case

$$\begin{aligned} T(r\mathbf{v} + s\mathbf{v}') &= \sum_{i=1}^n (rc_i + sc_i')\mathbf{w}_i && \text{(def. of } T) \\ &= r\sum_{i=1}^n c_i\mathbf{w}_i + s\sum_{i=1}^n c_i'\mathbf{w}_i = rT(\mathbf{v}) + sT(\mathbf{v}') \checkmark && \text{(def. of } T) \end{aligned}$$

$\square$

Transformations of $\mathbb{R}^n$

Corollary 1.1.1

Let $T\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Then $T = T_A$ for some $\underset{m\times n}{A}$.

In other words, any linear transformation whose domain is $\mathbb{R}^n$ for some n and whose codomain is $\mathbb{R}^m$ for some m, is in fact a matrix transformation $T = T_A$.

Proof.

Our proof includes a recipe for computing the matrix A such that $T = T_A$.
Namely, given a linear $T\colon \mathbb{R}^n \to \mathbb{R}^m$, let A be the matrix whose j-th column is $\mathbf{c}_j = T(\mathbf{e}_j)$, where $\mathbf{e}_j$ is the j-th element of the standard basis of $\mathbb{R}^n$.
I claim $T = T_A$.

According to the Theorem 1.1, I only need to show that T and T_A agree on a basis for $\mathbb{R}^n$. Let's take the standard basis $B = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$.
Then

$$\begin{aligned} T_A(\mathbf{e}_j) &= A\mathbf{e}_j && \text{(def. of } T_A\text{)} \\ &= \mathbf{c}_j && \text{(column expansion)} \\ &= T(\mathbf{e}_j) && \text{(def. of } A\text{)} \end{aligned}$$

We've shown that $T_A(\mathbf{e}_j) = T(\mathbf{e}_j)$ for all $\mathbf{e}_j \in B$. Theorem 1.1 implies $T = T_A$. $\square$

Linear transformations of $\mathbb{R}^n$

Once we know a given function $T\colon \mathbb{R}^n \to \mathbb{R}^m$ is linear, the recipe provided in the previous proof allows us to quickly compute the matrix $\underset{m\times n}{A}$ such that $T = T_A$: simply set the j-th column of A equal to $T(\mathbf{e}_j)$.

Example 1.1

Consider again rotation by θ, $T_\theta\colon \mathbb{R}^2 \to \mathbb{R}^2$, where θ is a fixed angle.
Once we know T_θ is linear (we do now, but this wasn't obvious), then we easily come up with the matrix A_θ that defines T_θ.
The first column of A_θ is

$$T_\theta(\mathbf{e}_1) = T_\theta(\cos(0), \sin(0)) = (\cos(\theta), \sin(\theta)).$$

The second column of A_θ is

$$T_\theta(\mathbf{e}_2) = T_\theta(\cos(\pi/2), \sin(\pi/2)) = (\cos(\pi/2+\theta), \sin(\pi/2+\theta)) = (-\sin(\theta), \cos(\theta)).$$

Thus $A_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.

Introduction

We have seen already how bases can be used to help computationally understand vector spaces and their subspaces; we will now see how they can be used to analyze and understand linear transformations.

Given a linear transformation $T\colon V \to W$, one thing we want to understand are the associated subspaces $\operatorname{null} T \subseteq V$ and $\operatorname{range} T \subseteq W$. The rank-nullity theorem, sometimes called the fundamental theorem of linear algebra, relates the dimension of these two spaces with the dimension of V.

Theorem 2.1 (Rank-nullity theorem)

Let V be a vector space with $\dim V = n < \infty$. Let $T \colon V \to W$ be a linear transformation. (We make no assumption about the dimension of W.) Then:

$$\dim \operatorname{null} T + \dim \operatorname{range} T = n.$$

Comment

We define the **nullity** of T as nullity $T = \dim \operatorname{null} T$, and the **rank** of T as rank $T = \dim \operatorname{range} T$. The rank-nullity theorem thus asserts that nullity T + rank $T = \dim V$.

Proof of rank-nullity theorem.

Let $B_1 = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ be a basis for null T. (It is possible to find such a finite basis since $W \subseteq V$ and $\dim V = n$.)

Extend B_1 to a basis $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r, \mathbf{v}_{r+1}, \mathbf{v}_{r+2}, \ldots, \mathbf{v}_n\}$ of V. (This is possible by the dimension theorem compendium. Note that in total B will have n elements.)

Claim: $B_2 = \{T(\mathbf{v}_{r+1}), T(\mathbf{v}_{r+2}), \ldots, T(\mathbf{v}_n)\}$ is a basis for range $T \subseteq W$.

I will prove the claim on the next slide. Assuming the claim is true, we are done since then

$$n = r + (n-r) = \#B_1 + \#B_2 = \dim \operatorname{null} T + \dim \operatorname{range} T.$$

$\square$

Proof of claim.

We let $B_2 = \{T(\mathbf{v}_{r+1}), T(\mathbf{v}_{r+2}), \ldots, T(\mathbf{v}_n)\}$, with notation as in the previous slide.

B_2 is linearly independent.

If $c_{r+1}T(\mathbf{v}_{r+1}) + c_{r+2}T(\mathbf{v}_{r+2}) + \cdots + c_n T(\mathbf{v}_n) = \mathbf{0}_W$, then $T(c_r\mathbf{v}_r + c_{r+1}\mathbf{v}_{r+2} + \cdots + c_n\mathbf{v}_n) = \mathbf{0}_W$, since T is linear.

Then $\mathbf{v} = c_r\mathbf{v}_r + c_{r+1}\mathbf{v}_{r+2} + \cdots + c_n\mathbf{v}_n \in \text{null}\, T$.

Then we can write $\mathbf{v} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_r\mathbf{v}_r$, since B_1 is a basis for null T.

Then $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_r\mathbf{v}_r = \mathbf{v} = c_r\mathbf{v}_r + c_{r+1}\mathbf{v}_{r+2} + \cdots + c_n\mathbf{v}_n$, and hence $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_r\mathbf{v}_r - c_{r+1}\mathbf{v}_{r+1} - \cdots - c_n\mathbf{v}_n = \mathbf{0}$

Then $c_1 = c_2 = \cdots = c_{r+1} = c_{r+2} = \cdots = c_n = 0$, since B is a basis. This implies the original linear combination of the $T(\mathbf{v}_i)$ was trivial, and thus that B_2 is independent.

B_2 spans range T. Take $\mathbf{w} \in \text{range}\, T$. Then $w = \mathbf{v}$ for some $\mathbf{v} \in V$.

Write $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_r\mathbf{v}_r + c_{r+1}\mathbf{v}_{r+1} + \cdots + c_n\mathbf{v}_n$. (Possible since B is a basis.) Then $\mathbf{w} = T(\mathbf{v}) = T(\sum_{i=1}^n c_i\mathbf{v}_i) = \sum_{i=1}^n c_i T(\mathbf{v}_i)$, since T is linear.

But we have $\sum_{i=1}^n c_i T(\mathbf{v}_i) = 0 + 0 + \cdots + 0 + \sum_{i=r+1}^n c_i T(\mathbf{v}_i)$, since $\mathbf{v}_i \in \text{null}\, T$ for $1 \le i \le r$.

Thus $\mathbf{w} = c_{r+1}T(\mathbf{v}_{r+1}) + c_{r+2}T(\mathbf{v}_{r+2}) + \cdots c_n T(\mathbf{v}_n)$, showing that $\mathbf{w} \in \text{span}\, B_2$, and thus that range $T \subseteq \text{span}\, B_2$. Since clearly span $B_2 \subseteq \text{range}\, T$, we have span $B_2 = \text{range}\, T_2$, as desired. $\square$

Example 2.1

Let $T = T_A$ where

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

A little Gaussian elimination shows that
$\operatorname{null} A = \{(s - 2t, -3(s - t), s, t) \colon s, t \in \mathbb{R}\}$.

Notice that the general form of an element of $\operatorname{null} A$ can be expressed as

$$(s - 2t, -3(s - t), s, t) = s(1, -3, 1, 0) + t(-2, 3, 0, 1).$$

From this it follows that $B = \{(1, -3, 1, 0), (-2, 3, 0, 1)\}$ is a basis for $\operatorname{null} A$, and thus that $\dim \operatorname{null} A = 2$.

The rank-nullity theorem now implies that
$\dim \operatorname{range} T = \dim \mathbb{R}^4 - \dim \operatorname{null} A = 4 - 2 = 2$. Since $\operatorname{range} T \subseteq \mathbb{R}^2$ and $\dim \operatorname{range} T = 2$, we conclude from the dimension theorem compendium that $\operatorname{range} T = \mathbb{R}^2$.

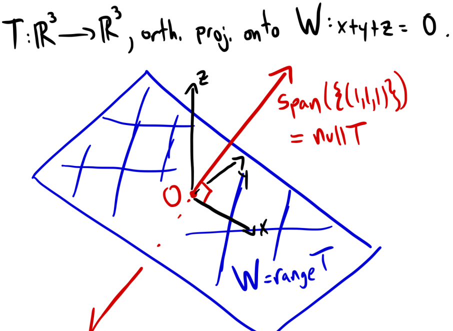
Thanks to the rank-nullity theorem, our quick computation of $\operatorname{null} A$ allowed us to determine $\operatorname{range} T$ with minimal additional effort!

Example 2.2

Let $T: \mathbb{R}^3 \to \mathbb{R}^3$ be orthogonal projection onto the plane $W: x+y+z=0$, as defined earlier.

It is clear that range $T = W$. Indeed T maps all vectors to vectors in W, by definition, so range $T \subseteq W$. Furthermore, given any $\mathbf{w} \in W$, we have $\mathbf{w} = T(\mathbf{w})$, since orthogonal projection does nothing to a vector that already lies in W. This proves range $T = W$. It follows that rank $T = \dim W = 2$.

The rank-nullity theorem then implies $\dim \operatorname{null} T = 3 - 2 = 1$. So null T is a line (dimension-1 subspace) passing through the origin. Which one? Geometrically this is easy to see: it is span($\{(1,1,1)\}$), the line passing through the origin and orthogonal to W.



Example 2.3

Define $T\colon M_{nn} \to M_{nn}$ as $T(A) = A^T - A$.

As we have seen elsewhere, null $T = \{A \in M_{nn} \colon A^T = A\}$ and range $T = \{A \in M_{nn} \colon A^T = -A\}$, the space of symmetric and skew-symmetric matrices, respectively.

As we have also seen, the dimension of the space of symmetric matrices is $\frac{n(n+1)}{2}$, and the dimension of skew-symmetric matrices is $\frac{n(n-1)}{2}$.

According to the rank-nullity theorem we must have

$$\begin{aligned} n^2 &= M_{nn} \\ &= \dim \operatorname{null} T + \dim \operatorname{range} T \\ &= \frac{n(n+1)}{2} + \frac{n(n-1)}{2}. \end{aligned}$$

We have thus given a linear algebraic proof of the identity $n^2 = \frac{n(n+1)}{2} + \frac{n(n-1)}{2}$.

Yes, there is a more straightforward arithmetic proof, but you must admit this one is pretty cool, and it illustrates how results in one area of mathematics (e.g., linear algebra) can sometimes be translated into results in a completely different area (e.g., combinatorics).

Relative sizes of null T and range T

Let $T: V \to W$, where $\dim V = n$. Since $\dim \operatorname{null} T + \dim \operatorname{range} T = n$, we see that the bigger the null space (dimension-wise), the smaller the range, and vice versa.

Let's see this numerically in action. Assume $T: V \to W$ is linear.

1. Suppose $\dim V = 5$ and $\dim W = 3$. Prove: null T is nontrivial.

   If $\operatorname{null} T = \{\mathbf{0}\}$, then $\dim \operatorname{range} T = 5 - 0 = 5$; but this is impossible since $\operatorname{range} T \subseteq W$ and $\dim W = 3$. Thus $\operatorname{null} T \neq \{\mathbf{0}\}$; i.e., there is a nonzero $\mathbf{v} \in \operatorname{null} T$. This shows null T is nontrivial.

2. Suppose $\dim V = 7$, $\dim W = 5$, and $\dim \operatorname{null} T = 2$. Prove: $\operatorname{range} T = W$.

   We have $\dim \operatorname{range} T = 7 - \dim \operatorname{null} T = 7 - 2 = 5$. Since $\operatorname{range} T \subseteq W$ and $\dim \operatorname{range} T = \dim W$, we conclude $\operatorname{range} T = W$.

Fundamental subspaces of a matrix

When $T = T_A$ for some $m \times n$ matrix A, we can develop a systematic way of computing bases for null A and range A. Not surprisingly this procedure involves Gaussian elimination, as we will outline below.

In fact the procedure allows us to compute bases for the three following subspaces associated to a matrix, the so-called fundamental subspaces of A.

Definition 2.1

Let A be a an $m \times n$ matrix with rows $\mathbf{r}_1, \dots, \mathbf{r}_m$ and columns $\mathbf{c}_1, \dots \mathbf{c}_n$. The following subspaces are called the **fundamental subspaces of** A.

1. The **null space** of A is defined as
$$\operatorname{null} A = \{\mathbf{x} \in \mathbb{R}^n \colon A\mathbf{x} = \mathbf{0}\} \subset \mathbb{R}^n.$$
2. The **row space** of A is defined as
$$\operatorname{row} A = \operatorname{span}(\{\mathbf{r}_1, \dots, \mathbf{r}_m\}) \subset \mathbb{R}^n.$$
3. The **column space** of A is defined as
$$\operatorname{col} A = \operatorname{span}(\{\mathbf{c}_1, \dots \mathbf{c}_n\}) \subset \mathbb{R}^m.$$

The careful reader will object that range A does not appear on this list! Fear not, as we show in the next slide $\operatorname{col} A = \operatorname{range} A$.

col A = range A

Take an $m \times n$ matrix and consider A as a collection of n columns $\mathbf{c}_j$, each of which lives in $\mathbb{R}^m$:

$$A = \begin{bmatrix} | & | & \cdots & | \\ \mathbf{c}_1 & \mathbf{c}_2 & \cdots & \mathbf{c}_n \\ | & | & \cdots & | \end{bmatrix}$$

Then we have

$$\begin{aligned}
\mathbf{b} \in \text{col}\, A \quad & \Leftrightarrow \quad \mathbf{b} \in \text{span}(\{\mathbf{c}_1, \ldots, \mathbf{c}_n\}) \\
& \Leftrightarrow \quad \mathbf{b} = a_1\mathbf{c}_1 + a_2\mathbf{c}_2 + \cdots + a_n\mathbf{c}_n \text{ for some } a_i \\
& \Leftrightarrow \quad \mathbf{b} = A \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \quad \text{(by column expansion!!)} \\
& \Leftrightarrow \quad \text{there is an } \mathbf{x} \in \mathbb{R}^n \text{ such that } A\mathbf{x} = \mathbf{b} \\
& \Leftrightarrow \quad \mathbf{b} \in \text{range}\, A.
\end{aligned}$$

We conclude:

$$\boxed{\text{col}\, A = \text{range}\, A}$$

Computing the fundamental spaces

Once again Gaussian elimination is the main tool for computing fundamental spaces: start with A, row reduce to U, compute the fundamental spaces of U. However, there are some subtleties involved. Here is the overall description for how to proceed:

Space	Relation	How to pick a basis
Null space	$\operatorname{null} A = \operatorname{null} U$	$\left(\begin{array}{c}\text{find vector parametrization} \\ \text{of solutions to } U\mathbf{x} = \mathbf{0}\end{array}\right)$
Row space	$\operatorname{row} A = \operatorname{row} U$	$\left(\begin{array}{c}\text{nonzero rows of } U \\ \text{form a basis of row}(A)\end{array}\right)$
Column space	$\operatorname{col} A \neq \operatorname{col} U$	$\left(\begin{array}{c}\text{pick columns of } A \text{ corresponding} \\ \text{to columns of } U \text{ with leading 1's}\end{array}\right)$

Let's prove some of the previous claims. We will begin by proving the following more general result.

Claim. If A and B are row equivalent, then $\text{null}(A) = \text{null}(B)$, $\text{row}(A) = \text{row}(B)$, and if a certain subset of the columns of B form a basis of $\text{col}(B)$, then the same is true of the corresponding columns of A and $\text{col}(A)$.

Proof.

First observe that A is row equivalent to B iff $(E_r E_{r-1} \cdots E_1)A = B$ for some elementary matrices E_i iff $QA = B$ for some invertible Q. (The latter "iff" follows since the E_i are elementary, and since all invertible matrices are products of elementary matrices.) So we assume $QA = B$ for some invertible Q.

Null space. We have shown in an exercise that $A\mathbf{x} = \mathbf{0}$ iff $QA\mathbf{x} = \mathbf{0}$ iff $B\mathbf{x} = \mathbf{0}$. It follows that $\text{null}(A) = \text{null}(B)$.

Row space To show $\text{row}(A) = \text{row}(B)$, it is enough to show that $\text{row}(B) \subseteq \text{row}(A)$; this is because we can then apply the same reasoning using the fact that $A = Q^{-1}B$, Q^{-1} invertible. The row method tells us that each row of $B = QA$ is a linear combination of the rows of A. Thus each row of B lies in $\text{row}(A)$, the span of the rows of A. But then we must have $\text{row}(B) \subseteq \text{row}(A)$, since $\text{row}(B)$ is the "smallest" subspace containing all rows of B (by properties of span).

Column space (Sketch). Here one can show that columns $\mathbf{c}_{i_1}, \mathbf{c}_{i_2}, \ldots, \mathbf{c}_{i_r}$ of A form a basis of $\text{col}(A)$ iff $Q\mathbf{c}_{i_1}, Q\mathbf{c}_{i_2}, \ldots, Q\mathbf{c}_{i_r}$ form a basis of $\text{col}(B)$. By the column method the vectors $Q\mathbf{c}_{i_j}$ are precisely the corresponding columns of $B = QA$. $\square$

Example

Let's compute bases/dimensions for the fundamental spaces of

$$A = \begin{bmatrix} 2 & 2 & 4 & 2 \\ 6 & 6 & 11 & 5 \\ -4 & -4 & -7 & -3 \end{bmatrix}.$$

A reduces to the matrix $U = \begin{bmatrix} 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

First compute

$$\operatorname{null}(U) = \{(s-r, r, -s, s) \colon r, s \in \mathbb{R}\} = \{s(1,0,-1,1)+r(-1,1,0,0) \colon r, s \in \mathbb{R}\}.$$

It follows that $\operatorname{null} A = \operatorname{null} U = \operatorname{span}\{(1,0,-1,1),(-1,1,0,0)\}$, and thus that $B = \{(-1,1,0,0),(1,0,-1,1)\}$ is a basis for $\operatorname{null}(A)$. We conclude $\dim \operatorname{null} A = 2$.

Next, the rank-nullity theorem implies $\dim \operatorname{range} U = \dim \mathbb{R}^4 - \dim \operatorname{null} U = 2$. Thus to choose a basis for $\operatorname{col} U = \operatorname{range} U$ we need only pick two linearly independent columns of U: the first and third columns will do. It follows that the first and third columns of A form a basis for $\operatorname{col} A$. This gives us $B'' = \{(2,6,-4),(4,11,-7)\}$ as a basis for $\operatorname{col} A$.

Finally, we have $\operatorname{row} A = \operatorname{row} U$, and clearly we can take the nonzero rows of U as a basis for this. Thus $B' = \{(1,1,2,1),(0,0,1,1)\}$ is a basis for $\operatorname{row} A$. We conclude $\dim \operatorname{row} A = 2$.

The preceding example nicely illustrates our general procedure for computing bases for the fundamental spaces of A.

Computing bases for the fundamental spaces

(i) Reduce A to row echelon form matrix U.

(ii) $\boxed{\text{null}(A) = \text{null}(U)}$. Use free/leading variable method to give full description of solutions $U\mathbf{x} = \mathbf{0}$. Extract a basis from the resulting parametric description.

(iii) $\boxed{\text{row}(A) = \text{row}(U)}$. A basis for $\text{row}(U)$ (and hence $\text{row}(A)$) consists of the nonzero rows of U.

(iv) $\boxed{\text{col}(A) \neq \text{col}(U)}$. The columns of U with leading 1's are a basis for $\text{col}(U)$. The *corresponding columns* of A form a basis for $\text{col}(A)$.

Comment

It is clear that the nonzero rows of U form a basis of row U: the staircase pattern of leading 1's guarantees they are linearly independent, and we can obviously discard the zero rows.

It is not difficult to show that the columns of U with leading 1's are linearly independent. (Exercise!) That they are in fact a basis follows from the fact that $\#(\text{leading 1's}) = n - \#(\text{free variables}) = n - \dim \text{null}\, U = \dim \text{col}\, U$.

Rank-nullity theorem for matrices

The previous discussion gives us a much more detailed analysis of the spaces involved in the rank-nullity theorem in the special case where $T = T_A$. We collect some of those details here.

Rank-nullity theorem for matrices

Let A be $m \times n$. Suppose A is row equivalent to the row echelon matrix U.

1. $\operatorname{col} A = \operatorname{range} A$
2. $\dim \operatorname{null} A = \#(\text{free variables in the system } U\mathbf{x} = \mathbf{0})$
3. $\operatorname{rank} A = \dim \operatorname{col} A = \dim \operatorname{row} A = \#(\text{leading 1's in } U)$
4. $\operatorname{rank} A \leq \min\{m, n\}$. (Since $\#(\text{leading 1's in } U) \leq m$ and $\#(\text{leading 1's in } U) \leq n$.)
5. $n = \dim \operatorname{null} A + \dim \operatorname{col} A = \dim \operatorname{null} A + \dim \operatorname{row} A$.

Extending/contracting sets to bases

Recall that if $\dim V = n$, then any linearly independent set can be extended to a basis of B, and any spanning set can be contracted to a basis.
In the special case when $V = \mathbb{R}^n$, our fundamental space algorithms provide a means of performing these extensions/contractions.

Let $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r \in \mathbb{R}^n$.

1. Extending to basis. If the $\mathbf{v}_i$ are independent, then to extend to a basis of $\mathbb{R}^n$ proceed as follows:
   1.1 Build the matrix A whose columns (in order) are $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r, \mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n$.
   1.2 Apply the column space algorithm to A.
2. Contracting to basis. If the $\mathbf{v}_i$ span the subspace $W \subseteq \mathbb{R}^n$, then to contract to a basis of W proceed as follows:
   2.1 Build the matrix A whose columns are $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r$.
   2.2 Apply the column space algorithm to A.

Example

Let $W = \text{span}\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\}$ where

$$\begin{array}{ll} \mathbf{v}_1 = (1, -1, 5, 2) & \mathbf{v}_2 = (-2, 3, 1, 0) \\ \mathbf{v}_3 = (4, -5, 9, 4) & \mathbf{v}_4 = (0, 4, 2, -3) \\ \mathbf{v}_5 = (-7, 18, 2, -8) & \end{array}$$

Find a subset of the $\mathbf{v}_i$ that yields a basis of W.

We know the $\mathbf{v}_i$ span W, so to get a basis we need to "throw out the redundant ones". To figure out which ones need to go, we create a matrix A by setting the $\mathbf{v}_i$ as its columns (not its rows)! The procedure for finding a basis for $\text{col}(A)$ then gives us a subset of these columns that forms a basis.

$$A = \begin{bmatrix} 1 & -2 & 4 & 0 & -7 \\ -1 & 3 & -5 & 4 & 18 \\ 5 & 1 & 9 & 2 & 2 \\ 2 & 0 & 4 & -3 & -8 \end{bmatrix} \xrightarrow{\text{row red.}} U = \begin{bmatrix} \boxed{1} & 0 & 2 & 0 & -1 \\ 0 & \boxed{1} & -1 & 0 & 3 \\ 0 & 0 & 0 & \boxed{1} & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

It follows that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_4\}$ is a basis for W.

Example

Extend the set $S = \{(1,1,1,1), (-2,-2,3,3)\}$ to a basis of $\mathbb{R}^4$.

Take the matrix

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

This matrix row reduces to

$$U = \begin{bmatrix} \boxed{1} & -2 & 1 & 0 & 0 & 0 \\ 0 & \boxed{1} & -1/5 & 0 & 1/5 & 0 \\ 0 & 0 & \boxed{1} & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} & -1 \end{bmatrix}$$

It follows that the first, second, third and fifth column of A form a basis of $\mathrm{col}(A) = \mathbb{R}^4$. Thus

$$B = \{(1,1,1,1), (-2,-2,3,3), (1,0,0,0), (0,0,1,0)\}$$

is a basis of $\mathbb{R}^4$ extending S.

Invertibility Theorem

Suppose A is a square $n \times n$ matrix . Recall that A is invertible if and only if $A\mathbf{x} = \mathbf{0}$ has a unique solution. This is equivalent to $\text{null}(A) = \{\mathbf{0}\}$. Thus we have:

$$A \text{ invertible } \Leftrightarrow \text{null}(A) = \{\mathbf{0}\} \Leftrightarrow \text{nullity}(A) = 0.$$

Similarly, we have A invertible if and only if $A\mathbf{x} = \mathbf{b}$ has a solution for all $\mathbf{b} \in \mathbb{R}^n$. As we saw earlier, $\text{col}(A) = \{\mathbf{b} \in \mathbb{R}^n \colon A\mathbf{x} = \mathbf{b} \text{ has a solution}\}$. Thus we see that

$$A \text{ invertible} \Leftrightarrow \text{col}(A) = \mathbb{R}^n \Leftrightarrow \text{rank}(A) = n \Leftrightarrow \text{row}(A) = \mathbb{R}^n,$$

where the last equivalence follows since $\text{row}(A) \subset \mathbb{R}^n$ and $\dim(\text{row}(A)) = n$.

Looks like we have quite a few new statements to add to our Invertibility Theorem!

Theorem 2.2 (Invertibility theorem)

Let A be $n \times n$. The following statements are equivalent.

(a) A is invertible.

(b) $A\mathbf{x} = \mathbf{0}$ has a unique solution (the trivial one).

(c) A is row equivalent to I_n, the $n \times n$ identity matrix.

(d) A is a product of elementary matrices.

(e) $A\mathbf{x} = \mathbf{b}$ has a solution for every $n \times 1$ column vector $\mathbf{b}$.

(f) $A\mathbf{x} = \mathbf{b}$ has a *unique* solution for every $n \times 1$ column vector $\mathbf{b}$.

(g) $\det A \neq 0$.

(h) $\operatorname{null} A = \{\mathbf{0}\}$.

(i) $\operatorname{nullity} A = 0$.

(j) $\operatorname{rank} A = n$.

(k) $\operatorname{col} A = \mathbb{R}^n$.

(l) $\operatorname{row} A = \mathbb{R}^n$.

(m) The columns of A are linearly independent (or span $\mathbb{R}^n$, or are a basis of $\mathbb{R}^n$).

(n) The rows of A are linearly independent (or span $\mathbb{R}^n$, or are a basis of $\mathbb{R}^n$).

Coordinate vectors relative to a basis B

Definition 3.1

Let $B = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis for V, and let $\mathbf{v} \in V$. According to Theorem 5.1 there is a unique choice of c_i such that

$$\mathbf{v} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 \cdots + c_n\mathbf{v}_n.$$

We define the **coordinate vector of v relative to the basis** B to be the n-tuple

$$[\mathbf{v}]_B := (c_1, c_2, \dots, c_n)$$

Comments

1. To compute the coordinate vector of $\mathbf{v}$ relative to $B = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ we must solve the vector equation $\mathbf{v} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_n\mathbf{v}_n$ for the coefficients $c_1, c_2, \dots, c_n$.

   For any given example this computation can usually be reduced to setting up and solving a certain system of linear equations.

2. As usual, we will be flexible in terms of how we treat the n-vector $(c_1, c_2, \dots, c_n)$. For example, we will often interpret this as a $n \times 1$ column vector.

Example

Let $V = P_2$.

1. Let $B = \{1, x, x^2\}$ be the standard basis of V. Computing $[p(x)]_B$ in this case is easy since any polynomial $p(x) = a + bx + cx^2$ is already expressed as a linear combination of the elements of B !!
   That is, we have $[a + bx + cx^2]_B = (a, b, c)$ for any polynomial $p(x) = a + bx + cx^2$.
   Some explicit examples:
   $$[7 - \pi x + \sqrt{2}x^2]_B = (7, -\pi, \sqrt{2})$$
   $$[1 + 9x^2]_B = (1, 0, 9)$$

2. Let $B' = \{1 + x + x^2, -x + x^2, -1 + x^2\} = \{p_1, p_2, p_3\}$ be the nonstandard basis we considered earlier. Now it requires more work to compute $[p(x)]_{B'}$. Some explicit examples:
   $$\begin{aligned} 1 + x + x^2 &= 1p_1 + 0p_2 + 0p_3 &\Rightarrow\quad& [1 + x + x^2]_{B'} = (1, 0, 0) \\ -x + x^2 &= 0p_1 + 1p_2 + 0p_3 &\Rightarrow\quad& [-x + x^2]_{B'} = (0, 1, 0) \\ x^2 &= \frac{1}{3}p_1 + \frac{1}{3}p_2 + \frac{1}{3}p_3 &\Rightarrow\quad& [x^2]_{B'} = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3}) \end{aligned}$$

The last example was computed by setting up the polynomial equation $x^2 = c_1(1 + x + x^2) + c_2(-x + x^2) + c_3(-1 + x^2)$ and solving for the c_i. Verify for yourself that $c_1 = c_2 = c_3 = 1/3$ is the solution!

Coordinate vector map

Theorem 3.1

Let V be a vector space, and suppose $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ be a basis for V. Define

$$\begin{aligned} T\colon V &\to \mathbb{R}^n \\ \mathbf{v} &\mapsto [\mathbf{v}]_B. \end{aligned}$$

1. T is a linear transformation. We will call T the **coordinate vector map with respect to** B.
2. $T(\mathbf{v}_1) = T(\mathbf{v}_2)$ if and only if $\mathbf{v}_1 = \mathbf{v}_2$: i.e., T is one-to-one.
   In particular, $T(\mathbf{v}) = \mathbf{0}$ if and only if $\mathbf{v} = \mathbf{0}_V$.
3. range $T = \mathbb{R}^n$: i.e. T is onto.
4. A set $S = \{w_1, w_2, \ldots, w_r\} \subseteq V$ is linear independent if and only if $T(S) = \{T(\mathbf{w}_1), T(\mathbf{w}_2), \ldots, T(\mathbf{w}_r)\} \subseteq \mathbb{R}^n$ is linearly independent.
5. A set $S = \{w_1, w_2, \ldots, w_r\} \subseteq V$ spans V if and only if $T(S) = \{T(\mathbf{w}_1), T(\mathbf{w}_2), \ldots, T(\mathbf{w}_r)\}$ spans $\mathbb{R}^n$.

Proof.

Exercise. $\square$

Fix vector space V and basis $B = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$. According to Theorem 3.1, the coordinate vector map $\mathbf{v} \mapsto [\mathbf{v}]_B$ is not only linear, it is also 1-1 and onto. Such functions are called isomorphisms.

Definition 3.2

Let V and W be vector spaces. An **isomorphism** is a linear transformation $T\colon V \to W$ that is 1-1 and onto.
The spaces V and W are called **isomorphic** in this case.

Comment

'Isomorphism' is derived from the Greek terms 'isos', meaning "equal", and 'morphe', meaning "form".

We do not have time in the course to study isomorphisms in detail. Instead we content ourselves with the following general principle: when V and W are isomorphic, as witnessed by an isomorphism $T\colon V \to W$, the spaces are identical as far as vector space structure is concerned, even though as sets they may look completely different.

Furthermore, since T is 1-1 and onto, it has an inverse function $T^{-1}\colon W \to V$. Furthermore, you can show that T^{-1} is also a linear transformation. The two functions T and T^{-1} allow us to to go back and forth between V and W, translating statements about V into corresponding statements about W with no information loss.

We apply the general principle described in the previous slide to the special case of a coordinate vector isomorphism $[\ \ ]_B\colon V \to \mathbb{R}^n$.

Coordinate vector technique

Suppose we have chosen a finite basis B for the vector space V. Let $[\ \ ]_B$ denote the corresponding coordinate vector map, and let $[\ \ ]_B^{-1}$ denote the inverse of this map.

Any linear algebraic questions we want to answer about V (involving span, linear independence, etc.) can be answered as follows:

1. First apply $[\ \ ]_B$ to all vectors $\mathbf{v}$ in question.
2. Answer the corresponding question in $\mathbb{R}^n$ about the column vectors $[\mathbf{v}]_B$.
3. If necessary, translate your results back to the setting of V by applying the inverse $[\ \ ]_B^{-1}$.

Example

The set

$$S = \left\{ A_1 = \begin{bmatrix} 2 & 1 \\ 0 & -2 \end{bmatrix}, A_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, A_3 = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, A_4 = \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix} \right\}$$

is a subset of the space $W = \{A \in M_{22} \colon \operatorname{tr} A = 0\}$. (Recall: the trace of a matrix, $\operatorname{tr} A$, is defined as the sum of its diagonal elements.)
Contract S to a basis of $\operatorname{span} S$, and determine whether $\operatorname{span} S = W$. Use the coordinate vector map technique!

We must first pick a basis for W. Observe that the general element of of W can be described as

$$\begin{bmatrix} a & b \\ c & -a \end{bmatrix} = a \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}_{B_1} + b \underbrace{\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}}_{B_2} + c \underbrace{\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}}_{B_3}.$$

It follows easily that $B = \{B_1, B_2, B_3\}$ is a basis for W.

Apply $[\quad]_B$ to the elements of the given S to get a corresponding set $S' \subseteq \mathbb{R}^3$:

$$S' = \{[A_1]_B = (2,1,0), [A_2]_B = (1,1,1), [A_3]_B = (0,1,2), [A_4]_B = (-1,0,1)\}$$

Now use the "contract to basis" algorithm on S' to conclude that the set $\{(2,1,0),(1,1,1)\}$ forms a basis for $\operatorname{span} S'$. Translating back to W, we see that A_1 and A_2 form a basis for $\operatorname{span} S$, that $\dim \operatorname{span} S = 2$, and hence that $\operatorname{span} S \neq W$, since $\dim W = 3$.

Matrix representations of transformations

We have seen how the coordinate vector map can be used to translate a linear algebraic question posed about the exotic vector space V into a question about the more familiar vector space $\mathbb{R}^n$, where we have many computational algorithms at our disposal.
We would like to extend this technique to linear transformations $T: V \to W$, where both V and W are finite-dimensional. The basic idea, to be fleshed out below, can be described as follows:

1. Pick a basis B for V, and a basis B' for W.
2. "Identify" V with $\mathbb{R}^n$ and W with $\mathbb{R}^m$ using the coordinate vector isomorphisms $[\quad]_B$ and $[\quad]_{B'}$, respectively.
3. "Model" the linear transformation $T: V \to W$ with a certain linear transformation $T_A: \mathbb{R}^n \to \mathbb{R}^m$.

The matrix A defining T_A will be called the matrix representing T with respect to our choice of basis B for V and B' for W.

In what sense does A "model" T? All the properties of T we are interested in (null T, nullity T, col T, rank T, etc.) are perfectly mirrored by the matrix A.

As a result, this technique allows us to answer questions about the original T essentially by applying a relevant matrix algorithm to A.

Matrix representations of transformations

Given: $T\colon V \to W$ a linear transformation, $\dim V = n$, $\dim W = m$.

First choose bases $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ for V and $B' = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ for W. These two bases give rise to two coordinate vector isomorphisms:

$$[\ \ ]_B \colon V \to \mathbb{R}^n$$
$$[\ \ ]_{B'} \colon W \to \mathbb{R}^m$$

Putting all three of these maps together yields the diagram

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, leftrightarrow, "{[\ \ ]_B}"'] & W \arrow[d, leftrightarrow, "{[\ \ ]_{B'}}"] \\ \mathbb{R}^n & \mathbb{R}^m \end{tikzcd}$$

where the double-headed arrows indicate the fact that the coordinate maps are isomorphisms: i.e., we also have inverse maps $([\ \ ]_B)^{-1}$, $([\ \ ]_{B'})^{-1}$ going up. The matrix A representing T with respect to the bases B and B' will be the matrix that "completes" this diagram by supplying an arrow from $\mathbb{R}^n$ to $\mathbb{R}^m$.

Crucial in our discussion will be the theorem stating that

(i) a linear transformation can be defined simply by declaring where basis elements are sent, and

(ii) the linear transformation is uniquely determined by this choice.

So we want a matrix A “completing” the previous diagram like so:

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, leftrightarrow, "{[\ \ ]_B}"'] & W \arrow[d, leftrightarrow, "{[\ \ ]_{B'}}"] \\ \mathbb{R}^n \arrow[r, "A"'] & \mathbb{R}^m \end{tikzcd}$$

More precisely, we want the diagram to be commutative.

This means that if we start at V and go right with T, then down with $[\ \ ]_{B'}$, this is the same as first going down with $[\ \ ]_B$, then right with A.

In terms of function compositions this means we want $[\ \ ]_{B'} \circ T = A \circ [\ \ ]_B$, or equivalently

$$\boxed{[T(\mathbf{v})]_{B'} = A[\mathbf{v}]_B, \text{ for all } \mathbf{v} \in V}.$$

Computing the matrix A

$$\boxed{[T(\mathbf{v})]_{B'} = A[\mathbf{v}]_B, \text{ for all } \mathbf{v} \in V}.$$

We now use the boxed condition to compute A column by column. Let $\mathbf{c}_j$ denote the j-th column of A.

By the column method of matrix multiplication we have

$$\begin{aligned}
\mathbf{c}_j &= A\mathbf{e}_j \text{ ($\mathbf{e}_j$ the j-th element of standard basis)} \\
&= A[\mathbf{v}_j]_B \text{ ($\mathbf{v}_j$ the j-th element of basis B)} \\
&= [T\mathbf{v}_j]_{B'}
\end{aligned}$$

Thus we have a formula for computing the j-th column of A:

$$\boxed{\mathbf{c}_j = [T[v_j]]_{B'}}$$

The matrix A we obtain in this fashion is called the **matrix for T relative to the bases B and B'**, and is denoted $A = [T]_B^{B'}$.

Let's record our results as a theorem.

Theorem 4.1 (Matrix representation theorem)

Let V, W be finite-dimensional vector spaces, let $T\colon V \to W$ be linear, let $B = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ be a basis for V, and let B' be a basis for W. There is a unique matrix A satisfying the following property:

$$[T(\mathbf{v})]_{B'} = A[\mathbf{v}]_B \text{ for all } \mathbf{v} \in V.$$

The matrix is denoted $A = [T]_B^{B'}$ and can be computed column by column using the recipe $\mathbf{a}_j = [T(\mathbf{v}_j)]_{B'}$, where $\mathbf{a}_j$ is the j-th column of A.

The theorem is summed up by the following commutative diagram:

$$\begin{tikzcd}
V \arrow[r, "T"] \arrow[d, leftrightarrow, "{[\ \ ]_B}"'] & W \arrow[d, leftrightarrow, "{[\ \ ]_{B'}}"] \\
\mathbb{R}^n \arrow[r, "{A=[T]_B^{B'}}"'] & \mathbb{R}^m
\end{tikzcd}$$

Corollary 4.1.1 (Computational method)

Any question about the linear transformation T can be answered by first answering the analagous question for the matrix $A = [T]_B^{B'}$, and then translating your results back to V and W using $[\ \ ]_B^{-1}$ and $[\ \ ]_{B'}^{-1}$.

Example

Define $T\colon P_3 \to P_2$ by $T(p(x)) = p'(x)$. Compute $A = [T]_B^{B'}$, where B and B' are the standard bases for P_3 and P_2, respectively.
Use A to determine null T and range T.

Solution: The matrix A will be 3×4. Denote by $\mathbf{c}_j$ the j-th column of A. We use the formula for $\mathbf{c}_j$:

$$\mathbf{c}_1 = [T(1)]_{B'} = [0]_{B'} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \qquad \mathbf{c}_2 = [T(x)]_{B'} = [1]_{B'} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

$$\mathbf{c}_3 = [T(x^2)]_{B'} = [2x]_{B'} = \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix} \qquad \mathbf{c}_4 = [T(x^3)]_{B'} = [3x^2]_{B'} = \begin{bmatrix} 0 \\ 0 \\ 3 \end{bmatrix}$$

Thus $A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$.

We see easily that null $A = \text{span}(\{(1,0,0,0)\})$ and range $A = \text{col}\, A = \mathbb{R}^3$. Translating everything back to the original spaces, we see that
null$(T) = \text{span}(\{1\}) = \{\text{constant poly.'s}\}$ and range$(T) = P_2$.

In the special case where $T\colon V \to V$ maps a space V to itself, when representing T with a matrix, we usually just pick a single basis B for V and compute

$$A = [T]_B^B =: [T]_B \quad \text{(our notation drops the redundant } B\text{)}$$

Example. Define $T\colon M_{22} \to M_{22}$ by $T(A) = A^T + A$.

Let B be the standard basis of M_{22}, and let

$$B' = \left\{ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

1. Compute $A = [T]_B$.
2. Compute $A' = [T]_{B'}$.

Solution:

$$A = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, A' = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Moral: our choice of basis affects the matrix representing T, and some choices are better than others!

$\mathbb{R}^n$ revisited

Consider the special case of the form $T\colon \mathbb{R}^n \to \mathbb{R}^m$. We know that in this case we have $T = T_A$, where

$$A = \begin{bmatrix} | & | & \cdots & | \\ T(\mathbf{e}_1) & T(\mathbf{e}_2) & \cdots & T(\mathbf{e}_n) \\ | & | & \cdots & | \end{bmatrix}.$$

In light of our recent discussion we recognize this as simply $A = [T]_B^{B'}$, where B, B' are the standard bases of $\mathbb{R}^n$ and $\mathbb{R}^m$.

This is certainly the most direct way of associating a matrix to the transformation T in this case, but it begs the question as to whether another choice of bases gives us a better matrix representation!
Example follows.

Example

Let $W\colon x + y + z = 0$ be the plane in $\mathbb{R}^3$ perpendicular to $\mathbf{n} = (1, 1, 1)$, and consider the orthogonal projection transformation $T = \mathrm{proj}_W\colon \mathbb{R}^3 \to \mathbb{R}^3$.

The recipe in the last slide tells us that $\mathrm{proj}_W = T_A$ where

$$A = \begin{bmatrix} 2/3 & -1/3 & -1/3 \\ -1/3 & 2/3 & -1/3 \\ -1/3 & -1/3 & 2/3 \end{bmatrix}.$$

This A is nothing more than $[T]_B$, where $B = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ is the standard basis of $\mathbb{R}^3$. We ask: Is there another basis B' for which the matrix $A' = [T]_{B'}$ is simpler?

Yes!! I'll build a basis that pays more attention to the geometry involved in defining T. Start first with a basis of the plane W: the set $\{\mathbf{v}_1 = (1, -1, 0), \mathbf{v}_2 = (0, 1, -1)\}$ will do. Now extend to a basis of $\mathbb{R}^3$. We need only add a vector that is not included already in W: the normal vector $\mathbf{v}_3 = (1, 1, 1)$ to the plane is a natural choice.

Thus we consider the basis $B' = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ and compute $A' = [\mathrm{proj}_W]_{B'}$: $A' =$

$$\begin{bmatrix} | & | & | \\ [T(\mathbf{v}_1)]_{B'} & [T(\mathbf{v}_2)]_{B'} & [T(\mathbf{v}_3)]_{B'} \\ | & | & | \end{bmatrix} = \begin{bmatrix} | & | & | \\ [\mathbf{v}_1]_{B'} & [\mathbf{v}_2]_{B'} & [\mathbf{0}]_{B'} \\ | & | & | \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Wow, A' is way simpler! How can both of these matrices "represent" the same linear transformation?

Example continued

Let $W\colon x+y+z=0$ be a the plane in $\mathbb{R}^3$ perpendicular to $\mathbf{n}=(1,1,1)$, and consider the orthogonal projection transformation $T=\operatorname{proj}_W\colon \mathbb{R}^3\to\mathbb{R}^3$.
Two different bases:
$B=\{\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3\}, B'=\{\mathbf{v}_1=(1,-1,0),\mathbf{v}_2=(0,1,-1),\mathbf{v}_3=(1,1,1)\}$.
Two different matrix representations:

$$A=[T]_B=\frac{1}{3}\begin{bmatrix}2&-1&-1\\-1&2&-1\\-1&-1&2\end{bmatrix},\ A'=[T]_{B'}=\begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix}.$$

The simpler matrix A' gives us a clear conceptual understanding of this orthogonal projection.
For example, we see that $\operatorname{col} A'=\operatorname{span}(\{(1,0,0),(0,1,0)\})$ and $\operatorname{null} A'=\operatorname{span}(\{(0,0,1)\})$, and furthermore A' acts as the identity on $\operatorname{col} A'$, and as the zero transformation on $\operatorname{null} A'$.

Using $[\ ]_{B'}^{-1}$ we can translate this information back to $T=\operatorname{proj}_W$. Namely, $\operatorname{range} T=\operatorname{span}\{(\mathbf{v}_1,\mathbf{v}_2)\}=W$, $\operatorname{null} T=\operatorname{span}\{\mathbf{v}_3\}=\operatorname{span}\{\mathbf{n}\}$, and furthermore, T acts as the identity on W and as the zero transformation on $\operatorname{span}\{\mathbf{n}\}$.

However, if we actually want an explicit formula for computing he orthogonal projection of a vector $\mathbf{x}\in\mathbb{R}^3$ onto W, we are better off using A, since we have $\operatorname{proj}_W(\mathbf{x})=A\mathbf{x}$.

So both representations have their own particular virtue! In the next section we develop a means for fluidly going back and forth between the two.

Change of basis

We have seen how the coordinate vector map $[\quad]_B$ and matrix representations $[T]_B^{B'}$ are two invaluable computational tools for dealing with abstract vector spaces.

As the notation indicates, both of these operations depend essentially on your choice of basis or bases. This gives rise to the following questions:

1. Given V and two choices of basis, B and B', what is the relation between $[\mathbf{v}]_B$ and $[\mathbf{v}]_{B'}$?
2. GIven $T\colon V \to W$ and two choices of pairs of bases, (B, B') and (B'', B'''), what is the relation between $[T]_B^{B'}$ and $[T]_{B''}^{B'''}$?

We will tackle both questions in turn. Both answers rely on something called a change of basis matrix $\underset{B\to B'}{P}$.

For question (2), we will look at the slightly less general situation where $T\colon V \to V$: i.e., the situation where $W = V$, and we choose the same basis for the domain and codomain. I leave the full general case as an exercise.

Change of basis matrix

Theorem/Definition

Given a vector space V of dimension n, and two different bases B and B', there is a unique $n \times n$ matrix $\underset{B \to B'}{P}$ satisfying the following defining property:

$$\underset{B \to B'}{P} [\mathbf{v}]_B = [\mathbf{v}]_{B'}.$$

The matrix $\underset{B \to B'}{P}$ is called the **change of basis matrix (or transition matrix) from B to B'**.

Proof/recipe.

Let $B = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ and let $B' = \{\mathbf{w}_1, \dots, \mathbf{w}_n\}$.
We build $\underset{B \to B'}{P}$ column by column: specifically, $\underset{B \to B'}{P}$ is the matrix whose j-th column is

$$\boxed{\mathbf{p}_j = [\mathbf{v}_j]_{B'}};$$

i.e., to compute the j-th column of $\underset{B \to B'}{P}$ you must find the B'-coordinates of the j-th basis element of B.
Thus defined, one can show using the column method that $\underset{B \to B'}{P} [\mathbf{v}_j]_B = [\mathbf{v}_j]_{B'}$.
One then argues that if the condition is true for each basis element $\mathbf{v}_j$, then it must be true for all $\mathbf{v}$. (Ask your professor for details!) □

Example. For any vector space V and basis B, we have $\underset{B\to B}{P} = I$.

Indeed for any vector $\mathbf{v}$, we have $I[\mathbf{v}]_B = [\mathbf{v}]_B$. Thus I satisfies the defining property of $\underset{B\to B}{P}$. By uniqueness, it follows that $I = \underset{B\to B}{P}$!!

Example. Let $V = \mathbb{R}^2$. Compute $\underset{B\to B'}{P}$ where $B = \{\mathbf{v}_1 = (1,1), \mathbf{v}_2 = (1,-1)\}$ and $B' = \{(1,2),(2,1)\}$.
Test that the matrix converts correctly using the vector
$\mathbf{v} = 1(1,1) + 3(1,-1) = (4,-2)$.

Solution: The recipe tells us that

$$\begin{aligned}\underset{B\to B'}{P} &= \begin{bmatrix} | & | \\ [\mathbf{v}_1]_{B'} & [\mathbf{v}_2]_{B'} \\ | & | \end{bmatrix} \\ &= \begin{bmatrix} 1/3 & -1 \\ 1/3 & 1 \end{bmatrix} \quad \text{(after some computation)}\end{aligned}$$

For $\mathbf{v} = 1(1,1) + 3(1,-1) = (4,-2)$, we have $(\mathbf{v})_B = (1,3)$. Thus we should have

$$[\mathbf{v}]_{B'} = \underset{B\to B'}{P}[\mathbf{v}]_B = \begin{bmatrix} 1/3 & -1 \\ 1/3 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 3 \end{bmatrix} = \begin{bmatrix} -8/3 \\ 10/3 \end{bmatrix}.$$

Indeed, one easily verifies that $(4,-2) = -8/3(1,2) + 10/3(2,1)$.

Example

Take $V = P_2$, $B = \{1, x, x^2\}$ and $B' = \{1, (x-2), (x-2)^2\}$. Compute $\underset{B \to B'}{P}$.

Follow the recipe: let $\mathbf{p}_j$ be the j-th column of $\underset{B \to B'}{P}$. We have (after some computation)

$$\mathbf{p}_1 = [1]_{B'} = (1, 0, 0), \ \mathbf{p}_2 = [x]_{B'} = (2, 1, 0), \ \mathbf{p}_3 = [x^2]_{B'} = (4, 4, 1).$$

Thus $\underset{B \to B'}{P} = \begin{bmatrix} 1 & 2 & 4 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}$

Let's check with the test vector $p(x) = 1 + x + x^2$. We have $(p)_B = (1, 1, 1)$.

Thus we should have $[p]_{B'} = \underset{B \to B'}{P}[p]_B = \begin{bmatrix} 1 & 2 & 4 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 7 \\ 5 \\ 1 \end{bmatrix}$.

Equivalently, this means that $p(x) = 7 + 5(x-2) + (x-2)^2$, as one easily verifies.

Cool fact. We could have derived the last equality using the theory of Taylor series. Namely any polynomial can be "expanded around $x = a$" as $p(x) = \sum_{i=0}^{n} \frac{p^{(i)}(a)}{a!}(x-a)^i$.

More generally, this means

$$(p(x))_{B'} = (p(a), p'(a), p''(a)/2, \ldots, p^{(n)}(a)/n!)$$

where $B' = \{1, x-a, (x-a)^2, \ldots, (x-a)^n\}$.

Theorem. Let V be a vector space of dimension n, and let B and B' be two different bases of V.
The change of basis matrix $\underset{B\to B'}{P}$ is invertible. In fact we have

$$\left(\underset{B\to B'}{P}\right)^{-1} = \underset{B'\to B}{P}$$

Proof. I will show that $\underset{B'\to B}{P} \cdot \underset{B\to B'}{P} = I_n$, proving that both matrices are invertible, and are in fact the inverses of one another. My proof will only make use of the defining property of change of basis matrices, and their uniqueness.
For any $\mathbf{v}$ we compute:

$$\begin{aligned} \underset{B'\to B}{P} \cdot \underset{B\to B'}{P}[\mathbf{v}]_B &= \underset{B'\to B}{P}\left(\underset{B\to B'}{P}[\mathbf{v}]_B\right) \\ &= \underset{B'\to B}{P}[\mathbf{v}]_{B'} \quad (\text{prop. of } \underset{B\to B'}{P}) \\ &= [\mathbf{v}]_B \qquad\quad (\text{prop. of } \underset{B'\to B}{P}) \end{aligned}$$

Thus $\underset{B'\to B}{P} \cdot \underset{B\to B'}{P}[\mathbf{v}]_B = [\mathbf{v}]_B$ for all $\mathbf{v} \in V$. But this means $\underset{B'\to B}{P} \cdot \underset{B\to B'}{P}$ satisfies the defining property of $\underset{B\to B}{P}$.

By uniqueness of the change of basis matrix, we must have

$$\underset{B'\to B}{P} \cdot \underset{B\to B'}{P} = \underset{B\to B}{P}$$

Lastly, in a previous example we showed that $P_{B\to B} = I_n$. Thus,

$$\underset{B'\to B}{P} \cdot \underset{B\to B'}{P} = \underset{B\to B}{P} = I_n,$$

as claimed.

Example: $V = \mathbb{R}^n$ and B is standard

Consider the simple example where $V = \mathbb{R}^n$, B is the standard basis, and $B' = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is some nonstandard basis.

I claim the matrix $P = \begin{bmatrix} | & \dots & | \\ \mathbf{v}_1 & \cdots & \mathbf{v}_n \\ | & \dots & | \end{bmatrix}$ whose columns are the elements of B' is the change of basis matrix $\underset{B' \to B}{P}$. This follows from our recipe since $\mathbf{v}_j = [\mathbf{v}_j]_B$. (Recall: when B is the standard basis $[(a_1, a_2, \dots, a_n)]_B = (a_1, a_2, \dots, a_n)$ for all $(a_1, a_2, \dots, a_n) \in \mathbb{R}^n$.)

Since $\underset{B \to B'}{P} = (\underset{B' \to B}{P})^{-1}$, we see that in this special case we can compute $\underset{B' \to B}{P}$ by placing the elements of B' as columns of a matrix, and then compute $\underset{B \to B'}{P}$ by taking the inverse of this matrix!

Example. Let $V = \mathbb{R}^2$, B the standard basis for $\mathbb{R}^2$, and $B' = \{(1, \sqrt{3}), (-\sqrt{3}, 1)\}$.
Find $P_{B \to B'}$.

Solution: The recipe above tells us that $\underset{B' \to B}{P} = \begin{bmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{bmatrix}$ and hence that

$$\underset{B \to B'}{P} = (\underset{B' \to B}{P})^{-1} = \left(\begin{bmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{bmatrix} \right)^{-1} = \frac{1}{4} \begin{bmatrix} 1 & \sqrt{3} \\ -\sqrt{3} & 1 \end{bmatrix}.$$

Alternative technique when $V = \mathbb{R}^n$

The following is another technique for computing $\underset{B \to B'}{P}$ in the special case where $V = \mathbb{R}^n$.

1. Let $\widetilde{B}$ and $\widetilde{B'}$ be the matrices obtained by arranging the elements of B, respectively B', as columns of a matirx. Build the augmented matrix

$$\left[\widetilde{B'} \mid \widetilde{B}\right]$$

2. Row reduce the augmented matrix until the left hand side is I_n:

$$\left[I_n \mid Q\right]$$

Then $Q = \underset{B \to B'}{P}$.

Why does this work?

The row reduction process amounts to multiplying both matrices on the left by $(\widetilde{B'})^{-1}$: that is, the matrix Q is $(\widetilde{B'})^{-1}\widetilde{B}$. As we saw in the last example, however, letting S be the standard basis of $\mathbb{R}^n$, we have

$$(\widetilde{B'})^{-1} = \underset{S \to B'}{P} \text{ and } \widetilde{B} = \underset{B \to S}{P}$$

Thus $Q = \underset{S \to B'}{P} \cdot \underset{B \to S}{P} = \underset{B \to B'}{P}$. (This last equality follows from one of the exercises.)

Change of basis for transformations

We now investigate how our choice of basis affects matrix representations of linear transformations. As mentioned above, we only consider the special case where $T\colon V \to V$ and we are comparing matrix representations $[T]_B$ and $[T]_{B'}$ for two choices of basis for V.

Theorem 5.1 (Change of basis for transformations)

Let V be finite-dimensional, let $T\colon V \to V$ be linear, and let B and B' be two bases for V. Then

$$\begin{aligned} [T]_{B'} &= \underset{B\to B'}{P}[T]_B \underset{B'\to B}{P} && (1) \\ &= \left(\underset{B'\to B}{P}\right)^{-1} [T]_B \underset{B'\to B}{P} && (2) \end{aligned}$$

Pro-tip

It is easy to get the various details of the change of basis formula wrong. Here is how I organize things in my mind.

1. We wish to relate $[T]_{B'}$ and $[T]_B$ with an equation of the form $[T]_{B'} = *[T]_B*$, where the asterisks are to be replaced with change of basis matrices or their inverses. Think of the three matrices on the RHS as a sequence of three things done to coordinate vectors, reading from right to left.
2. $[T]_{B'}$ takes as inputs B'-coordinates of vectors, and outputs B'-coordinates. Thus the same should be true for $*[T]_B*$.
3. Since $[T]_B$ takes as inputs B-coordinates, we must first convert from B'-coordinates to B-coordinates. So we should have $[T]_{B'} = *[T]_B \underset{B' \to B}{P}$.
4. Since $[T]_B$ outputs B-coordinates, we need to then convert back to B'-coordinates. Thus $[T]_{B'} = \underset{B \to B'}{P} [T]_B \underset{B' \to B}{P}$.
5. If desired you may replace $\underset{B \to B'}{P}$ with $\left(\underset{B' \to B}{P} \right)^{-1}$.

Proof of change of basis theorem

Theorem recap. Let V be finite-dimensional, let $T: V \to V$ be linear, let B and B' be two bases for V, and let $A = [T]_B$, $A' = [T]_{B'}$.

Then $\boxed{A = (\underset{B\to B'}{P})^{-1} A' \underset{B\to B'}{P}}$ and $\boxed{A' = (\underset{B'\to B}{P})^{-1} A \underset{B'\to B}{P}}$

First recall that $\underset{B'\to B}{P} = (\underset{B\to B'}{P})^{-1}$. Using this fact, it is easy to see that the second equality follows from the first by multiplying on the left and right by an appropriate matrix and its inverse.

We prove the first equality using the uniqueness property of $A = [T]_B$.

That is, set $C = (\underset{B\to B'}{P})^{-1} A' \underset{B\to B'}{P}$.

To show $C = A$, we need only show $[T(\mathbf{v})]_B = C[\mathbf{v}]_B$ for all $\mathbf{v} \in V$. Here goes:

$$\begin{aligned}
C[\mathbf{v}]_B &= (\underset{B\to B'}{P})^{-1} A' \underset{B\to B'}{P} [\mathbf{v}]_B \\
&= \underset{B'\to B}{P} A' \underset{B\to B'}{P} [\mathbf{v}]_B \quad (\text{since } \underset{B'\to B}{P} = (\underset{B\to B'}{P})^{-1}) \\
&= \underset{B'\to B}{P} A' [\mathbf{v}]_{B'} \quad (\text{prop. of } \underset{B\to B'}{P}) \\
&= \underset{B'\to B}{P} [T(\mathbf{v})]_{B'} \quad (\text{prop. of } A' = [T]_{B'}) \\
&= [T(\mathbf{v})]_B
\end{aligned}$$

Amazing! We didn't even have to get our hands dirty.

Example

Let $T\colon P_2 \to P_2$ be defined as $T(p(x)) = p(x) + 2p'(x) + xp''(x)$.

1. Let $B = \{1, x, x^2\}$. Compute $[T]_B$.
2. Let $B' = \{1 + x + x^2, 1 + x, 1 + x^2\}$. Use the change of basis formula to compute $[T]_{B'}$.

We easily compute $[T]_B = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}$ using our usual recipe.

We can also easily compute $\underset{B' \to B}{P} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$, essentially by inspection.

(In general it is easy to compute the change of basis matrix from a nonstandard basis to the standard basis.)

It follows that

$$
\begin{aligned}
[T]_B' &= \underset{B \to B'}{P} [T]_B \underset{B' \to B}{P} = \left(\underset{B' \to B}{P} \right)^{-1} [T]_B \underset{B' \to B}{P} \\
&= \left(\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \right)^{-1} \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & -2 & 4 \\ 2 & 3 & 0 \\ -2 & 2 & -3 \end{bmatrix}
\end{aligned}
$$

The change of basis formula is often used in the following type of situation.

1. I am interested in a linear transformation $T\colon V \to V$, where V is finite-dimensional.
2. I would like to compute $A = [T]_B$ with respect to a specific basis B. (Maybe B is a standard basis for V that I prefer to use.)
3. For whatever reason, it is easier to compute $A' = [T]_{B'}$ with respect to some other basis B'
4. Thus we first compute $[T]_{B'}$, then compute $[T]_B$ via the formula

$$[T]_B = \underset{B' \to B}{P} [T]'_B \underset{B \to B'}{P}.$$

The next example nicely illustrates this.

Example: orthogonal projection revisited

Let $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ be orthogonal projection onto the plane $\mathcal{P} : x + y + z = 0$, as defined earlier. We would like to derive a formula for T, which amounts to finding the A such that $T = T_A$.

As previously observed we have $A = [T]_B$, where B is the standard basis for $\mathbb{R}^3$. We can compute $[T]_B$ by first computing $[T]_{B'}$ for a cleverly chosen nonstandard basis B', and then using the change of basis formula.

As done previously, we let $B' = \{(1,-1,0),(1,0,-1),(1,1,1)$. Since T maps the first two vectors to themselves, and the third vector to $(0,0,0)$, we have $[T]_{B'} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. (Go back to original example for details.)

Then

$$
\begin{aligned}
A = [T]_B &= \underset{B'\to B}{P}[T]_{B'}\underset{B\to B'}{P} \\
&= \begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}\left(\begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{bmatrix}\right)^{-1} = \frac{1}{3}\begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}
\end{aligned}
$$

Lo and behold, we have rediscovered our matrix formula for orthogonal projection onto $\mathcal{P}$!!

(Note: since B is the standard basis in this case, $\underset{B'\to B}{P}$ was easy to compute.)

Similar matrices

Let $A = [T]_B$ and $A' = [T]_{B'}$ be two different representations of $T\colon V \to V$, and set $P = \underset{B' \to B}{P}$. Then we have $A' = P^{-1}AP$, according to the change of basis formula for transformations. We say A and A' are similar matrices in this case.

Definition 5.1

Matrices $A, A' \in M_{nn}$ are **similar** if there is an invertible matrix P such that $A' = P^{-1}AP$.

This notion of similarity is a technical one, but the name is fitting: A and A' really are similar in the sense that they are just two different matrix representations of the same linear transformation! (See Holy Commutative Tent of Linear Algebra on next slide.)

As we will see in coming sections, matrices that are similar in this technical sense do indeed share many of the same properties. We now have the theoretical foundation to understand why this is so: they simply inherit these common properties from the overlying linear transformation T, of which they are but earthly shadows.

There is but one true T!

Holy Commutative Tent of Linear Algebra

$$
\begin{tikzcd}
V \arrow[rrr, "T"] \arrow[dd, leftrightarrow, "{[\ ]_B}"'] \arrow[dr, leftrightarrow, "{[\ ]_{B'}}"] & & & V \arrow[dd, leftrightarrow, "{[\ ]_B}"'] \arrow[dr, leftrightarrow, "{[\ ]_{B'}}"] & \\
& \mathbb{R}^n \arrow[rrr, "{A'=[T]_{B'}}"] \arrow[dl, "P_{B'\to B}"'] & & & \mathbb{R}^n \\
\mathbb{R}^n \arrow[rrr, "{A=[T]_B}"] & & & \mathbb{R}^n \arrow[ur, "P_{B\to B'}"'] &
\end{tikzcd}
$$

$$\boxed{A' = P^{-1} A P, \text{ where } P = P_{B'\to B}}$$

Diagonalizable matrices

Definition 7.1

An $n \times n$ matrix A is **diagonalizable** if there is an invertible matrix P such that $D = P^{-1}AP$ is diagonal.

In other words, A is diagonalizable if it is similar to a diagonal matrix D.

Comments

1. If A is itself diagonal, then it is diagonalizable: we may choose $P = I_n$ in the definition.
2. In this section we will develop a systematic procedure for determining whether a matrix is diagonalizable. As we will see, the answer is yes if and only if A has "enough" linearly independent eigenvectors. Of course we will spell out precisely what we mean by "enough".
3. Not all matrices are diagonalizable. For example, $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ is not diagonalizable, as the aforementioned procedure will show.
4. Roughly speaking, you should interpret being diagonalizable as meaning "as good as diagonal". To elaborate: doing arithmetic with diagonal matrices D is extremely easy; if we know A is diagonalizable, meaning it is similar to a diagonal matrix D, then it shares many essential properties of D, and we can use the relation $D = P^{-1}AP$ to help ease arithmetic computations involving A.

Properties of conjugation

If we have, $D = P^{-1}AP$, why exactly is there such a close connection between D and A? One explanation has to do with the underlying operation

$$A \longmapsto P^{-1}AP,$$

which we call conjugation by P. As the following theorem outlines, conjugation by an invertible P satisfies many useful properties, and we use these to relate the matrix A with the matrix $P^{-1}AP$.

Theorem 7.1 (Properties of conjugation)

Let P be any invertible $n \times n$ matrix.

1. $P^{-1}(c_1A_1 + c_2A_2)P = c_1P^{-1}A_1P + c_2P^{-1}A_2P$. (Conjugation by P is a linear transformation.)
2. $P^{-1}A^nP = (P^{-1}AP)^n$ for any integer $n \geq 0$. If A is invertible, the equality holds for *all* integers n. (Conjugation preserves powers.)
3. Recall that given any polynomial $f(x) = a_nx^n + a_{n-1}x^{n-1} \cdots + a_1x + a_0$ and any $n \times n$ matrix A we define $f(A) = a_nA^n + a_{n-1}A^{n-1} + a_1A + a_0I_n$. We have $f(P^{-1}AP) = P^{-1}f(A)P$ for any polynomial $f(x)$, and any $n \times n$ matrix A. (Conjugation preserves polynomial evaluation.)

Proof.

Exercise. $\square$

Examples: utility of diagonalizability

Suppose A is diagonalizable, so that $D = P^{-1}AP$, where D is diagonal with diagonal entries d_i. Using Theorem 7.1, we can now see how to translate statements about D (which are generally easy to prove), to statements about A (which otherwise might have been difficult to show).

Example 7.1

To compute A^n (hard) we can just compute D^n (easy) and then observe that $A = PDP^{-1}$, and thus

$$A^n = (PDP^{-1})^n = PD^nP^{-1},$$

where the last equality follows from part (b) of Theorem 7.1; here we let P^{-1} assume the role of P in the theorem statement.

For example, let $A = \begin{bmatrix} 1 & 3 \\ 1 & -1 \end{bmatrix}$. Let's compute A^n for arbitrary n.

We have $D = P^{-1}AP$, where $D = \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix}$, and $P = \begin{bmatrix} 3 & 1 \\ 1 & -1 \end{bmatrix}$. (This is not obvious yet. Soon we will have the tools to see why this is so.)

Then $A = PDP^{-1}$, and thus

$$A^n = PD^nP^{-1} = P \begin{bmatrix} 2^{100} & 0 \\ 0 & (-2)^{100} \end{bmatrix} P^{-1} = \frac{1}{4} \begin{bmatrix} 3 \cdot 2^n + (-2)^n & 3 \cdot 2^n - 3(-2)^n \\ 2^n - (-2)^n & 2^n + 3(-2)^n \end{bmatrix}.$$

Examples: utility of diagonalizability

Suppose A is diagonalizable, so that $D = P^{-1}AP$, where D is diagonal with diagonal entries d_i.

Example 7.2

More generally, we have $f(A) = f(PDP^{-1}) = Pf(D)P^{-1}$ for any polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} \cdots + a_1 x + a_0$. Since D is diagonal, with diagonal entries d_i, it is easy to see that $f(D)$ is also diagonal, with diagonal entries $f(d_i)$.

In particular we see that $f(A) = \underset{n \times n}{\mathbf{0}}$ if and only if $f(D) = \underset{n \times n}{\mathbf{0}}$, and this holds if and only if $f(d_i) = 0$ for each diagonal entry d_i of D.

Take the matrix A from Example 7.1, and let $f(x) = (x-2)(x+2) = x^2 - 4$. Since $f(2) = f(-2) = 0$, it follows that $f(D) = f(A) = \underset{2 \times 2}{\mathbf{0}}$. In other words, $A^2 - 4I = \underset{2 \times 2}{\mathbf{0}}$, as you can easily check.

Examples: utility of diagonalizability

Suppose A is diagonalizable, so that $D = P^{-1}AP$, where D is diagonal with diagonal entries d_i.

Example 7.3

A has a square-root (i.e., a matrix B such that $B^2 = A$) iff D has a square-root.

Indeed, suppose $B^2 = A$. Set $C = P^{-1}BP$. Then $C^2 = P^{-1}B^2P = P^{-1}AP = D$. Similarly, if $C^2 = D$, then $B^2 = A$, where $B = PCP^{-1}$.

As an example, the matrix $A = \begin{bmatrix} 0 & -2 \\ 1 & 3 \end{bmatrix}$, satisfies $D = P^{-1}AP$, where $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$, and $P = \begin{bmatrix} 2 & 1 \\ -1 & -1 \end{bmatrix}$. Since $C = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{bmatrix}$ is a square-root of D, $B = PCP^{-1} = \begin{bmatrix} 2-\sqrt{2} & 2-2\sqrt{2} \\ -1+\sqrt{2} & -1+2\sqrt{2} \end{bmatrix}$ is a square-root of A, as you can easily check.

So when exactly does a diagonal matrix D have a square-root? Clearly, it is sufficient that $d_i \geq 0$ for all i, as in the example above. Interestingly, this is not a necessary condition! Indeed, consider the following example:

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

Properties of similarity

Before investigating the question of when a matrix is diagonalizable, we record a few more properties illustrating the close connection between similar matrices.

Theorem 7.2 (Properties of similarity)

Suppose A is similar to B: i.e., there is an invertible matrix P such that $B = P^{-1}AP$. Then:

(a) B is similar to A. (Similarity is symmetric.)

(b) A and B have the same trace and determinant.

(c) A and B have the same rank.

(d) A and B have the same characteristic polynomial.

(e) A and B have the same eigenvalues.

(f) Given any $\lambda \in \mathbb{R}$, let W_λ be the corresponding eigenspace for A, and W'_λ the corresponding eigenspace for B. Then $\dim W_\lambda = \dim W'_\lambda$.

The proof of (d) follows. I leave the rest as an exercise.

Proof of Theorem 7.2.d.

By definition we have $B = P^{-1}AP$ for some matrix P. We wish to show the characteristic polynomials $p_A(t)$ and $p_B(t)$ of the two matrices are equal. Compute:

$$
\begin{aligned}
p_B(t) &= \det(tI - B) \\
&= \det(tI - P^{-1}AP) \\
&= \det(tP^{-1}IP - P^{-1}AP) \;\; (\text{since } P^{-1}IP = I) \\
&= \det(P^{-1}tIP - P^{-1}AP) \;\; (t \text{ behaves as scalar}) \\
&= \det(P^{-1}(tI - A)P) \\
&= \det(P^{-1})\det(tI - A)\det(P) \\
&= (\det(P))^{-1}\det(P)\det(tI - A) \\
&= \det(tI - A) = p_A(t).
\end{aligned}
$$

$\square$

The true meaning of similarity

Hopefully Theorems 7.1 and 7.2 convince you that similar matrices (in the linear algebraic sence) are truly similar (in the usual sense).

There is, however, a deeper explanation for this. Namely, if A and A' are similar, then they are simply two different matrix representations of a common linear transformation!

In more detail: suppose we have $A' = P^{-1}AP$.

- Let B be the standard basis of $\mathbb{R}^n$, and let B' be the basis of $\mathbb{R}^n$ obtained by taking the columns of the invertible matrix P. Finally, let $T = T_A$ be the matrix transformation associated to A.
- Then $A = [T]_B$, $P = \underset{B' \to B}{P}$, and $P^{-1} = \underset{B \to B'}{P}$.
- From the change of basis formula it follows that

$$A' = P^{-1}AP = \underset{B \to B'}{P}[T]_B \underset{B' \to B}{P} = [T]_{B'}$$

In other words to say A and A' are similar is simply to say that they are different matrix representations of the same overlying linear transformation T (see Holy Commutative Tent of Linear Algebra on next slide). All their shared properties (same eigenvalues, same determinant, same trace, etc.) are simply the properties they inherit from this one overlying T, of which they are but earthly shadows.

There is one true T!

Holy Commutative Tent of Linear Algebra

$$\begin{tikzcd}
V \arrow[rr, "T"] \arrow[dd, leftrightarrow, "{[\ ]_B}"'] \arrow[dr, leftrightarrow, "{[\ ]_{B'}}"] & & V \arrow[dd, leftrightarrow, "{[\ ]_B}"'] \arrow[dr, leftrightarrow, "{[\ ]_{B'}}"] & \\
& \mathbb{R}^n \arrow[rr, "{A' = [T]_{B'}}"] \arrow[dl, "P_{B' \to B}"'] & & \mathbb{R}^n \\
\mathbb{R}^n \arrow[rr, "{A = [T]_B}"] & & \mathbb{R}^n \arrow[ur, "P_{B \to B'}"'] &
\end{tikzcd}$$

$$\boxed{A' = P^{-1} A P, \text{ where } P = P_{B' \to B}}$$

The previous theorem allows us to extend some of our matrix definitions to linear transformations.

Definition 7.2

Let $T\colon V \to V$ be linear, let B be any basis of V, and let $A = [T]_B$. We define the **characteristic polynomial** of T to be $p(t) = \det(tI - A)$.

Comment

Note that the characteristic polynomial defined above does not depend on the choice of basis B. If B' is another basis, and $A' = [T]_{B'}$, then A' and A are similar, as we have seen, and thus have the same characteristic polynomial.

Definition 7.3

A linear transformation $T\colon V \to V$ is **diagonalizable** if there exists a basis B of V for which $[T]_B$ is a diagonal matrix.

Comment

Equivalently, T is diagonalizable if for any choice of basis B the matrix $[T]_B$ is diagonalizable.

Diagonalizability and eigenvectors

At last we relate the property of being diagonalizable with the notion of eigenvectors. In the process we make clear what we mean when we say T is diagonalizable if and only if it has "enough" linearly independent eigenvectors.

Theorem 7.3 (Diagonalizability theorem)

Let $T\colon V \to V$ be linear, $\dim(V) = n$.

1. (Qualitative) Given basis B of V, the matrix $[T]_B$ is diagonal if and only if B consists of eigenvectors of T.

   Thus T is diagonalizable if and only if there is a basis of V consisting of eigenvectors of T.

2. (Quantitative) Let $\lambda_1, \lambda_2, \ldots, \lambda_r$ be the distinct eigenvalues of T, let W_{λ_j} be the corresponding eigenspaces, and let $n_j = \dim W_{\lambda_j}$.

   Then T is diagonalizable $\iff n_1 + n_2 + \cdots + n_r = n$.

Proof.

The first statement was a homework exercise. The proof of the second statement is within our means, but somewhat lengthy. I will sketch its proof elsewhere. For now it is more important to understand how to use the result. $\square$

Deciding whether $T\colon V \to V$ is diagonalizable

Suppose $\dim(V) = n$.

1. Pick a basis B of V. Set $A = [T]_B$
2. Find the distinct eigenvalues, $\lambda_1, \ldots, \lambda_r$, of A, let W_{λ_i} be the corresponding eigenspaces, and let $n_i = \dim W_{\lambda_i}$.
3. A (and thus T) is diagonalizable if and only if $n_1 + n_2 + \cdots + n_r = n$.
4. If the above equality is true, compute bases for each W_{λ_i} in $\mathbb{R}^n$.
5. Lift all vectors from all these bases back to V using $[\ \ ]_B$. This is a new basis B' of V consisting of eigenvectors of T.
6. $[T]_{B'} = D$ is diagonal.

Deciding whether $A_{n\times n}$ is diagonalizable

1. Find the distinct eigenvalues, $\lambda_1, \ldots, \lambda_r$, of A, let W_{λ_i} be the corresponding eigenspaces, and let $n_i = \dim W_{\lambda_i}$.
2. A is diagonalizable if and only if $n_1 + n_2 + \cdots + n_r = n$.
3. If the above equality is true, compute bases B_j for each W_{λ_j}.
4. Place all the vectors from the bases B_j as columns of a matrix P. As these eigenvectors are linearly independent, P is invertible.
5. The matrix $D = P^{-1}AP$ is diagonal.

   In more detail, the j-th diagonal entry of D is the eigenvalue associated to the eigenvector in the j-th column of P. This means the first n_1 diagonal entries of D are equal to λ_1, the next n_2 entries are equal to λ_2, etc.

Example

Take $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Earlier I claimed that this matrix is not diagonalizable. Let's see why.

The characteristic polynomial of A is $p(t) = (t-1)^2$. Thus $\lambda = 1$ is the only eigenvalue of A.

We have $W_1 = \text{null}(I - A) = \text{null} \begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix}$. We see clearly that $\text{rank}(I - A) = 1$, and hence $\dim W_1 = \dim \text{null}(I - A) = 2 - 1 = 1$.

Since W_1 is the only eigenspace, and since $\dim W_1 = 1 \neq 2$, we conclude A is not diagonalizable.

Example

Let $A = \begin{bmatrix} 14 & 21 & 3 & -39 \\ 12 & 25 & 3 & -41 \\ 12 & 24 & 5 & -42 \\ 12 & 22 & 3 & -38 \end{bmatrix}$.

The characteristic polynomial of A is $p(t) = x^4 - 6x^3 + 9x^2 + 4x - 12$. (This is not obvious, but would be a pain to compute in detail. You may take this for granted.)

Our usual factoring tricks allow us to factor this as $p(x) = (x-2)^2(x+1)(x-3)$.

The eigenspaces are $W_2 = \text{null}(2I - A)$, $W_{-1} = \text{null}(-I - A)$, and $W_3 = (3I - A)$. I'll leave it to you to verify that they have bases $B = \{(3, 2, 0, 2), (1, 1, 2, 1)\}$, $B' = \{(1, 1, 1, 1)\}$, and $B'' = \{(3, 5, 6, 4)\}$, respectively.

It follows that the dimensions of the eigenspaces are 2, 1, and 1, respectively. Since $2 + 1 + 1 = 4$, we conclude that A is diagonalizable.

In more detail, we have $D = P^{-1}AP$, where

$$D = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \quad P = \begin{bmatrix} 3 & 1 & 1 & 3 \\ 2 & 1 & 1 & 5 \\ 0 & 2 & 1 & 6 \\ 2 & 1 & 1 & 4 \end{bmatrix}$$

Geometric and algebraic multiplicity

Take A (or T) and suppose the characteristic polynomial $p(t)$ factors as

$$p(t) = (t - \lambda_1)^{n_1}(t - \lambda_2)^{n_2} \cdots (t - \lambda_r)^{n_r},$$

where the λ_i are the *distinct* eigenvalues of A (or T). It turns out that the exponent n_i, called the **algebraic multiplicity** of the eigenvalue λ_i, is an upper bound on $m_i = \dim W_{\lambda_i}$, called the **geometric multiplicity**.

Theorem 7.4 (Algebraic and geometric multiplicity theorem)

Let A (or T) have characterisitc polynomial

$$p(t) = (t - \lambda_1)^{n_1}(t - \lambda_2)^{n_2} \cdots (t - \lambda_r)^{n_r},$$

where the λ_i are the *distinct* eigenvalues of A (or T). Then

$$\dim W_{\lambda_i} \leq n_i :$$

i.e., the geometric multiplicity is less than or equal to the algebraic multiplicity.

Linear independence and eigenvectors

The following result is used to prove the diagonalizability theorem (Theorem 7.3), but is also very useful in its own right.

Theorem 7.5

Let $T\colon V \to V$ be a linear transformation, and let $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ be a set of eigenvectors of T with $T\mathbf{v}_i = \lambda_i \mathbf{v}_i$.
If the λ_i are all distinct, then S is linearly independent.

Proof.

Proved elsewhere. □

Corollary 7.5.1

Let $T\colon V \to V$ be a linear transformation, and suppose $\dim V = n$.
If T has n distinct eigenvalues, then T is diagonalizable.

Proof.

Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ be eigenvectors corresponding to these n distinct eigenvalues. The theorem tells us they form a linearly independent set. Since $\dim V = n$, they form a basis for V by the dimension theorem compendium. Since T has a basis of eigenvectors, it is diagonalizable. □

Theorem 7.5 makes no assumption about the dimension of V. It can thus be applied to interesting infinite-dimensional examples.

Example 7.4

Let $V = C^\infty(\mathbb{R})$, and let $T\colon V \to V$ be defined as $T(f) = f'$.
Let $f_i(x) = e^{k_i x}$, where the k_i are all distinct constants. I claim $S = \{f_1, f_2, \dots, f_r\}$ is linearly independent.

Indeed, each f_i is an eigenvector of T, since $T(f_i) = (e^{k_i x})' = k_i e^{k_i x} = k_i f_i$.

Since the k_i's are all distinct, it follows that the f_i are eigenvectors with distinct eigenvalues, hence linearly independent!
Note: try proving that S is linearly independent using the the Wronskian! You get a very interesting determinant computation.

Final extension of the invertibility theorem

Lastly, we can add one final statement to the invertibility theorem: A is invertible if and only if 0 is not an eigenvalue of A.

Indeed 0 is an eigenvalue of A if and only if $p(0) = \det(0I - A) = \det(-A) = 0$ if and only if $\det A = 0$, since $\det(-A) = (-1)^n \det A$.

Since $\det A = 0$ if and only if A is not invertible, we conclude that 0 is an eigenvalue of A if and only if A is not invertible.

You find the final version of the invertibility theorem on the next slide.

Theorem 7.6 (Invertibility theorem (final version))

Let A be $n \times n$. The following statements are equivalent.

(a) A is invertible.

(b) $A\mathbf{x} = \mathbf{0}$ has a unique solution (the trivial one).

(c) A is row equivalent to I_n, the $n \times n$ identity matrix.

(d) A is a product of elementary matrices.

(e) $A\mathbf{x} = \mathbf{b}$ has a solution for every $n \times 1$ column vector $\mathbf{b}$.

(f) $A\mathbf{x} = \mathbf{b}$ has a *unique* solution for every $n \times 1$ column vector $\mathbf{b}$.

(g) $\det(A) \neq 0$.

(h) $\mathrm{null}(A) = \{\mathbf{0}\}$.

(i) $\mathrm{nullity}(A) = 0$.

(j) $\mathrm{rank}(A) = n$.

(k) $\mathrm{col}(A) = \mathbb{R}^n$.

(l) $\mathrm{row}(A) = \mathbb{R}^n$.

(m) The columns of A are linearly independent (or span $\mathbb{R}^n$, or are a basis of $\mathbb{R}^n$).

(n) The rows of A are linearly independent (or span $\mathbb{R}^n$, or are a basis of $\mathbb{R}^n$).

(o) A does not have 0 as an eigenvalue.

Inner product spaces

We now define the notion of an inner product $\langle v, w \rangle$ on a vector space V.

An inner product is an additional layer of structure added to the vector space operations defined on V. As with those operations, we define inner products axiomatically.

The dot product operation defined on $\mathbb{R}^2$ and $\mathbb{R}^3$ serves as the basic model of an inner product; our axioms simply generalize prominent and useful properties of this particular inner product.

The main virtues of an inner product are:

1. it allows us to define notions of orthogonality, distance and angle on V;
2. it allows us to construct orthonormal bases of V, which are computationally very easy to work with.

Definition of inner product

Definition 1.1

Let V be a vector space. An **inner product** on V is an operation

$$\begin{aligned} \langle\ ,\rangle \colon V \times V &\to \mathbb{R} \\ (\mathbf{v}_1, \mathbf{v}_2) &\mapsto \langle \mathbf{v}_1, \mathbf{v}_2 \rangle \end{aligned}$$

satisfying the following axions:

$$\langle \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{w}, \mathbf{v} \rangle \qquad \text{(Symmetry)}$$

$$\langle c\mathbf{u} + d\mathbf{v}, \mathbf{w} \rangle = c\langle \mathbf{u}, \mathbf{w} \rangle + d\langle \mathbf{v}, \mathbf{w} \rangle \qquad \text{(Linearity in first variable)}$$

$$\langle \mathbf{v}, \mathbf{v} \rangle \geq 0 \text{ and } \langle \mathbf{v}, \mathbf{v} \rangle = 0 \text{ iff } \mathbf{v} = \mathbf{0} \qquad \text{(Positivity)}$$

A vector space V along with a choice of inner product $\langle\ ,\rangle$ is called an **inner product space**.

Example: the dot product on $\mathbb{R}^n$

Definition 1.2

Given $\mathbf{v} = (v_1, \ldots, v_n), \mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{R}^n$, we define the **dot product** as

$$\mathbf{v} \cdot \mathbf{w} = v_1 w_1 + v_2 w_2 + \cdots + v_n w_n.$$

It is easy to see that the dot product satisfies the axioms of an inner product on $\mathbb{R}^n$

In fact, if we identify n-tuples with column vectors (or row vectors), then we can express the dot product as a certain matrix multiplication, in which case the inner product axioms follow simply from properties of matrix multiplication!

Columns: think of $\mathbf{v}$ and $\mathbf{w}$ as $n \times 1$ column vectors. Then

$$\mathbf{v} \cdot \mathbf{w} = \mathbf{v}^T \mathbf{w}.$$

Rows: think of $\mathbf{v}$ and $\mathbf{w}$ as $1 \times n$ row vectors. Then

$$\mathbf{v} \cdot \mathbf{w} = \mathbf{v} \mathbf{w}^T$$

Dot product method of matrix multiplication

The last observations also give us yet another way of looking at matrix multiplication!

Take $A = [a_{ij}]_{m \times n}$ and $B = [b_{ij}]_{n \times r}$. Think of $A = \begin{bmatrix} -\mathbf{a}_1- \\ \vdots \\ -\mathbf{a}_m- \end{bmatrix}$ as a collection of m row vectors in $\mathbb{R}^n$, and $B = \begin{bmatrix} | & & | \\ \mathbf{b}_1 & \cdots & \mathbf{b}_r \\ | & & | \end{bmatrix}$ as a collection of r column vectors in $\mathbb{R}^n$.

Set $AB = C = [c_{ij}]_{m \times r}$. It follows directly from the original definition of matrix multiplication that

$$c_{ij} = \mathbf{a}_i \cdot \mathbf{b}_j.$$

That is, the ij-th entry of AB is simply the dot product of the i-th row of A and the j-th column of B!

Inner products on $\mathbb{R}^n$

Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots y_n)$ throughout. We consider $\mathbf{x}$ and $\mathbf{y}$ as columns by default.

Example 1. The dot product $\langle \mathbf{x}, \mathbf{y} \rangle := x_1 y_1 + x_2 y_2 + \cdots x_n y_n$ is an inner product on $\mathbb{R}^n$.

Example 2. For any choice of positive constants $c_1, c_2, \ldots c_n > 0$, the weighted dot product $\langle \mathbf{x}, \mathbf{y} \rangle := c_1 x_1 y_1 + c_2 x_2 y_2 + \cdots + c_n x_n y_n$ is an inner product on $\mathbb{R}^n$.

Example 3. (Why we need $c_i > 0$). The operation $\langle \mathbf{x}, \mathbf{y} \rangle = 2x_1 y_1 + (-1)x_2 y_2$ is NOT an inner product on $\mathbb{R}^2$ as $\langle (1, \sqrt{2}), (1, \sqrt{2}) \rangle = 2 - 2 = 0$, in violation of positivity.

Example 4. Looking forward a bit, it turns out that Examples 1 and 2 are cases of the following more general construction.
Let A be any symmetric $n \times n$ matrix, all of whose eigenvalues are positive.
Then the operation

$$\langle \mathbf{x}, \mathbf{y} \rangle := \mathbf{x}^T A \mathbf{y}$$

defines an inner product on $\mathbb{R}^n$.
Example 1 is the case where $A = I$.

Example 2 is the case where $A = \begin{bmatrix} c_1 & 0 & 0 & \ldots \\ 0 & c_2 & 0 & \ldots \\ \vdots & & & \\ 0 & 0 & \ldots & c_n \end{bmatrix}$

Inner products on P_n

Throughout we let $p(x) = a_n x^n + \cdots + a_1 x + a_0$ and $q(x) = b_n x^n + \cdots + b_1 x + b_0$.

Example 1. The operation $\langle p(x), q(x) \rangle := a_0 b_0 + a_1 b_1 + \cdots + a_n b_n$ defines an inner product on P_n. (This is just the dot product in disguise!)

Example 2. Fix any distinct constants $c_0, c_1, \ldots, c_n$. Then the operation $\langle p(x), q(x) \rangle = p(c_0)q(c_0) + p(c_1)q(c_1) + \cdots + p(c_n)q(c_n)$ defines an inner product, called an evaluation inner product.

Proof.

It is fairly clear that the evaluation product is symmetric and linear in each variable.
Consider positivity. We have
$\langle p(x), p(x) \rangle := p(c_0)^2 + p(c_1)^2 + \cdots + p(c_n)^2 \geq 0$, since each term is a square. Furthermore we see this sum is equal to 0 iff $p(c_i) = 0$ for all i. But this is the case iff $p(x) = \mathbf{0}$ is the zero polynomial, as no other polynomial in P_n can have $n+1$ distinct roots! $\square$

Standard inner product on M_{mn}

Given $A, B \in M_{mn}$, we define $\langle A, B \rangle = \mathrm{tr}(A^T B)$. Recall: the trace $\mathrm{tr}(C)$ of a matrix is the sum of its diagonal entries.
It is an interesting exercise to show the operation thus defined does indeed satisfy three axioms.

(i) The fact that $\langle A, B \rangle = \langle B, A \rangle$ follows from the fact that $\mathrm{tr}(A^T B) = \mathrm{tr}(B^T A)$. Can you prove the latter? Hint: what is the relation between $A^T B$ and $B^T A$?

(ii) Bilinearity follows easily from three different distributive properties: (a) for matrix multiplication, (b) for taking transposes, and (c) for taking the trace.

(iii) Positivity is the most challenging. The most direct way of proving that this property holds is to let $A = [a_{ij}]$ and actually compute a formula for $\mathrm{tr}(A^T A)$ in terms of the a_{ij}. I leave it to you.

Standard inner product on function spaces

Let $V = C([a,b])$ where $[a,b]$ is some fixed interval.
The standard inner product on $C([a,b])$ is defined via an integral:

$$\langle f(x), g(x)\rangle := \int_a^b f(x)g(x)\,dx.$$

(Note that continuity of f and g ensures this integral exists and is finite!)

Proof.

Symmetry: $\langle f, g\rangle = \int_a^b fg\,dx = \int_a^b gf\,dx = \langle g, f\rangle$
Linearity: $\langle cf + dg, h\rangle = \int_a^b (cf(x) + dg(x))h(x)\,dx =$
$c\int_a^b f(x)h(x)\,dx + d\int_a^b g(x)h(x)\,dx = c\langle f, h\rangle + d\langle g, h\rangle$
Positivity: we have $\langle f, f\rangle = \int_a^b f^2(x)\,dx$.
We have $f^2(x) \geq 0$ for all x; i.e., f^2 is nonnegative. It follows from some basic calculus that the integral of f^2 is always nonnegative. Furthermore, since f^2 is also continuous the integral is 0 iff $f^2 = 0$ iff $f = 0$. This proves positivity. $\square$

Further properties of inner products

The following properties follow formally from the defining axioms of an inner product space.

$$\langle \mathbf{u}, c\mathbf{v} + d\mathbf{w} \rangle = c\langle \mathbf{u}, \mathbf{v} \rangle + d\langle \mathbf{u}, \mathbf{w} \rangle \qquad \text{(Linearity in second variable)}$$
$$\langle \mathbf{0}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{0} \rangle = 0$$

The first property follows easily from linearity in the first variable and symmetry. Note: the fact that the inner product is linear in both variables is an important property that we call bilinearity.

To prove the second property it is enough by symmetry to prove $\langle \mathbf{0}, \mathbf{v} \rangle = 0$. (Note the two different types of zero here!)
We have

$$\begin{aligned} \langle \mathbf{0}, \mathbf{v} \rangle &= \langle 0 \cdot \mathbf{0}, \mathbf{v} \rangle && \text{(since } 0 \cdot \mathbf{0} = \mathbf{0}\text{)} \\ &= 0\langle \mathbf{0}, \mathbf{v} \rangle && \text{(linearity in first variable)} \\ &= 0 \end{aligned}$$

Orthogonality, norm, distance, angle

Given an inner product space $(V, \langle\ ,\ \rangle)$ we define the following notions.
Orthogonality: vectors $\mathbf{v}$ and $\mathbf{w}$ are **orthogonal** if $\langle \mathbf{v}, \mathbf{w} \rangle = 0$.
Norm: the **norm** (or **length**) of a vector $\mathbf{v}$ is defined as

$$\|\mathbf{v}\| := \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}.$$

A **unit vector** is a vector $\mathbf{v}$ with $\|\mathbf{v}\| = 1$. Given any vector $\mathbf{v}$, one can show that $\mathbf{u} = (\frac{1}{\|\mathbf{v}\|})\mathbf{v}$ (or $\frac{\mathbf{v}}{\|\mathbf{v}\|}$ by slight abuse of notation) is a unit vector.
Distance: the **distance** between two vectors $\mathbf{v}$ and $\mathbf{w}$ is defined as

$$d(\mathbf{v}, \mathbf{w}) = \|\mathbf{v} - \mathbf{w}\|.$$

Angle: the **angle** between two vectors $\mathbf{v}$ and $\mathbf{w}$ is defined as the unique $0 \leq \theta \leq \pi$ satisfying

$$\cos(\theta) = \frac{\langle \mathbf{v}, \mathbf{w} \rangle}{\|\mathbf{v}\| \, \|\mathbf{w}\|}.$$

Of course for this to make sense we better have

$$|\langle \mathbf{v}, \mathbf{w} \rangle| \leq \|\mathbf{v}\| \, \|\mathbf{w}\|$$

This is the content of the Cauchy-Schwarz inequality!

Cauchy-Schwarz Inequality

Theorem 1.1 (Cauchy-Schwarz inequality)

Let $(V, \langle\ ,\rangle)$ be an inner product space. Then for all $\mathbf{v}, \mathbf{w} \in V$

$$|\langle \mathbf{v}, \mathbf{w}\rangle| \leq \|\mathbf{v}\| \, \|\mathbf{w}\| \, .$$

Furthermore, we have an actual equality above iff $\mathbf{v} = c\mathbf{w}$ for some $c \in \mathbb{R}$.

Proof.

Fix any two vectors $\mathbf{v}$ and $\mathbf{w}$. For any $t \in \mathbb{R}$ we have by positivity

$$0 \leq \langle t\mathbf{v} - \mathbf{w}, t\mathbf{v} - \mathbf{w}\rangle = \langle \mathbf{v}, \mathbf{v}\rangle t^2 - 2\langle \mathbf{v}, \mathbf{w}\rangle t + \langle \mathbf{w}, \mathbf{w}\rangle = at^2 - 2bt + c = f(t),$$

where $a = \langle \mathbf{v}, \mathbf{v}\rangle = \|v\|^2$, $b = \langle \mathbf{v}, \mathbf{w}\rangle$ and $c = \langle \mathbf{w}, \mathbf{w}\rangle = \|w\|^2$.

The inequality $f(t) \geq 0$ tells us that the quadratic polynomial $f(t)$ has at most one root. This means its discriminant $4b^2 - 4ac \leq 0$, since otherwise there would be two roots.

Subbing back in for a, b, c and rearranging yields

$$(\langle \mathbf{v}, \mathbf{w}\rangle)^2 \leq \|\mathbf{v}\|^2 \, \|\mathbf{w}\|^2 \, .$$

Taking square-roots yields the desired inequality.
The same reasoning shows that the Cauchy-Schwarz inequality is an actual equality iff $f(t) = 0$ for some t iff $0 = \langle t\mathbf{v} - \mathbf{w}, t\mathbf{v} - \mathbf{w}\rangle$ iff $\mathbf{v} = t\mathbf{w}$ for some t (by positivity). $\square$

Triangle Inequalities

The following so-called triangle inequalities are now just formal consequences of Cauchy-Schwarz.

Theorem 1.2 (Triangle Inequalities)

Let $(V, \langle\ ,\rangle)$ be any inner product space. Then

1. $\|\mathbf{v} + \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|$
2. $d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{u}) + d(\mathbf{u}, \mathbf{w})$

Choosing your inner product

Why, given a fixed vector space V, would we prefer one inner product definition to another?

One way of understanding a particular choice of inner product is to ask what its corresponding notion of distance measures.

Example. Take P_n with the evaluation inner product at inputs $x = c_0, c_1, \dots, c_n$. Given two polynomials $p(x), q(x)$, the distance between them with respect to this inner product is

$$\|p(x) - q(x)\| = \sqrt{(p(c_0) - q(c_0))^2 + (p(c_1) - q(c_1))^2 + \cdots + (p(c_n) - q(c_n))^2}.$$

So in this inner product space the "distance" between two polynomials is a measure of how different their values are at the inputs $x = c_0, c_1, \dots, c_n$. This inner product may be useful if you are particularly interested in how a polynomial behaves at this finite list of inputs.

Example. Take $C[a, b]$ with the standard inner product $\langle f, g \rangle = \int_a^b f(x)g(x)\, dx$. Here the distance between two functions is defined as $\|f - g\| = \sqrt{\int_a^b (f(x) - g(x))^2\, dx}$. In particular, a function f is "close" to the zero function (i.e. "is small") if the *integral* of f^2 is small. This notion is useful in settings where integrals of functions represent quantities we are interested in (e.g. in probability theory, thermodynamics, wave and quantum mechanics).

Orthogonal sets

Definition 2.1

Let $(V, \langle\ ,\rangle)$ be an inner product space.
A set $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ of *nonzero vectors* is **orthogonal** if $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0$ for all $i \neq j$: i.e., the elements are pairwise orthogonal.
An orthogonal set that further satisfies $\|\mathbf{v}_i\| = 1$ for all i is called **orthonormal**.

Theorem 2.1

Let $(V, \langle\ ,\rangle)$ be an inner product space. If $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ is orthogonal, then S is linearly independent.

Proof.

$$\begin{aligned}
a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_r\mathbf{v}_r = \mathbf{0} \quad &\Rightarrow \quad \langle a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_r\mathbf{v}_r, \mathbf{v}_i \rangle = \langle \mathbf{0}, \mathbf{v}_i \rangle \\
&\Rightarrow \quad a_1\langle \mathbf{v}_1, \mathbf{v}_i \rangle + a_2\langle \mathbf{v}_2, \mathbf{v}_i \rangle + \cdots + a_r\langle \mathbf{v}_r, \mathbf{v}_i \rangle = 0 \\
&\Rightarrow \quad a_i\langle \mathbf{v}_i, \mathbf{v}_i \rangle = 0 \ \ (\text{since } \langle \mathbf{v}_j, \mathbf{v}_i \rangle = 0 \text{ for } j \neq i) \\
&\Rightarrow \quad a_i = 0 \ (\text{since } \langle \mathbf{v}_i, \mathbf{v}_i \rangle \neq 0)
\end{aligned}$$

We have shown that if $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_r\mathbf{v}_r = \mathbf{0}$, then $a_i = 0$ for all i, proving that S is linearly independent. $\square$

Example

Let $V = C([0,2\pi])$ with standard inner product $\langle f, g\rangle = \int_0^{2\pi} f(x)g(x)\,dx$.
Let

$$S = \{\cos(x), \sin(x), \cos(2x), \sin(2x), \dots\} = \{\cos(nx) \colon n \in \mathbb{Z}_{>0}\} \cup \{\sin(mx) \colon m \in \mathbb{Z}_{>0}\}$$

Then S is orthogonal, hence linearly independent.

Proof.

Using some trig identities, one can show the following:

$$\langle \cos(nx), \cos(mx)\rangle = \int_0^{2\pi} \cos(nx)\cos(mx)\,dx = \begin{cases} 0 & \text{if } n \neq m \\ \pi & \text{if } n = m \end{cases}$$

$$\langle \sin(nx), \sin(mx)\rangle = \int_0^{2\pi} \sin(nx)\sin(mx)\,dx = \begin{cases} 0 & \text{if } n \neq m \\ \pi & \text{if } n = m \end{cases}$$

$$\langle \cos(nx), \sin(mx)\rangle = \int_0^{2\pi} \cos(nx)\sin(mx)\,dx = 0 \text{ for any } n, m$$

$\square$

Orthogonality holds more generally if we replace the interval $[0, 2\pi]$ with any interval of length L, and replace S with

$$\left\{\cos\left(\frac{2\pi x}{L}\right), \sin\left(\frac{2\pi x}{L}\right), \cos\left(2\cdot\frac{2\pi x}{L}\right), \sin\left(2\cdot\frac{2\pi x}{L}\right), \dots\right\}.$$

Orthogonal basis

Definition 2.2

Let $(V, \langle\ ,\rangle)$ be an inner product space, $\dim V = n$.
An **orthogonal basis** is a basis $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ that is an orthogonal set; an orthogonal basis B is **orthonormal** if B is orthonormal.

Theorem 2.2 (Existence/extension of orthonormal bases)

Let $(V, \langle\ ,\rangle)$ be a finite-dimensional inner product vector space.
Then (1) V has an ortho(gonal/normal) basis. (Proof is the Gram-Schmidt process. See two slides on.)
Furthermore, (2) any ortho(gonal/normal) set can be extended to an ortho(gonal/normal) basis of V.

Theorem 2.3 (Calculating with ortho(gonal/normal) bases)

Let $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be an orthogonal basis for V.
Given any $\mathbf{v} \in V$ we have $\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{v}_n$ where $a_i = \frac{\langle \mathbf{v}, \mathbf{v}_i \rangle}{\langle \mathbf{v}_i, \mathbf{v}_i \rangle}$.
Equivalently,

$$[\mathbf{v}]_B = \begin{bmatrix} \frac{\langle \mathbf{v}, \mathbf{v}_1 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} \\ \frac{\langle \mathbf{v}, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_2, \mathbf{v}_2 \rangle} \\ \vdots \\ \frac{\langle \mathbf{v}, \mathbf{v}_n \rangle}{\langle \mathbf{v}_n, \mathbf{v}_n \rangle} \end{bmatrix}$$

If B is orthonormal then these formulas simplify to

$$a_i = \langle \mathbf{v}, \mathbf{v}_i \rangle \text{ for all } i.$$

Example

Let $V = \mathbb{R}^2$ with the standard inner produce (aka the dot product).
(a) Verify that $B' = \{\mathbf{v}_1 = (\sqrt{3}/2, 1/2), \mathbf{v}_2 = (-1/2, \sqrt{3}/2)\}$ is an orthonormal basis.
(b) Compute $[\mathbf{v}]_{B'}$ for $\mathbf{v} = (4, 2)$.
(c) Compute $\underset{B \to B'}{P}$, where B is the standard basis.

Solution:
(a) Easily seen to be true.
(b) Since B' is orthonormal, $\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2$ where $a_1 = \mathbf{v} \cdot \mathbf{v}_1 = 2\sqrt{3} + 1$ and $a_2 = \mathbf{v} \cdot \mathbf{v}_2 = \sqrt{3} - 2$. Thus $[\mathbf{v}]_{B'} = \begin{bmatrix} 2\sqrt{3}+1 \\ \sqrt{3}-2 \end{bmatrix}$
(c) As we have seen before, $\underset{B' \to B}{P} = \begin{bmatrix} \sqrt{3}/2 & -1/2 \\ 1/2 & \sqrt{3}/2 \end{bmatrix}$ (put elements of B' in as columns). Hence $\underset{B \to B'}{P} = (\underset{B' \to B}{P})^{-1} = \begin{bmatrix} \sqrt{3}/2 & 1/2 \\ -1/2 & \sqrt{3}/2 \end{bmatrix}$
Useful fact. If the columns of an $n \times n$ matrix P are orthonormal, then P is invertible, and $\boxed{P^{-1} = P^T}$.

Proof. Let $\mathbf{p}_j$ be the j-th column of P. By the dot product method of matrix multiplication, we have $P^TP = [\mathbf{p}_i \cdot \mathbf{p}_j] = I_n$, since the $\mathbf{p}_i$ are orthonormal. This proves $P^T = P^{-1}$.

Gram-Schmidt Process

The proof that every finite-dimensional vector space has an orthogonal basis is actually a procedure, called the Gram-Schmidt process, for converting an arbitrary basis for an inner product space to an orthogonal basis.

Theorem 2.4 (Gram-Schmidt process)

Let $(V, \langle\ ,\ \rangle)$ be an inner product space, and let $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ be a basis for V. We can convert B into an orthogonal basis $B' = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n\}$ using the following recursive procedure:

1. Set $\mathbf{w}_1 = \mathbf{v}_1$.
2. For $2 \leq r \leq n$ replace $\mathbf{v}_r$ with

$$\mathbf{w}_r := \mathbf{v}_r - \frac{\langle \mathbf{v}_r, \mathbf{w}_{r-1} \rangle}{\langle \mathbf{w}_{r-1}, \mathbf{w}_{r-1} \rangle}\mathbf{w}_{r-1} - \frac{\langle \mathbf{v}_r, \mathbf{w}_{r-2} \rangle}{\langle \mathbf{w}_{r-2}, \mathbf{w}_{r-2} \rangle}\mathbf{w}_{r-2} - \cdots - \frac{\langle \mathbf{v}_r, \mathbf{w}_1 \rangle}{\langle \mathbf{w}_1, \mathbf{w}_1 \rangle}\mathbf{w}_1$$

Lastly, to further transform to an orthonormal basis, replace each $\mathbf{w}_i$ with $\mathbf{u}_i = \dfrac{\mathbf{w}_i}{\|\mathbf{w}_i\|}$.

Orthogonal complement

Definition 2.3

. Let $(V, \langle\ ,\rangle)$ be an inner product vector space, and let $W \subseteq V$ be a finite-dimensional subspace. The **orthogonal complement of** W is defined as

$$W^\perp := \{\mathbf{v} \in V \colon \langle \mathbf{v}, \mathbf{w}\rangle = 0 \text{ for all } \mathbf{w} \in W\}.$$

In English: $W^\perp$ is the set of vectors that are orthogonal to *all* vectors in W.

Theorem 2.5 (Orthogonal complement theorem)

Let $(V, \langle\ ,\rangle)$ be an inner product vector space, and let $W \subseteq V$ be a subspace.

(a) $W^\perp$ is a subspace of V.

(b) $W \cap W^\perp = \{\mathbf{0}\}$

Example. Let $V = \mathbb{R}^3$ equipped with the dot product, and let $W = \text{span}\{(1,1,1)\} \subset \mathbb{R}^3$. This is the line defined by the vector $(1,1,1)$. Then $W^\perp$ is the set of vectors orthogonal to $(1,1,1)$: i.e., the plane perpendicular to $(1,1,1)$.

Geometry of fundamental spaces

The notion of orthogonal complement gives us a new way of understanding the relationship between the various fundamental spaces of a matrix.

Theorem 2.6

Let A be $m \times n$, and consider $\mathbb{R}^n$ and $\mathbb{R}^m$ as inner product spaces with respect to the dot product. Then:

(i) $\text{null}(A) = (\text{row}(A))^{\perp}$, and thus $\text{row}(A) = (\text{null}(A))^{\perp}$.

(ii) $\text{null}(A^T) = (\text{col}(A))^{\perp}$, and thus $\text{col}(A) = \left(\text{null}(A^T)\right)^{\perp}$.

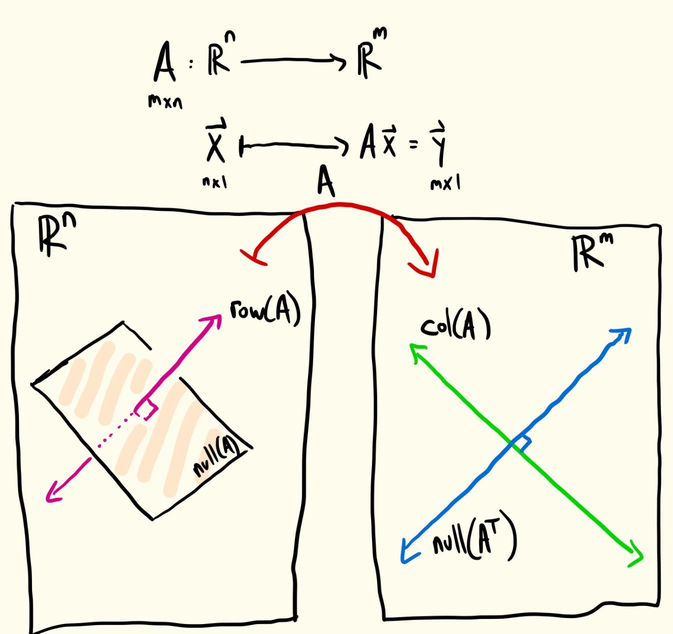
Proof.

(i) Using the dot product method of matrix multiplication, we see that a vector $\mathbf{v} \in \text{null}(A)$ if and only if $\mathbf{v} \cdot \mathbf{r}_i = 0$ for each row $\mathbf{r}_i$ of A. Since the $\mathbf{r}_i$ span $\text{row}(A)$, the linear properties of the dot product imply that $\mathbf{v} \cdot \mathbf{r}_i = 0$ for each row $\mathbf{r}_i$ of A if and only if $\mathbf{v} \cdot \mathbf{w} = 0$ for all $\mathbf{w} \in \text{row}(A)$ if and only if $\mathbf{v} \in \text{row}(A)^{\perp}$.

(ii) This follows from (i) and the fact that $\text{col}(A) = \text{row}(A^T)$.

□

Visualizing the rank-nullity theorem



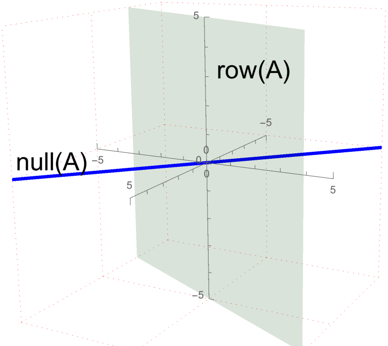
Example

Understanding the orthogonal relationship between null(A) and row(A) allows us in many cases to quickly determine/visualize the one from the other.

Consider the example $A = \begin{bmatrix} 1 & -1 & 1 \\ 1 & -1 & -1 \end{bmatrix}$. Looking at the columns, we see easily that $\operatorname{rank}(A) = 2$, which implies that $\operatorname{nullity}(A) = 3 - 2 = 1$. Since $(1, -1, 0)$ is an element of null(A) and $\dim(\operatorname{null}(A)) = 1$, we must have $\operatorname{null}(A) = \operatorname{span}\{(1, -1, 0)\}$, a line.

By orthogonality, we conclude that

$$\operatorname{row}(A) = \operatorname{null}(A)^{\perp} = (\text{plane perpendicular to } (1, -1, 0)).$$



Orthogonal Projection

Theorem 2.7 (Orthogonal projection theorem)

Let $(V, \langle\ ,\rangle)$ be an inner product space, and let $W \subseteq V$ be a finite-dimensional subspace.

(a) (Orthogonal decomposition). For all $\mathbf{v} \in V$ there is a unique choice of vectors $\mathbf{w} \in W$ and $\mathbf{w}^\perp \in W^\perp$ such that $\mathbf{v} = \mathbf{w} + \mathbf{w}^\perp$.

We call this vector expression an **orthogonal decomposition** of $\mathbf{v}$, and denote $\mathbf{w} = \operatorname{proj}_W(\mathbf{v})$ and $\mathbf{w}^\perp = \operatorname{proj}_{W^\perp}(\mathbf{v})$, the **orthogonal projections** of $\mathbf{v}$ onto W and $W^\perp$, respectively.

(b) The orthogonal projection $\mathbf{w} = \operatorname{proj}_W(\mathbf{v})$ is the element of W closest to $\mathbf{v}$. This means $\|\mathbf{v} - \operatorname{proj}_W(\mathbf{v})\| \leq \|\mathbf{v} - \mathbf{w}'\|$ for any other $\mathbf{w}' \in W$. We thus define the distance from $\mathbf{v}$ to W as $d(\mathbf{v}, W) = \|\mathbf{v} - \operatorname{proj}_W(\mathbf{v})\| = \left\|\mathbf{w}^\perp\right\|$.

(c) (Orthogonal projection formula). Pick an *orthogonal* basis

$B = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r\}$ of W. Then $\operatorname{proj}_W(\mathbf{v}) = \displaystyle\sum_{i=1}^{r} \frac{\langle \mathbf{v}, \mathbf{v}_i\rangle}{\langle \mathbf{v}_i, \mathbf{v}_i\rangle}\mathbf{v}_i$.

Comment

An important consequence of this theorem is that $\operatorname{proj}_W(\mathbf{v})$ can be uniquely characterized by two distinct properties:

(i) it is the unique element $\mathbf{w}$ of W closest to $\mathbf{v}$

(ii) it is the unique element $\mathbf{w}$ of W such that $\mathbf{v} - \mathbf{w}$ is orthogonal to W.

Proof of orthogonal projection theorem

Pick an *orthogonal* basis $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ of W and set $\mathbf{w} = \sum_{i=1}^{r} \frac{\langle \mathbf{v}, \mathbf{v}_i \rangle}{\langle \mathbf{v}_i, \mathbf{v}_i \rangle} \mathbf{v}_i$. This is clearly an element of W. Next we set $\mathbf{w}^{\perp} = \mathbf{v} - \mathbf{w} = \mathbf{v} - \sum_{i=1}^{r} \frac{\langle \mathbf{v}, \mathbf{v}_i \rangle}{\langle \mathbf{v}_i, \mathbf{v}_i \rangle} \mathbf{v}_i$.

To complete the proof, we must show the following: (A) $\mathbf{w}^{\perp} \in W^{\perp}$, (B) this choice of $\mathbf{w}$ and $\mathbf{w}^{\perp}$ is unique, and (C) $\mathbf{w}$ is the closest element of W to $\mathbf{v}$.

(A). For all i we have

$$\begin{aligned}
\langle \mathbf{w}^{\perp}, \mathbf{v}_i \rangle &= \langle \mathbf{v} - \sum_{i=1}^{r} \frac{\langle \mathbf{v}, \mathbf{v}_i \rangle}{\langle \mathbf{v}_i, \mathbf{v}_i \rangle} \mathbf{v}_i, \mathbf{v}_i \rangle \\
&= \langle \mathbf{v}, \mathbf{v}_i \rangle - \langle \sum_{i=1}^{r} \frac{\langle \mathbf{v}, \mathbf{v}_i \rangle}{\langle \mathbf{v}_i, \mathbf{v}_i \rangle} \mathbf{v}_i, \mathbf{v}_i \rangle \quad \text{(distr.)} \\
&= \langle \mathbf{v}, \mathbf{v}_i \rangle - \frac{\langle \mathbf{v}, \mathbf{v}_i \rangle}{\langle \mathbf{v}_i, \mathbf{v}_i \rangle} \langle \mathbf{v}_i, \mathbf{v}_i \rangle \quad \text{(by orthogonality)} \\
&= 0
\end{aligned}$$

(B)+(C). Recall: $\mathbf{w}$ satisfies $\mathbf{v} = \mathbf{w} + \mathbf{w}^{\perp}$, where $\mathbf{w}^{\perp} \in W^{\perp}$. Now take any other $\mathbf{w}' \in W$. Then

$$\begin{aligned}
\left\| \mathbf{v} - \mathbf{w}' \right\|^2 &= \left\| \mathbf{w}^{\perp} + (\mathbf{w} - \mathbf{w}') \right\|^2 = \left\| \mathbf{w}^{\perp} \right\|^2 + \left\| \mathbf{w} - \mathbf{w}' \right\|^2 \quad \text{(Pythag. theorem)} \\
&\geq \left\| \mathbf{w}^{\perp} \right\|^2 = \left\| \mathbf{v} - \mathbf{w} \right\|^2 .
\end{aligned}$$

Taking square-roots now proves the desired inequality. Furthermore, we have *equality* iff the last inequality is an equality iff $\|\mathbf{w}''\| = \|\mathbf{w} - \mathbf{w}'\| = 0$ iff $\mathbf{w} = \mathbf{w}'$. This proves our choice of $\mathbf{w}$ is the *unique* element of W minimizing the distance to $\mathbf{v}$!

Corollary 2.7.1

Let $(V, \langle\ ,\ \rangle)$ be an inner product space, and let $W \subseteq V$ be a finite-dimensional subspace. Then $(W^\perp)^\perp = W$.

Proof.

Clearly $W \subseteq (W^\perp)^\perp$.

For the other direction, take $\mathbf{v} \in (W^\perp)^\perp$. Using the orthogonal projection theorem, we can write $\mathbf{v} = \mathbf{w} + \mathbf{w}^\perp$ with $\mathbf{w} \in W$ and $\mathbf{w}^\perp \in W^\perp$. We will show $\mathbf{w}^\perp = \mathbf{0}$.

Since $\mathbf{v} \in (W^\perp)^\perp$ we have $\langle \mathbf{v}, \mathbf{w}^\perp \rangle = 0$. Then we have

$$\begin{aligned}
0 &= \langle \mathbf{v}, \mathbf{w}^\perp \rangle \\
&= \langle \mathbf{w} + \mathbf{w}^\perp, \mathbf{w}^\perp \rangle \\
&= \langle \mathbf{w}, \mathbf{w}^\perp \rangle + \langle \mathbf{w}^\perp, \mathbf{w}^\perp \rangle && \text{(since } W \perp W^\perp\text{)} \\
&= 0 + \langle \mathbf{w}^\perp, \mathbf{w}^\perp \rangle
\end{aligned}$$

Thus $\langle \mathbf{w}^\perp, \mathbf{w}^\perp \rangle = 0$.

It follows that $\mathbf{w}^\perp = \mathbf{0}$, and hence $\mathbf{v} = \mathbf{w} + \mathbf{0} = \mathbf{w} \in W$. $\square$

Corollary 2.7.2

Let $(V, \langle\ ,\ \rangle)$ be an inner product space, and let $W \subseteq V$ be a finite-dimensional subspace.
Define $T\colon V \to V$ as $T(\mathbf{v}) = \mathrm{proj}_W(\mathbf{v})$. Then T is a linear transformation.
In other words, orthogonal projection onto W defines a linear transformation of V.

Proof.

We must show that $T(c\mathbf{v}_1 + d\mathbf{v}_2) = cT(\mathbf{v}_1) + dT(\mathbf{v}_2)$ for all $c, d \in \mathbb{R}$ and $\mathbf{v}_1, \mathbf{v}_2 \in V$. This is easily shown by picking an orthonormal basis $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ of W and using the formula from the orthogonal projection theorem. $\square$

Projection onto lines and planes in $\mathbb{R}^3$

Let's revisit orthogonal projection onto lines and planes in $\mathbb{R}^3$ passing through the origin. Here the relevant inner product is dot product.

Projection onto a line ℓ

Any line in $\mathbb{R}^3$ passing through the origin can be described as $\ell = \text{span}\{\mathbf{v}_0\}$, for some $\mathbf{v}_0 = (a, b, c) \neq 0$. Since this is an orthogonal basis of ℓ, by the orthogonal projection theorem we have, for any $\mathbf{v} = (x, y, z)$

$$\text{proj}_\ell(\mathbf{v}) = \frac{\mathbf{v} \cdot \mathbf{v}_0}{\mathbf{v}_0 \cdot \mathbf{v}_0}\mathbf{v}_0 = \frac{ax + by + cz}{a^2 + b^2 + c^2}(a, b, c) = \frac{1}{a^2 + b^2 + c^2}\begin{bmatrix} a^2 & ab & ac \\ ab & b^2 & bc \\ ac & bc & c^2 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

We have re-derived the matrix formula for orthogonal projection onto ℓ.

Projection onto lines and planes in $\mathbb{R}^3$

Let's revisit orthogonal projection onto lines and planes in $\mathbb{R}^3$ passing through the origin. Here the relevant inner product is dot product.

Projection onto a plane $\mathcal{P}$

Any plane in $\mathbb{R}^3$ passing through the origin can be described with the equation $\mathcal{P}\colon ax + by + cz = 0$ for some $\mathbf{n} = (a, b, c) \neq 0$. This says precisely that $\mathcal{P}$ is the orthogonal complement of the line $\ell = \operatorname{span}\{(a, b, c)\}$: i.e., $\mathcal{P} = \ell^\perp$.

From the orthogonal projection theorem, we know that

$$\mathbf{v} = \operatorname{proj}_\ell(\mathbf{v}) + \operatorname{proj}_{\ell^\perp}(\mathbf{v}) = \operatorname{proj}_\ell(\mathbf{v}) + \operatorname{proj}_{\mathcal{P}}(\mathbf{v}).$$

But then

$$\operatorname{proj}_{\mathcal{P}}(\mathbf{v}) = \mathbf{v} - \operatorname{proj}_\ell(\mathbf{v}) = I\,\mathbf{v} - \operatorname{proj}_\ell(\mathbf{v}) = (I - A)\mathbf{v},$$

where A is the matrix formula for $\operatorname{proj}_\ell(\mathbf{v})$ from the previous example. We conclude that the matrix defining $\operatorname{proj}_{\mathcal{P}}(\mathbf{v})$ is

$$I - \frac{1}{a^2 + b^2 + c^2}\begin{bmatrix} a^2 & ab & ac \\ ab & b^2 & bc \\ ac & bc & c^2 \end{bmatrix} = \frac{1}{a^2 + b^2 + c^2}\begin{bmatrix} b^2 + c^2 & -ab & -ac \\ -ab & a^2 + c^2 & -bc \\ -ac & -bc & a^2 + b^2 \end{bmatrix}$$

Example: sine/cosine series

Let $V = C[0, 2\pi]$ with inner product $\langle f, g\rangle = \int_0^{2\pi} f(x)g(x)\,dx$.
We have seen that the set

$$B = \{1, \cos(x), \sin(x), \cos(2x), \sin(2x), \ldots, \cos(nx), \sin(nx)\}$$

is orthogonal. Thus B is an orthogonal basis of $W = \text{span}(B)$, which we might describe as the space of **trigonometric polynomials of degree at most** n.

Given an arbitrary function $f(x) \in C[0, 2\pi]$, its orthogonal projection onto W is the function

$$\hat{f}(x) = a_0 + a_1\cos(x) + b_1\sin(x) + a_2\cos(2x) + b_2\sin(2x) + \cdots + a_n\cos(nx) + b_n\sin(nx),$$

where

$$a_0 = \frac{1}{2\pi}\int_0^{2\pi} f(x)\,dx,\ a_j = \frac{1}{\pi}\int_0^{2\pi} f(x)\cos(jx)\,dx,\ b_k = \frac{1}{\pi}\int_0^{2\pi} f(x)\sin(kx)\,dx.$$

The projection theorem tells us that $\hat{f}$ is the "best" trigonometric polynomial approximation of $f(x)$ (of degree at most n), in the sense that for any other sinusoidal $g \in W$, $\left\|f - \hat{f}\right\| \leq \|f - g\|$.

This means in turn

$$\int_0^{2\pi} (f - \hat{f})^2\,dx \leq \int_0^{2\pi} (f - g)^2\,dx.$$

Example: least-squares solution to $A\mathbf{x} = \mathbf{y}$

Often in applications we have an $m \times n$ matrix A and vector $\mathbf{y} \in \mathbb{R}^m$ for which the matrix equation

$$A\mathbf{x} = \mathbf{y}$$

has no solution. In terms of fundamental spaces, this means simply that $\mathbf{y} \notin \mathrm{col}(A)$. Set $W = \mathrm{col}(A)$.

In such situations we speak of a least-squares solution to the matrix equation. This is a vector $\hat{\mathbf{x}}$ such that $A\hat{\mathbf{x}} = \hat{\mathbf{y}}$, where $\hat{\mathbf{y}} = \mathrm{proj}_W(\mathbf{y})$. Here the inner product is taken to be the dot product.
Note: the equation $A\hat{\mathbf{x}} = \hat{\mathbf{y}}$ is guaranteed to have a solution since $\hat{\mathbf{y}} = \mathrm{proj}_W(\mathbf{y})$ lies in $\mathrm{col}(A)$.
The vector $\hat{\mathbf{x}}$ is called a least-square solutions because its image $\hat{\mathbf{y}}$ is the element of $\mathrm{col}(A)$ that is "closest" to $\mathbf{y}$ in terms of the dot product.

Writing $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ and $\hat{\mathbf{y}} = (y_1', y_2', \ldots, y_n')$, this means that $\hat{\mathbf{y}}$ minimizes the distance

$$\|\mathbf{y} - \hat{\mathbf{y}}\| = \sqrt{(y_1 - y_1')^2 + (y_2 - y_2')^2 + \cdots + (y_n - y_n')^2}.$$

Least-squares example (curve fitting)

Suppose we wish to find an equation of a line $y = mx + b$ that best fits (in the least-square's sense) the following (x, y) data points:
$P_1 = (-3, 1), P_2 = (1, 2), P_3 = (2, 3)$.
Then we seek m and b such that

$$\begin{aligned} 1 &= m(-3) + b \\ 2 &= m(1) + b \\ 3 &= m(2) + b, \end{aligned}$$

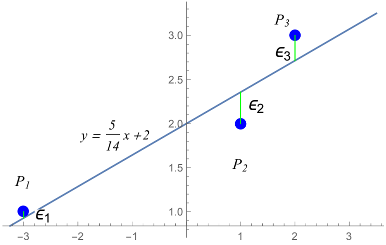
or equivalently, we wish to solve $\begin{bmatrix} -3 & 1 \\ 1 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} m \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$.

This equation has no solution as $\mathbf{y} = (1, 2, 3)$ does no lie in $W = \text{col}(A) = \text{span}(\{(-3, 1, 2), (1, 1, 1)\}$. So instead we compute $\hat{\mathbf{y}} = \text{proj}_W(\mathbf{y}) = (13/14, 33/14, 38/14)$. (This was not hard to compute as conveniently the given basis of W was already orthogonal!)

Finally we solve $A \begin{bmatrix} m \\ b \end{bmatrix} = \hat{\mathbf{y}}$, getting $m = 5/14$, $b = 28/14 = 2$. Thus $y = \frac{5}{14}x + 2$ is the line best fitting the data in the least-squares sense.

Least-squares example contd.

In what sense does $y = \frac{5}{14}x + 2$ "best" fit the data?



Let $\mathbf{y} = (1,2,3) = (y_1, y_2, y_3)$ be the given y-values of the points, and $\hat{\mathbf{y}} = (y_1', y_2', y_3')$ be the projection we computed before. In the graph the values ϵ_i denote the vertical difference $\epsilon_i = y_i - y_i'$ between the data points, and our fitting line.

The projection $\hat{\mathbf{y}}$ makes the error $\|\mathbf{y} - \hat{\mathbf{y}}\| = \sqrt{\epsilon_1^2 + \epsilon_2^2 + \epsilon_3^2}$ as small as possible. This means if I draw *any other line* and compute the corresponding differences ϵ_i' at the x-values -3, 1 and 2, then we have

$$\epsilon_1^2 + \epsilon_2^2 + \epsilon_3^2 \le (\epsilon_1')^2 + (\epsilon_2')^2 + (\epsilon_3')^2$$

Finding least squares solutions

As the last example illustrated, one method of finding a least-squares solution $\mathbf{x}$ to $A\mathbf{x} = \mathbf{y}$ is to first produce an orthogonal basis for $\text{col}(A)$, then compute $\hat{\mathbf{y}} = \text{proj}_{\text{col}(A)}(\mathbf{y})$, and then use GE to solve $A\mathbf{x} = \hat{\mathbf{y}}$.

Alternatively, it turns out (through a little trickery) that $\hat{\mathbf{y}} = A\mathbf{x}$, where $\mathbf{x}$ is a solution to the equation

$$\boxed{A^T A\mathbf{x} = A^T\mathbf{y}}.$$

This solves us the hassle of computing an orthogonal basis for $\text{col}(A)$; to find a least-squares solution $\mathbf{x}$ for $A\mathbf{x} = \mathbf{y}$, we simply use GE to solve the boxed equation. (Some more trickery shows a solution is guaranteed to exist!)

Example. In the previous example we were seeking a least-squares solution $\mathbf{x} = \begin{bmatrix} m \\ b \end{bmatrix}$ to $A\mathbf{x} = \mathbf{y}$, where $A = \begin{bmatrix} -3 & 1 \\ 1 & 1 \\ 2 & 1 \end{bmatrix}, \mathbf{y} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$.

The equation $A^T A\mathbf{x} = A^T\mathbf{y}$ is thus

$$\begin{bmatrix} 14 & 0 \\ 0 & 3 \end{bmatrix} \mathbf{x} = \begin{bmatrix} 5 \\ 6 \end{bmatrix}$$

As you can see, $\mathbf{x} = \begin{bmatrix} m \\ b \end{bmatrix} = \begin{bmatrix} 5/14 \\ 2 \end{bmatrix}$ is a least-squares solution, just as before