HKU MATH2101 Study Notes

Chiu Ka Long (Leo)*

Last Updated: 2024-12-14

Contents

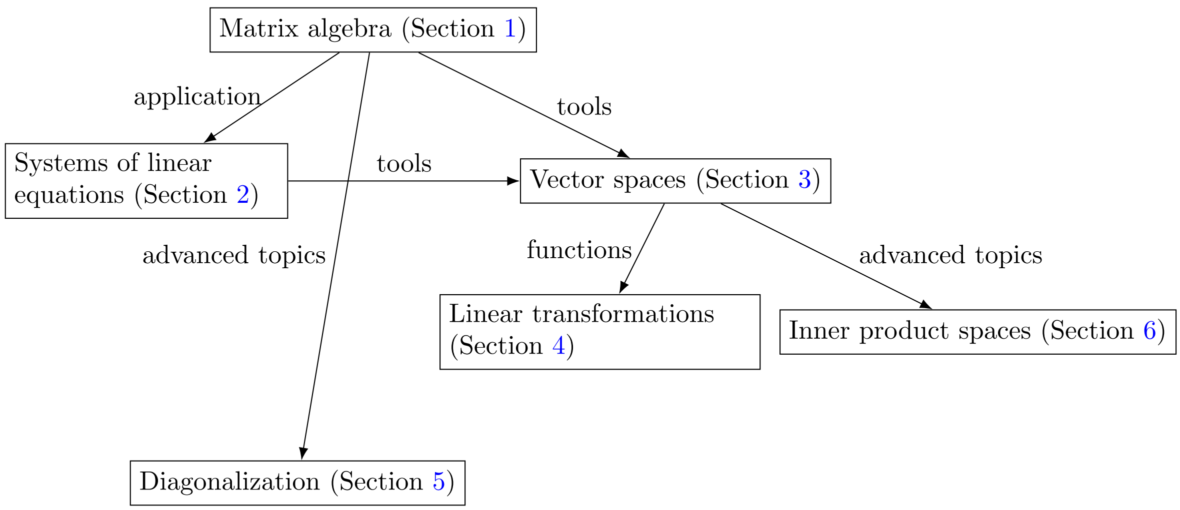
*email: leockl@connect.hku.hk; personal website: https://leochiukl.github.io

1 Matrix Algebra

1.0.1 *Linear algebra* is central to many areas of mathematics, and has also many applications in fields outside mathematics, e.g., engineering, economics, etc. It is related to *linear equations* and *linear transformations* (between *vector spaces*).

1.0.2 In linear algebra, a popular mathematical concept with wide applicability is *matrix*, which is essentially a rectangular array. So we will study it in Section 1. Nonetheless, from a mathematical point of view, the more important (but also more abstract) concepts in linear algebra are instead *vector spaces* and *linear transformations* (which are somehow related to matrices, as we will see).

1.0.3 Before studying matrices, we shall illustrate the stricture and the relationship between different topics in MATH2101:



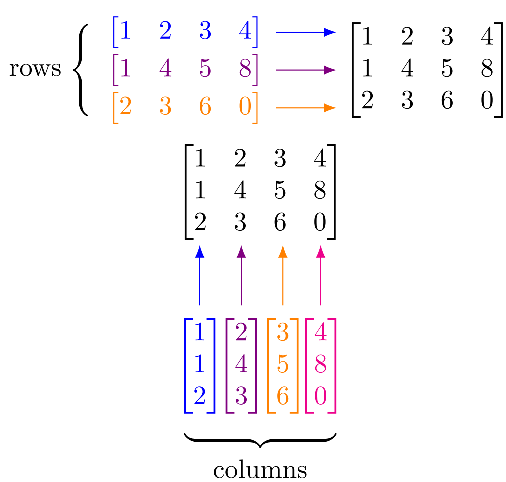
1.1 Introduction to Matrices

1.1.1 A **matrix** is a rectangular array of objects (called **entries**). In MATH2101, each entry can be assumed to be a real number (unless otherwise specified).

[Note: Unless otherwise specified, we shall use capital letters (A, B, etc.) to denote arbitrary matrices, and small letters (s, t, etc.) to denote arbitrary scalars (synonymous as real numbers in MATH2101).]

1.1.2 Some terminologies:

- A horizontal (vertical) unit of a matrix is called a **row** (**column**).



- A matrix with m rows and n columns is called an **$m \times n$ matrix**, and we call $m \times n$ the **size** of the matrix.

  [Note: Each row (column) of an $m \times n$ matrix can be viewed as a $1 \times n$ ($m \times 1$) matrix.]
- The **(i,j)-entry** of a matrix is the entry in its ith row and jth column. [Note: Sometimes we denote the (i,j)-entry of a matrix A by A_{ij}.]
- A **square matrix** is a matrix with the same number of rows and columns.
- A **submatrix** of a matrix M is a matrix whose rows and columns are both subsets of those of M, in the same relative order.
- The **main diagonal** of a matrix is the collection of all (i,j)-entries where $i=j$.
- A **triangular matrix** is a square matrix that is either *upper triangular* or *lower triangular*:
  - A square matrix is **upper triangular** if all entries below the main diagonal are 0. Example:

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{bmatrix}$$

  - A square matrix is **lower triangular** if all entries above the main diagonal are 0. Example:

$$\begin{bmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 4 & 5 & 6 \end{bmatrix}$$

- A **diagonal matrix** is a square matrix which is both upper and lower triangular, i.e., its off-diagonal entries (entries not in the main diagonal) are all 0. Example:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 6 \end{bmatrix}$$

- Two matrices A and B are **equal**, written as $A = B$, if:
  - they have the same size, and
  - their corresponding entries are equal, i.e., $a_{ij} = b_{ij}$ for any i and j, where a_{ij} (b_{ij}) denote the (i,j)-entry of A (B).

  [Note: For convenience, sometimes we write $A = [a_{ij}]$ to denote the (i,j)-entry of matrix A is a_{ij} (for any i and j). Also, unless otherwise specified, $a_{ij}, b_{ij}, c_{ij}, \ldots$ denote the (i,j) entry of matrices $A, B, C, \ldots$ respectively.]

1.2 Operations on Matrices

1.2.1 **Matrix addition** is defined *entrywise*, i.e., if $A = [a_{ij}]$ and $B = [b_{ij}]$, then

$$A + B = [a_{ij} + b_{ij}].$$

[Note: Matrix addition is well-defined only when the two matrices involved have the same size.] Examples:

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix} + \begin{bmatrix} 5 & 1 & 0 \\ 2 & 1 & 4 \end{bmatrix} = \begin{bmatrix} 1+5 & 2+1 & 3+0 \\ 2+2 & 3+1 & 4+4 \end{bmatrix},$$

and

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix} + \begin{bmatrix} 5 & 1 \\ 2 & 1 \end{bmatrix} \text{ is not well-defined!}$$

1.2.2 Matrix addition is both:

(a) *commutative*, i.e., $A + B = B + A$ for any matrices A and B of the same size, and

(b) *associative*, i.e., $A + (B + C) = (A + B) + C$ for any matrices A, B, and C of the same size.

Proof. It follows from the commutativity and associativity of the usual addition (of two real numbers). $\square$

1.2.3 Recall that for real numbers, subtraction is defined using the notion of *negative* (which is in turn originated from the concept of *additive inverse*). Here we adopt a similar approach for defining matrix subtraction.

First, we introduce several more terminologies:

- A **zero matrix** is a matrix where each entry is 0. The $m \times n$ zero matrix is denoted by $O_{m\times n}$ (or simply O). It is also the *additive identity* for matrix addition since $A + O = A$ for any matrix A (whenever the sizes of the matrices involved are proper).
- For any matrix $A = [a_{ij}]$, the matrix $[-a_{ij}]$ is called the **negative** or **additive inverse** of A. It is denoted by $-A$ and we have $A + (-A) = O$.

Then, the **matrix subtraction** can be defined by

$$A - B = A + (-B)$$

for any matrices A and B of the same size.

1.2.4 After introducing *matrix addition* and *matrix subtraction*, naturally the next operation we want to define would be related to *multiplication*. It turns out that for matrices, there are two kinds of multiplications: (i) *scalar multiplication* and (ii) *matrix multiplication*. Here, we first introduce *scalar multiplication* and we defer *matrix multiplication* to later part.

1.2.5 For any $m \times n$ matrix $A = [a_{ij}]$ and scalar k, we define $kA = [ka_{ij}]$ (i.e, $k[a_{ij}] = [ka_{ij}]$), and this is known as **scalar multiplication of a matrix**. Examples:

- $$3\begin{bmatrix}1 & 2\\ 3 & 4\\ 5 & 6\end{bmatrix} = \begin{bmatrix}3\cdot 1 & 3\cdot 2\\ 3\cdot 3 & 3\cdot 4\\ 3\cdot 5 & 3\cdot 6\end{bmatrix}.$$
- $0A = O$.
- $1A = A$.
- $(-1)A = -A$.

1.2.6 Like the usual addition and multiplication (of real numbers), the addition and scalar multiplication of matrices satisfy *distributive laws*:

- $s(A + B) = sA + sB$.
- $(s + t)A = sA + tA$.

Proof. Note that

$$s(A + B) = s[(a_{ij} + b_{ij})] = [s(a_{ij} + b_{ij})] = [sa_{ij} + sb_{ij}] = [sa_{ij}] + [sb_{ij}] = s[a_{ij}] + s[b_{ij}] = sA + sB,$$

and

$$(s + t)A = (s + t)[a_{ij}] = [(s + t)a_{ij}] = [sa_{ij} + ta_{ij}] = [sa_{ij}] + [ta_{ij}] = s[a_{ij}] + t[a_{ij}] = sA + tA.$$

$\square$

1.2.7 The scalar multiplication of matrices also satisfies the following "associative" property:

$$(st)A = s(tA).$$

Proof. Note that
$$(st)A = [st \cdot a_{ij}] = s[t \cdot a_{ij}] = s(tA).$$
□

1.2.8 The next operation to be discussed is exclusively for matrices (not useful for scalars): *matrix transpose*. The **transpose** of a matrix $A = [a_{ij}]$, denoted by A^T, is defined by $A^T = [a_{ji}]$, i.e., the matrix obtained from interchanging the rows and columns of A, while preserving the relative order. Example:

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

1.2.9 A square matrix A is called **symmetric** if $A^T = A$. Example:

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}^T = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}.$$

[Note: A symmetric matrix is symmetric along its main diagonal:

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

]

1.2.10 For any matrices A and B of the same size and scalar s, we have:

- $(A + B)^T = A^T + B^T$.
  Proof. Let $c_{ij} = a_{ij} + b_{ij}$ for any i and j. Then,
  $$(A + B)^T = [c_{ij}]^T = [c_{ji}] = [a_{ji} + b_{ji}] = [a_{ji}] + [b_{ji}] = A^T + B^T.$$
  □

- $(sA)^T = sA^T$.
  Proof. Let $c_{ij} = sa_{ij}$ for any i and j. Then,
  $$(sA)^T = [c_{ij}]^T = [c_{ji}] = [sa_{ji}] = s[a_{ji}] = sA^T.$$
  □

- $(A^T)^T = A$.
  Proof. Let $c_{ij} = a_{ji}$ for any i and j. Then,
  $$(A^T)^T = [a_{ji}]^T = [c_{ij}]^T = [c_{ji}] = [a_{ij}] = A.$$
  □

1.3 Introduction to Vectors

1.3.1 A **vector** refers to either a *row vector* or a *column vector*:

- A **row vector** is a matrix with one row.
- A **column vector** is a matrix with one column.

Unless otherwise specified, a vector would refer to a *column* vector (since it is more commonly used, as we will see later). To denote a vector, we usually use a bold small letter like $\boldsymbol{v}$. In written form, we usually use notations like $\underline{v}$ or $\vec{v}$ instead.

1.3.2 Some terminologies:

- The **zero vector** is a zero matrix with one column (i.e., a column vector where each entry is 0). It is denoted by $\mathbf{0}$. More explicitly, we may denote an $n \times 1$ zero vector by $\mathbf{0}_n$.
- The notation $\mathbb{R}^n$ denotes the set of all *column* vectors with n real entries.
- A (column) vector in $\mathbb{R}^n$, whose ith entry is 1 and other entries are 0, is denoted by $\boldsymbol{e}_i$. The vectors $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ are known as the **standard vectors/standard unit vectors/standard basis vectors** of $\mathbb{R}^n$.

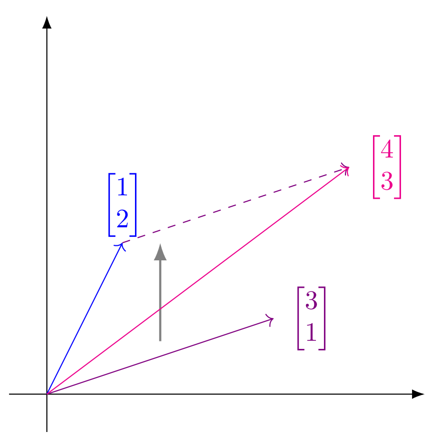
  [Note: When $n = 2$, sometimes we denote $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$ by $\boldsymbol{i}$ and $\boldsymbol{j}$ respectively. Also, when $n = 3$, sometimes we denote $\boldsymbol{e}_1$, $\boldsymbol{e}_2$, and $\boldsymbol{e}_3$ by $\boldsymbol{i}$, $\boldsymbol{j}$, and $\boldsymbol{k}$ respectively.]

1.3.3 Since vectors are matrices according to the definition, addition and scalar multiplication of vectors work in the same way as addition and scalar multiplication of matrices (defined in Section 1.2). Examples:

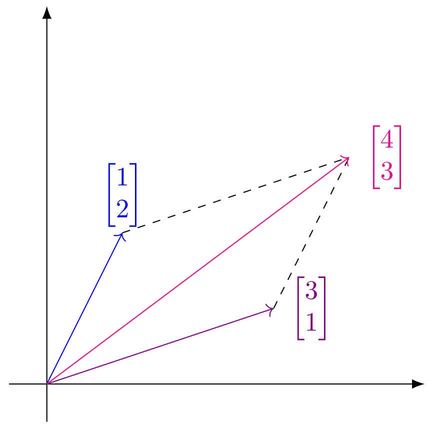
- $\begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix} + \begin{bmatrix} 2 \\ 4 \\ 6 \end{bmatrix} = \begin{bmatrix} 1+2 \\ 3+4 \\ 5+6 \end{bmatrix}$.
- $\begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix} + \begin{bmatrix} 2 \\ 4 \end{bmatrix}$ is not well-defined!
- $3 \begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix} = \begin{bmatrix} 3 \cdot 1 \\ 3 \cdot 3 \\ 3 \cdot 5 \end{bmatrix}$.

1.3.4 We would then like to investigate the *geometric meaning* behind addition and scalar multiplication of vectors. Addition of vectors can be performed geometrically by the *tip-to-tail method* or *parallelogram rule*.

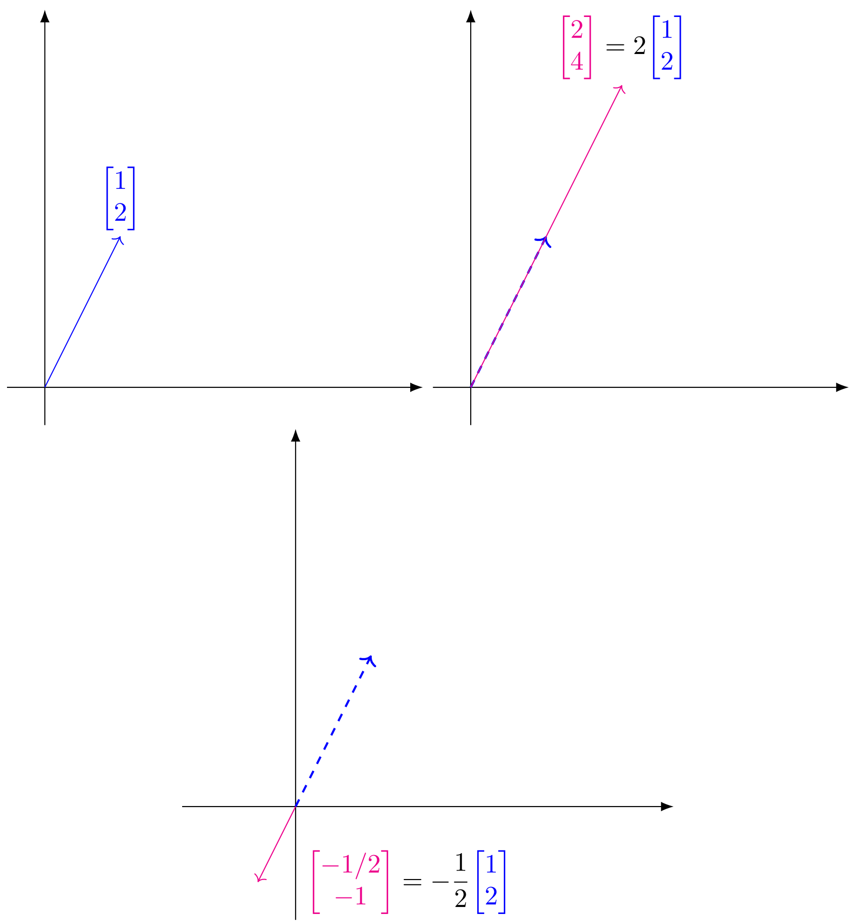
- *tip-to-tail method:*



- *parallelogram rule:*



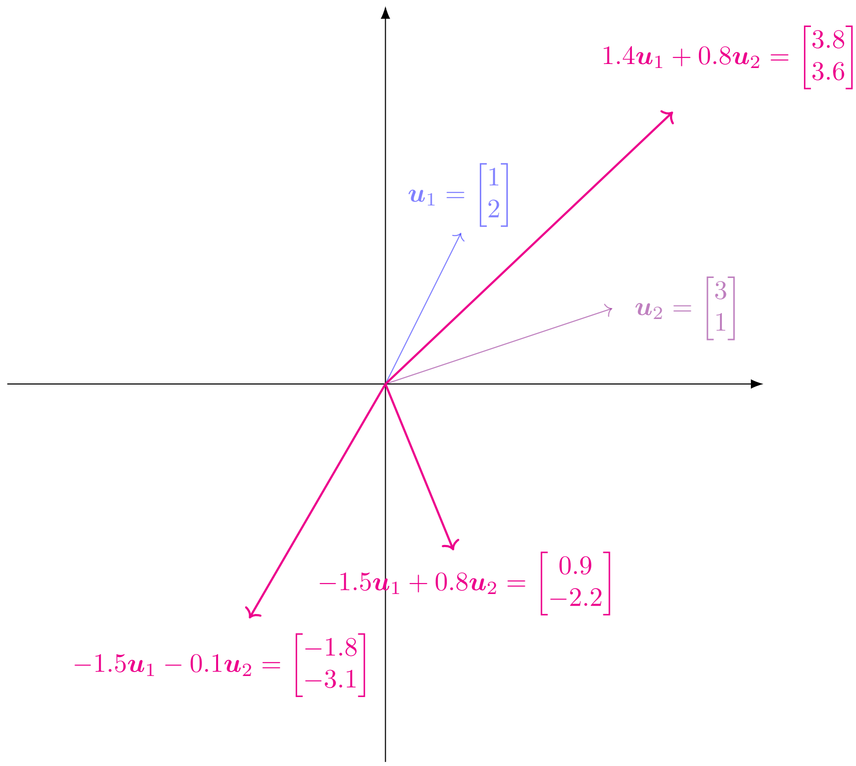
1.3.5 Scalar multiplication of vectors can also be performed geometrically, by "scaling" the vectors.



1.3.6 A **linear combination** of the vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ is a vector of the form

$$c_1\boldsymbol{u}_1 + \cdots + c_n\boldsymbol{u}_n$$

where $c_1, \ldots, c_n$ are constant scalars.



1.4 The Matrix-Vector Product

1.4.1 Before defining matrix product, we first introduce the notion of *matrix-vector product*. For a matrix A and a column vector $\boldsymbol{v}$, the **matrix-vector product** $A\boldsymbol{v}$ is defined by

$$A\boldsymbol{v} = v_1\boldsymbol{a}_1 + \cdots + v_n\boldsymbol{a}_n$$

where $\boldsymbol{v} = \begin{bmatrix}v_1\\ \vdots\\ v_n\end{bmatrix}$, and $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ denote the columns of A (as column vectors), i.e., $A = \begin{bmatrix}\boldsymbol{a}_1 & \cdots & \boldsymbol{a}_n\end{bmatrix}$.

Example:

$$\begin{bmatrix}1 & 2 & 3\\4 & 5 & 6\end{bmatrix}\begin{bmatrix}3\\2\\1\end{bmatrix} = 3\begin{bmatrix}1\\4\end{bmatrix} + 2\begin{bmatrix}2\\5\end{bmatrix} + 1\begin{bmatrix}3\\6\end{bmatrix} = \begin{bmatrix}3\cdot 1 + 2\cdot 2 + 1\cdot 3\\3\cdot 4 + 2\cdot 5 + 1\cdot 6\end{bmatrix} = \begin{bmatrix}10\\28\end{bmatrix}.$$

Remarks:

- If the number of columns of A is *not* n, then the matrix-product $A\boldsymbol{v}$ is *not well-defined!*
- We can observe that the matrix-vector product is yet another column vector. This is indeed not a coincidence: From the definition we know that for an $m \times n$ matrix A, the matrix-product vector must be an $m \times 1$ column vector (as $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ are all $m \times 1$ column vectors).
- An important point of view that relates matrices and *linear transformations* is to consider the function $\boldsymbol{v} \mapsto A\boldsymbol{v}$ (which is indeed a linear transformation), that sends a column vector $\boldsymbol{v} \in \mathbb{R}^n$ to another column vector $A\boldsymbol{v} \in \mathbb{R}^m$ (with possibly different size), when the size of matrix A is $m \times n$.
- The column vector $A\boldsymbol{v}$ is a linear combination of $\boldsymbol{v}$.

1.4.2 We have the following results regarding matrix-vector product (whenever the sizes of the matrices involved are proper):

- $A\boldsymbol{e}_j = \boldsymbol{a}_j$, where $\boldsymbol{a}_j$ is the jth column of A.

- $A\mathbf{0} = 0$.
- $O\boldsymbol{v} = 0$ for any column vector $\boldsymbol{v}$.

1.4.3 Recall the concept of *identity function*, which sends any input in its domain back to its own (symbolically, $f(x) = x$ for any x in the domain of f). We know from the previous remark that we can associate the concept of *matrix-vector product* with *function* (linear transformation), so now we are interested in investigating what kind of matrix-vector product corresponds to an *identity function*.

1.4.4 It turns out that setting the matrix A as the *identity matrix* (of appropriate size) connects the matrix-vector product with identity function. The **identity matrix** I is a square matrix whose all diagonal entries are 1 and other entries are 0. Examples:

$$I = \begin{bmatrix} 1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \text{ etc.}$$

For the $n \times n$ identity matrix ($n \in \mathbb{N}$), we may denote it more specifically by I_n.

[Note: The columns of an identity matrix I are *standard vectors*. More specifically, the jth column of I is $\boldsymbol{e}_j$.]

1.4.5 For any (column) vector $\boldsymbol{v}$, we have $I\boldsymbol{v} = \boldsymbol{v}$ (as long as the size of I is right).

Proof. Note that

$$I\boldsymbol{v} = v_1\boldsymbol{e}_1 + v_2\boldsymbol{e}_2 + \cdots + v_n\boldsymbol{e}_n = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \boldsymbol{v}.$$

□

1.4.6 For matrix-vector product, we have the following results. For any $m \times n$ matrices A, B, any vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^n$, and any scalar c,

- (distributive) $A(\boldsymbol{u} + \boldsymbol{v}) = A\boldsymbol{u} + A\boldsymbol{v}$.

  Proof. Note that

$$\begin{aligned} A(\boldsymbol{u} + \boldsymbol{v}) &= (u_1 + v_1)\boldsymbol{a}_1 + \cdots + (u_n + v_n)\boldsymbol{a}_n \\ &= (u_1\boldsymbol{a}_1 + \cdots + u_n\boldsymbol{a}_n) + (v_1\boldsymbol{a}_1 + \cdots + v_n\boldsymbol{a}_n) \\ &= A\boldsymbol{u} + A\boldsymbol{v}. \end{aligned}$$

  □

- (distributive) $(A + B)\boldsymbol{v} = A\boldsymbol{v} + B\boldsymbol{v}$.

  Proof. Note that

$$\begin{aligned} (A + B)\boldsymbol{v} &= v_1(\boldsymbol{a}_1 + \boldsymbol{b}_1) + \cdots + v_n(\boldsymbol{a}_n + \boldsymbol{b}_n) \\ &= (v_1\boldsymbol{a}_1 + \cdots + v_n\boldsymbol{a}_n) + (v_1\boldsymbol{b}_1 + \cdots + v_n\boldsymbol{b}_n) \\ &= A\boldsymbol{v} + B\boldsymbol{v}. \end{aligned}$$

  □

- ("associative") $A(c\boldsymbol{v}) = (cA)\boldsymbol{v}$.

  Proof. Note that

$$A(c\boldsymbol{v}) = (cv_1)\boldsymbol{a}_1 + \cdots + (cv_n)\boldsymbol{a}_n = v_1(c\boldsymbol{a}_1) + \cdots + v_n(c\boldsymbol{a}_n) = (cA)\boldsymbol{v}.$$

  □

[Note: In the proofs above, the notations $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ ($\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$) denote the columns of A (B), and we have

$$\boldsymbol{u} = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} \quad \text{and} \quad \boldsymbol{v} = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}.$$

]

1.5 Matrix Multiplication

1.5.1 *Matrix multiplication* may be seen as a "collection" of matrix-vector products (since a matrix can always be seen as a "collection" of column vectors; each column corresponds to a column vector).

1.5.2 In view of this, given an $m \times n$ matrix A and an $n \times p$ matrix B, we may first write

$$B = \begin{bmatrix} \boldsymbol{b}_1 & \cdots & \boldsymbol{b}_p \end{bmatrix}$$

where $\boldsymbol{b}_j$ is an $n \times 1$ column vector for each $j = 1, \ldots, p$. We know that how $A\boldsymbol{b}_j$ is defined for each j. So, to serve as a "collection" of matrix-vector products (or linear transformations), the **matrix product** AB should be defined as an $m \times p$ matrix

$$AB = \begin{bmatrix} A\boldsymbol{b}_1 & \cdots & A\boldsymbol{b}_p \end{bmatrix},$$

so that the jth column of AB is the matrix-vector product $A\boldsymbol{b}_j$.

[Note: It is important that the number of columns of A equals the number of rows of B. Otherwise, the matrix product is *not well-defined* (as the underlying matrix-vector products would also be not well-defined in such case).]

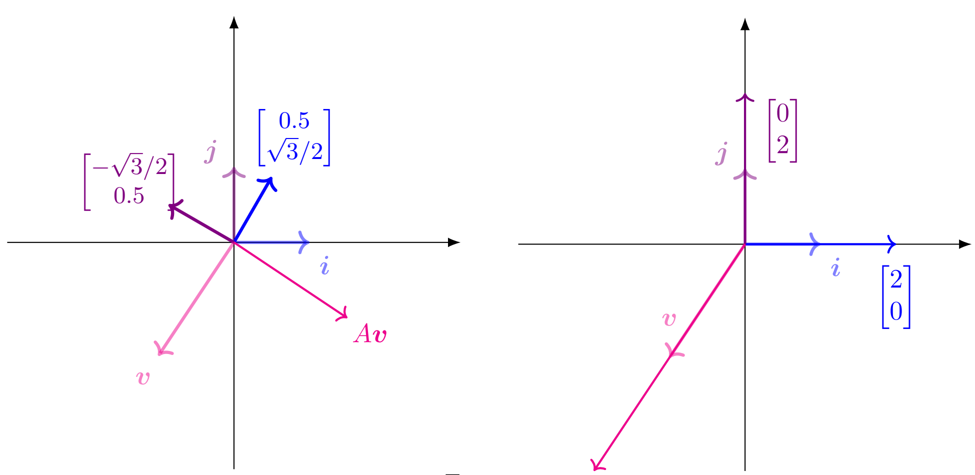
1.5.3 We can observe that such matrix multiplication induces linear transformations of p column vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_p$ respectively to another p column vectors $A\boldsymbol{b}_1, \ldots, A\boldsymbol{b}_p$, collected in the matrix product AB.

1.5.4 Particularly, for any $n \times n$ (square) matrix A, we have

$$A = AI_n = A\begin{bmatrix} \boldsymbol{e}_1 & \cdots & \boldsymbol{e}_n \end{bmatrix} = \begin{bmatrix} A\boldsymbol{e}_1 & \cdots & A\boldsymbol{e}_n \end{bmatrix}.$$

This suggests an interpretation of the columns of a square matrix A: the column vectors obtained by having a certain *linear transformation* (as specified by matrix A) on each of the standard vector. Indeed, we can view the matrix A as "representing" a certain kind of linear transformation.

Examples:



$$A = \begin{bmatrix} \cos\pi/3 & -\sin\pi/3 \\ \sin\pi/3 & \cos\pi/3 \end{bmatrix} = \begin{bmatrix} 0.5 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 0.5 \end{bmatrix} \qquad B = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

From the figure above, the (square) matrix $A = \begin{bmatrix} 0.5 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 0.5 \end{bmatrix}$ may be seen as representing a linear transformation of "rotating anticlockwise by 60°", and the (square) matrix $B = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ may be seen as representing a linear transformation of "scaling by 2 in all directions".

1.5.5 Furthermore, for $m \times n$ and $n \times p$ matrices A and B (respectively) and $p \times 1$ vector $\boldsymbol{v} = \begin{bmatrix} v_1 \\ \vdots \\ v_p \end{bmatrix}$, we have

$$A(B\boldsymbol{v}) = A(v_1\boldsymbol{b}_1 + \cdots + v_p\boldsymbol{b}_p) = (v_1 A\boldsymbol{b}_1 + \cdots + v_p A\boldsymbol{b}_p) = \boxed{(AB)\boldsymbol{v}}.$$

Viewing this based on a "linear transformation" interpretation, it suggests that the linear transformation specified by AB is indeed a "composition" of the linear transformation specified by B, *followed by* that specified by A:

$$\begin{tikzcd} \boldsymbol{v} \arrow[r, "\text{lin. trans. } (B)"] \arrow[rr, bend right, "\text{lin. trans. } (AB)"'] & \boldsymbol{Bv} \arrow[r, "\text{lin. trans. } (A)"] & \boldsymbol{A(Bv)} \end{tikzcd}$$

1.5.6 We can express the matrix product in a more explicit (and more familiar) form as follows: For any $i = 1, \ldots, m$ and $k = 1, \ldots, p$, the (i,k)-entry of AB is

$$(AB)_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

where we write $A = [a_{ij}]$ and $B = [b_{jk}]$.

Examples:

- $$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 2 \end{bmatrix} = \left[\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} \right]$$
$$= \left[1\begin{bmatrix} 1 \\ 3 \end{bmatrix} + 0\begin{bmatrix} 2 \\ 2 \end{bmatrix} + 1\begin{bmatrix} 3 \\ 1 \end{bmatrix} \quad 0\begin{bmatrix} 1 \\ 3 \end{bmatrix} + 1\begin{bmatrix} 2 \\ 2 \end{bmatrix} + 2\begin{bmatrix} 3 \\ 1 \end{bmatrix} \right]$$
$$= \begin{bmatrix} 4 & 8 \\ 4 & 4 \end{bmatrix}$$

- $$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 2 \end{bmatrix} = \left[\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} \right]$$
$$= \left[1\begin{bmatrix} 1 \\ 3 \end{bmatrix} + 0\begin{bmatrix} 2 \\ 2 \end{bmatrix} + 1\begin{bmatrix} 3 \\ 1 \end{bmatrix} \quad 0\begin{bmatrix} 1 \\ 3 \end{bmatrix} + 1\begin{bmatrix} 2 \\ 2 \end{bmatrix} + 2\begin{bmatrix} 3 \\ 1 \end{bmatrix} \right]$$
$$= \begin{bmatrix} 4 & 8 \\ 4 & 4 \end{bmatrix}$$

1.5.7 We can also express the (i,k)-entry of AB as

$$(AB)_{ik} = \boldsymbol{a}_i'\boldsymbol{b}_k = \begin{bmatrix} a_{i1} & \cdots & a_{in} \end{bmatrix} \begin{bmatrix} b_{1k} \\ \vdots \\ b_{nk} \end{bmatrix} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

where $\boldsymbol{a}_i'$ and $\boldsymbol{b}_k$ are ith row of A and kth column of B respectively. [Note: This is sometimes known as the **dot product** of $\boldsymbol{a}_i$ and $\boldsymbol{b}_k$ (which sums the products of the corresponding pairs of entries in the vectors).]

1.5.8 We have defined matrix product using a "by column" approach. But actually we can also define it using a "by row" approach. First, we write

$$A = \begin{bmatrix} \boldsymbol{a}_1' \\ \vdots \\ \boldsymbol{a}_m' \end{bmatrix}.$$

Then, we have

$$AB = \begin{bmatrix} \boldsymbol{a}_1'B \\ \vdots \\ \boldsymbol{a}_m'B \end{bmatrix}$$

where the "left matrix-vector product" $\boldsymbol{v}'B$ is defined by

$$\boldsymbol{v}'B = v_1\boldsymbol{b}_1' + \cdots + v_n\boldsymbol{b}_n'$$

with $\boldsymbol{v}' = \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix}$ and $B = \begin{bmatrix} \boldsymbol{b}_1' \\ \vdots \\ \boldsymbol{b}_n' \end{bmatrix}$, so that $(\boldsymbol{v}'B)^T = B^T(\boldsymbol{v}')^T$ where the RHS $B^T(\boldsymbol{v}')^T$ carries the meaning from the usual matrix-vector product discussed previously.

Examples:

- $$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 2 \end{bmatrix} \\ \begin{bmatrix} 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 2 \end{bmatrix} \end{bmatrix}$$
$$= \begin{bmatrix} 1\begin{bmatrix} 1 & 0 \end{bmatrix} + 2\begin{bmatrix} 0 & 1 \end{bmatrix} + 3\begin{bmatrix} 1 & 2 \end{bmatrix} \\ 3\begin{bmatrix} 1 & 0 \end{bmatrix} + 2\begin{bmatrix} 0 & 1 \end{bmatrix} + 1\begin{bmatrix} 1 & 2 \end{bmatrix} \end{bmatrix}$$
$$= \begin{bmatrix} 4 & 8 \\ 4 & 4 \end{bmatrix}$$

- $$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 2 \end{bmatrix} \\ \begin{bmatrix} 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 2 \end{bmatrix} \end{bmatrix}$$
$$= \begin{bmatrix} 1\begin{bmatrix} 1 & 0 \end{bmatrix} + 2\begin{bmatrix} 0 & 1 \end{bmatrix} + 3\begin{bmatrix} 1 & 2 \end{bmatrix} \\ 3\begin{bmatrix} 1 & 0 \end{bmatrix} + 2\begin{bmatrix} 0 & 1 \end{bmatrix} + 1\begin{bmatrix} 1 & 2 \end{bmatrix} \end{bmatrix}$$
$$= \begin{bmatrix} 4 & 8 \\ 4 & 4 \end{bmatrix}$$

1.5.9 Another remarkable approach for matrix multiplication is *block multiplication*, which can be helpful especially when the sizes of the matrices involved are large.

The basic idea of **block multiplication** is to divide a large matrix into several partitions or *blocks*, and "treat" each block like a scalar. Then, it can be shown that performing matrix multiplication as usual under this treatment results in a correct matrix product.

1.5.10 From a "partition" perspective, the previous "by column" ("by row") definition of matrix multiplication is actually indeed just block multiplication with the matrix B (A) having columns (rows) partitioned, and the whole matrix A (B) treated as a single block (a matrix with one "block entry") respectively.

- ("by column")

$$AB = \begin{bmatrix} A \end{bmatrix} \begin{bmatrix} \boldsymbol{b}_1 & \cdots & \boldsymbol{b}_p \end{bmatrix} \overset{\text{entries treated as scalars}}{=} \begin{bmatrix} A\boldsymbol{b}_1 & \cdots & A\boldsymbol{b}_p \end{bmatrix}.$$

- ("by row")

$$AB = \begin{bmatrix} \boldsymbol{a}_1' \\ \vdots \\ \boldsymbol{a}_m' \end{bmatrix} \begin{bmatrix} B \end{bmatrix} \overset{\text{entries treated as scalars}}{=} \begin{bmatrix} \boldsymbol{a}_1' B \\ \vdots \\ \boldsymbol{a}_m' B \end{bmatrix}.$$

1.5.11 In general, under block multiplication, we can partition a matrix into *rectangular blocks*/submatrices (partition *both* rows and columns), and then carry out the matrix multiplication (treating each block as scalar), *as long as* matrix multiplication under such treatment is *well-defined*.

To ensure the well-definedness, for matrix product AB, the *columns* of A and the *rows* of B should be partitioned in the *same pattern*. Example:

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

1.5.12 To justify the block multiplication approach, we can utilize the explicit form of matrix multiplication in [1.5.6]. Intuitively, each "partition" in block multiplication indeed corresponds to a certain "splitting" of the sum. For example, in the block multiplication

$$\begin{bmatrix} 1 & 2 & 1 & 3 & 5 \\ 0 & 7 & 0 & 3 & 1 \\ 1 & 5 & 1 & 4 & 3 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 1 & 6 \\ 0 & 0 \\ 1 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 7 & 0 \\ 1 & 5 & 1 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 1 & 6 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 5 \\ 3 & 1 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix},$$

the $(1, 1)$-entry can be obtained by

$$1 \cdot 2 + 2 \cdot 1 + 1 \cdot 0 + 3 \cdot 1 + 5 \cdot 2 \overset{\text{split}}{=} (1 \cdot 2 + 2 \cdot 1 + 1 \cdot 0) + (3 \cdot 1 + 5 \cdot 2).$$

1.5.13 To close Section 1.5, we introduce the concept of *matrix power*. If A is a *square* matrix and k is a positive integer, then the **kth power of A** is

$$A^k = \underbrace{AA \cdots A}_{k \text{ times}}.$$

1.6 Properties of Matrix Multiplication

1.6.1 Here we will introduce several properties of matrix multiplication. To prove them, we will mainly utilize the explicit form of matrix multiplication in [1.5.6].

1.6.2 The first property is *associativity* (like matrix addition). Let A, B, and C be $m \times n$, $n \times p$, and $p \times q$ matrices respectively. Then, we have

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

Proof. For any $i = 1, \ldots, m$ and $\ell = 1, \ldots, q$,

$$\begin{aligned}
[(AB)C]_{i\ell} &= \sum_{k=1}^{p} (AB)_{ik} C_{k\ell} \\
&= \sum_{k=1}^{p} \sum_{j=1}^{n} A_{ij} B_{jk} C_{k\ell} \\
&= \sum_{j=1}^{n} \sum_{k=1}^{p} A_{ij} B_{jk} C_{k\ell} && \text{(switching summation order)} \\
&= \sum_{j=1}^{n} \underbrace{A_{ij}}_{\text{independent of } k} \sum_{k=1}^{p} B_{jk} C_{k\ell} \\
&= \sum_{j=1}^{n} A_{ij} (BC)_{j\ell} \\
&= [A(BC)]_{i\ell}.
\end{aligned}$$

□

1.6.3 The next one is *distributivity* (like matrix addition again). Let A be an $m \times n$ matrix, and let B and C be $n \times p$ matrices. Then,

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

Proof. For any $i = 1, \ldots, m$ and $k = 1, \ldots, p$,

$$\begin{aligned}
[A(B + C)]_{ik} &= \sum_{j=1}^{n} A_{ij} (B + C)_{jk} \\
&= \sum_{j=1}^{n} A_{ij} (B_{jk} + C_{jk}) \\
&= \sum_{j=1}^{n} (A_{ij} B_{jk} + A_{ij} C_{jk}) \\
&= \sum_{j=1}^{n} A_{ij} B_{jk} + \sum_{j=1}^{n} A_{ij} C_{jk} \\
&= (AB)_{ik} + (AC)_{ik}.
\end{aligned}$$

□

The above property is *left-distributivity* to be more specific. The *right-distributivity* also holds, but we need to adjust the sizes of the matrices:

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

when A and B are $m \times n$ matrices, and C is an $n \times p$ matrix.

Proof. Similar to the proof above. □

1.6.4 This “property” is of particular importance: *non-commutativity* (unlike matrix addition!). Even for two square matrices A and B, we do *not* always have $AB = BA$!

Proof. To prove this, it suffices to give a counterexample. Take $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Then,

$$AB = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \quad \text{while} \quad BA = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

$\square$

1.6.5 The final property we discuss here is related to *matrix transpose*. Let A be an $m \times n$ matrix and B be an $n \times p$ matrix. Then we have the following *anti-commutativity* for transpose of AB:

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

Proof. For any $i = 1, \dots, m$ and $k = 1, \dots, p$, we have

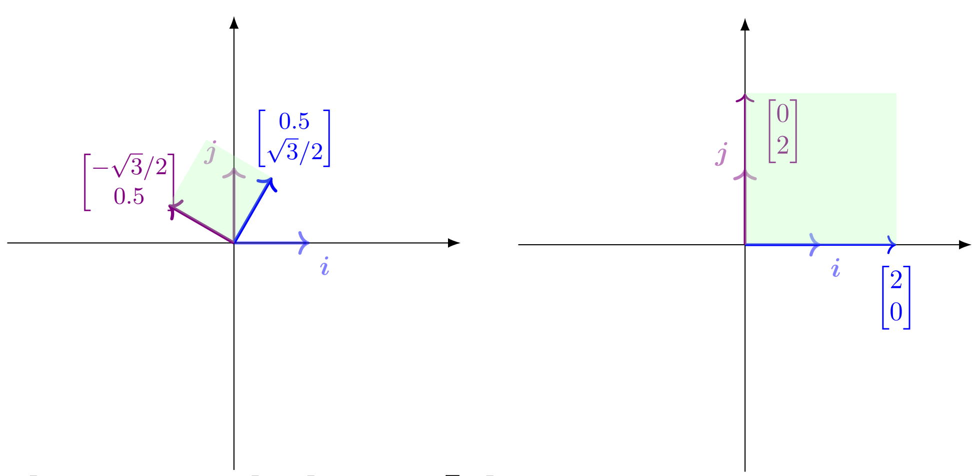
$$\begin{aligned} [(AB)^T]_{ki} &= (AB)_{ik} \\ &= \sum_{j=1}^{n} A_{ij} B_{jk} \\ &= \sum_{j=1}^{n} (B^T)_{kj} (A^T)_{ji} \\ &= (B^T A^T)_{ki}. \end{aligned}$$

$\square$

1.7 Determinants

1.7.1 Recall the “linear transformation” interpretation of a square matrix in [1.5.4]. Basically, the concept of *determinant* aims to “quantify” the linear transformation “represented” by the square matrix.

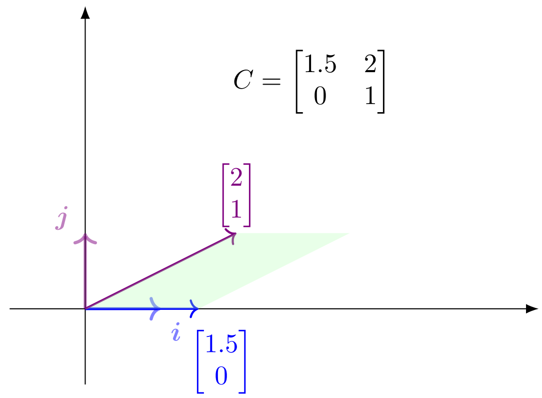
More specifically, the *determinant* of an $n \times n$ square matrix is the *signed* “area”[1] (or its analogue in other dimension) of the geometrical object “spanned” by the vectors linearly transformed from the standard vectors (i.e., “parallelogram”[2] with those transformed vectors as sides, roughly speaking).



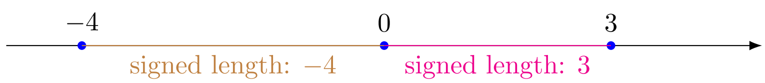
$$A = \begin{bmatrix} \cos \pi/3 & -\sin \pi/3 \\ \sin \pi/3 & \cos \pi/3 \end{bmatrix} = \begin{bmatrix} 0.5 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 0.5 \end{bmatrix} \qquad B = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

[1] For the 2×2 case, this means that the area “above” (“below”) the vector linearly transformed from $\boldsymbol{i}$ contributes positively (negatively) to this quantity, and the area on the “right” (“left”) of the vector linearly transformed from $\boldsymbol{j}$ contributes positively (negatively) to this quantity.

[2] or its analogue in other dimension, e.g., parallelepiped in 3-dimensional case



1.7.2 First, we consider a special case where $n = 1$. In such case, instead of considering signed *area*, we consider a *lower-dimensional* analogue: signed *length*. In the $n = 1$ case, the **determinant of a 1×1 matrix** $[a]$ is just the signed length of line segment joining 0 and a in the real number line, namely $\boxed{a}$.



The determinant of a matrix A is denoted by $\det A$ or $|A|$. When, we write out the entries of A explicitly like $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we can also denote its determinant by $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ (replacing the brackets by vertical bars). [⚠ Warning: It may lead to some ambiguity for the 1×1 matrix case as we would just write $|a|$, which may be understood as the absolute value of a. But it may <u>not</u> equal the determinant of 1×1 matrix $[a]$!]

1.7.3 For 2×2 and 3×3 matrices, the determinant is defined as follows.

- The **determinant of a 2×2 matrix** $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is

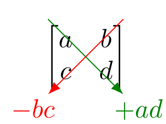
$$\boxed{ad - bc}.$$

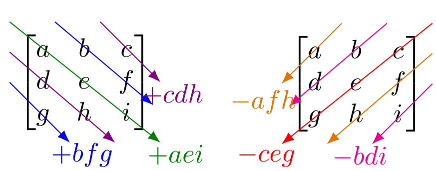
- The **determinant of a 3×3 matrix** $\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$ is

$$\boxed{aei + bfg + cdh - ceg - bdi - afh}.$$

This definition turns out to coincide with the geometrical interpretation in [1.7.1], by considering *cross product* (2×2 case) and *scalar triple product* (3×3 case).

[Mnemonic: Both expressions can be viewed via "diagonal multiplication":





]

1.7.4 Observe that the determinant of a 3×3 matrix can actually be expressed in terms of determinants of 2×2 matrices:

$$\begin{aligned}\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} &= aei + bfg + cdh - ceg - bdi - afh \\ &= a(ei - fh) - b(di - fg) + c(dh - eg) \\ &= a\begin{vmatrix} e & f \\ h & i \end{vmatrix} - b\begin{vmatrix} d & f \\ g & i \end{vmatrix} + c\begin{vmatrix} d & e \\ g & h \end{vmatrix}.\end{aligned}$$

Indeed, the determinant of a 2×2 matrix can also be expressed in terms of determinants of 1×1 "matrices" (which are scalars essentially), obviously:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc = a\det[d] - b\det[c].$$

Additionally, we have the following observations:

- The signs of the terms are alternating ("chessboard pattern": $+$, $-$, $+$, ...).
- The coefficients of the determinants originate from the first row of the original matrix.
- The "child" determinants are determinants of some submatrices of the original. In fact, they are obtained by deleting a row and a column:

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} \longrightarrow \begin{vmatrix} e & f \\ h & i \end{vmatrix} \qquad \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} \longrightarrow \begin{vmatrix} d & f \\ g & i \end{vmatrix} \qquad \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} \longrightarrow \begin{vmatrix} d & e \\ g & h \end{vmatrix}$$

These lead to the following general (*cofactor expansion*) definition of determinant.

1.7.5 Let $A = [a_{ij}]$ be an $n \times n$ matrix with $n \geq 2$. Let $\widetilde{A}_{ij}$ be the $(n-1) \times (n-1)$ matrix obtained by deleting the ith row and the jth column of A.

Then, we have the following terminologies:

- The **(i,j)-minor** of A is $\det \widetilde{A}_{ij}$.
- The **(i,j)-cofactor** of A is $C_{ij} = (-1)^{i+j} \det \widetilde{A}_{ij}$.
- The **cofactor matrix** of A is the $n \times n$ matrix $[C_{ij}]$.

[Note: When $i + j$ is odd (even), the sign for the (i,j)-cofactor is negative (positive). The following shows the sign for the cofactor at different locations (corresponding to different values of i and j) for some cases, which are of "chessboard pattern":

$$\begin{bmatrix} + & - \\ - & + \end{bmatrix} \quad \begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix} \quad \begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{bmatrix}$$

]

The **determinant** of A is then recursively defined as

$$\det A = a_{11}C_{11} + a_{12}C_{12} + \cdots + a_{1n}C_{1n}.$$

<u>Remarks</u>:

- This process is also known as *cofactor expansion along the first row*.
- This definition is *recursive* since the definition for $n \times n$ determinant utilizes the notion of $(n-1)\times(n-1)$ determinant, which is assumed to be already defined.
- Note that this definition does not include the case for 1×1 matrix. However, we have already defined that $\det[a] = a$.
- It is not hard to verify that the previous definitions of determinants of 2×2 and 3×3 matrices are consistent with this general definition.

1.7.6 The general definition of determinant allows us to compute the determinant of a matrix with size larger than 3×3. Examples:

- $\begin{vmatrix} 2 & 0 & 0 & 3 \\ 1 & 2 & 0 & -1 \\ -2 & 1 & 2 & 0 \\ 0 & -3 & 1 & 2 \end{vmatrix} = 2\begin{vmatrix} 2 & 0 & -1 \\ 1 & 2 & 0 \\ -3 & 1 & 2 \end{vmatrix} - 3\begin{vmatrix} 1 & 2 & 0 \\ -2 & 1 & 2 \\ 0 & -3 & 1 \end{vmatrix} = 2(1) - 3(11) = -31.$
- $\det I_n = 1$ for any $n \in \mathbb{N}$.

  Proof. Firstly, we have $\det I_1 = 1$. Then, assume for induction that $\det I_k = 1$ for a certain $k \in \mathbb{N}$. Then,
  $$\det I_{k+1} = 1 \cdot \det I_k + \underbrace{0 + \cdots + 0}_{k \text{ times}} = \det I_k = 1.$$
  Thus, the result follows by induction. □

[⚠ Warning: The "diagonal multiplication" does <u>not</u> hold for (square) matrices with size larger than 3×3. A counterexample is
$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$
where the "diagonal multiplication" yields 0, but the actual determinant (found by cofactor expansion along the first row) is -1.]

1.7.7 The *definition* of determinant utilizes cofactor expansion along the *first row*. Naturally, one may then ask whether we can perform cofactor expansion along other row (or even column). It turns out cofactor expansion along *any* row or column gives the same result, by the *cofactor expansion theorem*.

Theorem 1.7.a (Cofactor expansion theorem). Let $A = [a_{ij}]$ be an $n \times n$ matrix with the (i,j)-cofactor being C_{ij}. Then, we have
$$\det A = a_{i1}C_{i1} + \cdots + a_{in}C_{in} \quad \text{(cofactor expansion along the } i\text{th row)}$$
for any $i = 1, \ldots, n$, and
$$\det A = a_{1j}C_{1j} + \cdots + a_{nj}C_{nj} \quad \text{(cofactor expansion along the } j\text{th column)}$$
for any $j = 1, \ldots, n$.

[⚠ Warning: Be careful about the signs of the cofactors!]

1.7.8 The cofactor expansion theorem is helpful for simplifying (possibly substantially) the computations of determinants (compared with cofactor expansion along the first row). Examples:

- $\begin{vmatrix} 1 & 2 & 3 & 0 & 4 \\ 1 & 0 & 0 & 0 & 0 \\ 4 & 3 & 2 & 2 & 1 \\ -1 & -2 & 0 & 0 & 2 \\ 2 & -3 & -2 & 0 & -1 \end{vmatrix} = -1\begin{vmatrix} 2 & 3 & 0 & 4 \\ 3 & 2 & 2 & 1 \\ -2 & 0 & 0 & 2 \\ -3 & -2 & 0 & -1 \end{vmatrix} + 0 = 2\begin{vmatrix} 2 & 3 & 4 \\ -2 & 0 & 2 \\ -3 & -2 & -1 \end{vmatrix} = 2(0) = 0.$

- The determinant of a triangular (upper triangular or lower triangular) matrix is the product of all its diagonal entries.

  Proof. WLOG, suppose the matrix is upper triangular (the argument is similar for lower triangular matrix). Then, it is of the form

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1,n-1} & a_{1n} \\ 0 & a_{22} & \cdots & a_{2,n-1} & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{nn} \end{bmatrix}.$$

  Now performing cofactor expansion along the last (nth) row gives

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1,n-1} & a_{1n} \\ 0 & a_{22} & \cdots & a_{2,n-1} & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{nn} \end{vmatrix} = a_{nn} \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1,n-2} & a_{1,n-1} \\ 0 & a_{22} & \cdots & a_{2,n-2} & a_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{n,n-1} \end{vmatrix}.$$

  For the matrix on RHS, performing cofactor expansion along the last ($n-1$th) row gives

$$a_{nn}a_{n-1,n-1} \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1,n-3} & a_{1,n-2} \\ 0 & a_{22} & \cdots & a_{2,n-3} & a_{2,n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{n,n-2} \end{vmatrix}$$

  Repeating this process, we know that the determinant is

$$a_{nn}a_{n-1,n-1}\cdots a_{11},$$

  the product of all its diagonal entries. □

1.7.9 It turns out that we have a similar result regarding the determinant of a **block triangular matrix** (i.e., when viewing the blocks as scalars (zero matrix ➔ zero scalar), the matrix is triangular).

Consider an $n \times n$ matrix A which is block triangular, i.e.,

$$A = \begin{bmatrix} A_{11} & * & \cdots & * \\ O & A_{22} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & A_{kk} \end{bmatrix} \quad \text{or} \quad A = \begin{bmatrix} A_{11} & O & \cdots & O \\ * & A_{22} & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & A_{kk} \end{bmatrix}.$$

[3] Suppose that A_{ii} is a square matrix for any $i = 1, \ldots, n$. Then,

$$\det A = \det A_{11} \times \cdots \times \det A_{nn},$$

i.e., the determinant of A is the product of the *determinants* of all its diagonal *blocks*.

1.8 Properties of Determinants

1.8.1 In general, computing determinants can be quite laborious and tedious (especially for large matrices). So, here we introduce some properties of determinants that can simplify the computations of determinants (in some cases).

1.8.2 The first property suggests the effect of *switching rows* on the determinant. It is also known as the *alternating* property (as the sign "alternates" through switching rows).

[3] $*$'s denote arbitrary blocks (with appropriate sizes).

Proposition 1.8.a (Alternating)**.** Let $A = [a_{ij}]$ be an $n \times n$ matrix. Suppose that $B = [b_{ij}]$ is obtained from A by switching two of its rows. Then,

$$\det B = -\det A.$$

Proof. WLOG, we can assume that the two rows being switched are adjacent. (For switching of two non-adjacent rows, we can show that it is equivalent to switching adjacent rows for *odd number* of times ➔ $(-1)^{\text{odd number}} = -1$.)

Now, let the two rows being switched be rows i and $i+1$. Then, we can see that for any $j = 1, \ldots, n$,

$$\widetilde{A}_{ij} = \widetilde{B}_{i+1,j} \quad \text{and} \quad a_{ij} = b_{i+1,j}.$$

Now, we perform cofactor expansion along the ith ($i+1$th) row for matrix A (B):

- $\det A = \sum_{j=1}^{n} a_{ij}(-1)^{i+j} \det \widetilde{A}_{ij}$.
- $\det B = \sum_{j=1}^{n} b_{i+1,j}(-1)^{i+1+j} \det \widetilde{B}_{i+1,j} = -\sum_{j=1}^{n} b_{i+1,j}(-1)^{i+j} \det \widetilde{B}_{i+1,j}$.

By comparing the two expressions, we can observe that

$$\det B = -\det A.$$

□

Example:

$$\begin{vmatrix} 2 & 1 \\ 3 & -1 \end{vmatrix} = -\begin{vmatrix} 3 & -1 \\ 2 & 1 \end{vmatrix}.$$

1.8.3 A corollary from Proposition 1.8.a is the following.

Corollary 1.8.b. Let A be an $n \times n$ matrix. If A has two identical rows, then $\det A = 0$.

Proof. Switching the two identical rows of A results in the same matrix A. But then by Proposition 1.8.a, we must have

$$\det A = -\det A \implies 2\det A = 0 \implies \det A = 0.$$

□

Example:

$$\begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 3 & 3 & 1 \\ 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 7 & 5 & 9 \end{vmatrix} = 0.$$

1.8.4 The next property is about *adding a scalar multiple of row vector to a row.* It is also known as *multilinearity* since it suggests a "linearity" property on each row (when there are multiple rows in a matrix).

Proposition 1.8.c (Multilinearity)**.** Let $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_n$ be $1 \times n$ row vectors and let $\boldsymbol{u}$ be another $1 \times n$ row vector. Let $c \in \mathbb{R}$. Then,

$$\det \begin{bmatrix} \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_{i-1} \\ \boldsymbol{r}_i + c\boldsymbol{u} \\ \boldsymbol{r}_{i+1} \\ \vdots \\ \boldsymbol{r}_n \end{bmatrix} = \det \begin{bmatrix} \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_{i-1} \\ \boldsymbol{r}_i \\ \boldsymbol{r}_{i+1} \\ \vdots \\ \boldsymbol{r}_n \end{bmatrix} + c \det \begin{bmatrix} \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_{i-1} \\ \boldsymbol{u} \\ \boldsymbol{r}_{i+1} \\ \vdots \\ \boldsymbol{r}_n \end{bmatrix}$$

Proof. For convenience, we denote the equality above (which is to be proved) by

$$\det A = \det B + c \det C.$$

We then perform cofactor expansion along the ith row for evaluating $\det A$, $\det B$, and $\det C$. First, note that for any $j = 1, \ldots, n$,

$$\widetilde{A}_{ij} = \widetilde{B}_{ij} = \widetilde{C}_{ij}.$$

We denote the common (i,j)-*cofactor* by C_{ij} (without $\widetilde{\ }$).

Now, write $\boldsymbol{r}_i = \begin{bmatrix} r_{i1} & \cdots & r_{in} \end{bmatrix}$ and $\boldsymbol{u} = \begin{bmatrix} u_1 & \cdots & u_n \end{bmatrix}$. Then, we have:

- $\det A = \displaystyle\sum_{j=1}^{n} (r_{ij} + cu_j) C_{ij} = \sum_{j=1}^{n} r_{ij} C_{ij} + c \sum_{j=1}^{n} u_j C_{ij}$.
- $\det B = \displaystyle\sum_{j=1}^{n} r_{ij} C_{ij}$.
- $\det C = \displaystyle\sum_{j=1}^{n} u_j C_{ij}$.

It is then not hard to see that the equality holds. ∎

Example:

$$\begin{vmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{vmatrix} + \underbrace{\begin{vmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 3 & 4 & 5 \end{vmatrix}}_{0} = \begin{vmatrix} 1 & 1 & 1 \\ 3 & 4 & 5 \\ 3 & 4 & 5 \end{vmatrix} = 0.$$

1.8.5 The next property is about matrix transpose. It turns out that taking transpose does not affect the determinant.

Proposition 1.8.d. Let $A = [a_{ij}]$ be an $n \times n$ matrix (where $n \in \mathbb{N}$). Then, $\det A^T = \det A$.

Proof. We prove this by induction. The case $n = 1$ clearly holds since the transpose of a 1×1 matrix is still the 1×1 matrix itself. Next, assume that the result holds for $n = k$, for a certain $k \in \mathbb{N}$. Now, consider the case $n = k + 1$ (where A is a $(k+1) \times (k+1)$ matrix).

Firstly, performing cofactor expansion along the first row for $\det A$ gives

$$\det A = \sum_{j=1}^{k+1} a_{1j} (-1)^{1+j} \det \widetilde{A}_{1j}.$$

Now, write $A^T = [b_{ij}]$ (then $b_{ij} = a_{ji}$). Note that for any $j = 1, \ldots, k+1$, $(\widetilde{A^T})_{j1} = (\widetilde{A}_{1j})^T$. Then, by induction hypothesis we have for any $j = 1, \ldots, k+1$,

$$\det\left(\widetilde{A^T}\right)_{j1} = \det\left(\widetilde{A}_{1j}\right)^T \overset{\text{induction hypothesis}}{=} \det \widetilde{A}_{1j}$$

(as $\widetilde{A}_{1j}$ is of size $k \times k$).

Thus, performing cofactor expansion along the first *column* for $\det A^T$ gives

$$\det A^T = \sum_{j=1}^{k+1} b_{j1} (-1)^{j+1} \det\left(\widetilde{A^T}\right)_{j1} = \sum_{j=1}^{k+1} a_{1j} (-1)^{1+j} \det \widetilde{A}_{1j} = \det A,$$

so the case $n = k + 1$ holds. Hence, the result follows by induction. ∎

1.8.6 Since taking *transpose* interchanges rows and columns (while preserving the relative order), Proposition 1.8.d "translates" the previous *alternating* and *multilinear* properties for rows into the corresponding "column version":

Proposition 1.8.e (Column version of alternating and multilinear properties)**.** Let A be an $n \times n$ matrix. Then,

(a) If two *columns* of A are switched to obtain a matrix B, then $\det B = -\det A$.

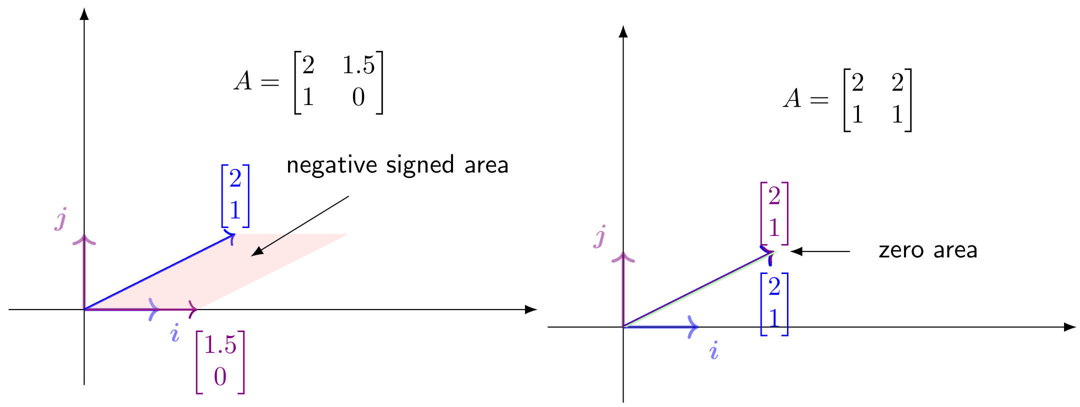
(b) If A has two identical *columns*, then $\det A = 0$.

(c) Let $\boldsymbol{c}_1, \dots, \boldsymbol{c}_n$ be $n \times 1$ *column* vectors, and let $\boldsymbol{u}$ be another $n \times 1$ *column* vector. Let $c \in \mathbb{R}$. Then,

$$\begin{aligned}&\det \begin{bmatrix}\boldsymbol{c}_1 & \cdots & \boldsymbol{c}_{i-1} & \boldsymbol{c}_i + c\boldsymbol{u} & \boldsymbol{c}_{i+1} & \cdots & \boldsymbol{c}_n\end{bmatrix} \\ &\quad = \det \begin{bmatrix}\boldsymbol{c}_1 & \cdots & \boldsymbol{c}_{i-1} & \boldsymbol{c}_i & \boldsymbol{c}_{i+1} & \cdots & \boldsymbol{c}_n\end{bmatrix} + c \det \begin{bmatrix}\boldsymbol{c}_1 & \cdots & \boldsymbol{c}_{i-1} & \boldsymbol{u} & \boldsymbol{c}_{i+1} & \cdots & \boldsymbol{c}_n\end{bmatrix}.\end{aligned}$$

Proof. They follow from taking transpose on the matrices for the respective results proved before. □

[Intuition 💡: We can gain some intuition on [1.8.6]a and [1.8.6]b by considering the geometrical interpretation of determinant:



]

1.8.7 Next, we consider some properties that apply to the "whole" matrix (not rows or columns). The first one is about scalar multiplication.

Proposition 1.8.f. Let A be an $n \times n$ matrix and let $k \in \mathbb{R}$. Then,

$$\det(kA) = k^n \det A.$$

[⚠ Warning: We do <u>not</u> have $\det(kA) = k \det A$ (unless $n = 1$)!]

Proof. Write $A = \begin{bmatrix}\boldsymbol{c}_1 & \boldsymbol{c}_2 & \cdots & \boldsymbol{c}_n\end{bmatrix}$. Then,

$$kA = \begin{bmatrix}k\boldsymbol{c}_1 & \boldsymbol{c}_2 & \cdots & k\boldsymbol{c}_n\end{bmatrix}.$$

Now, applying [1.8.6]c n times gives

$$\begin{aligned}\det(kA) &= \det \begin{bmatrix}k\boldsymbol{c}_1 & k\boldsymbol{c}_2 & \cdots & k\boldsymbol{c}_n\end{bmatrix} \\ &= k \det \begin{bmatrix}\boldsymbol{c}_1 & k\boldsymbol{c}_2 & \cdots & k\boldsymbol{c}_n\end{bmatrix} \\ &= k^2 \det \begin{bmatrix}\boldsymbol{c}_1 & \boldsymbol{c}_2 & \cdots & k\boldsymbol{c}_n\end{bmatrix} \\ &= \cdots \\ &= k^n \det \begin{bmatrix}\boldsymbol{c}_1 & \boldsymbol{c}_2 & \cdots & \boldsymbol{c}_n\end{bmatrix} \\ &= k^n \det A.\end{aligned}$$

□

1.8.8 Apart from scalar multiplication, we also have a property regarding *matrix multiplication*. It turns out that there is a *multiplicative* property.

Proposition 1.8.g (Multiplicative)**.** Let A and B be two $n \times n$ matrices. Then,

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

1.8.9 To close Section 1.8, we introduce a "rule" that simplifies computation of determinants, based on the properties we derive. Consider an $n \times n$ matrix A, written by

$$A = \begin{bmatrix} \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_n \end{bmatrix}.$$

The "rule" is that *subtracting the ith row of A by a scalar multiple of another row of A does not affect the determinant.* More specifically, fix a $i = 1, \ldots, n$, and let $j = 1, \ldots, n$ with $j \neq i$. Let $c \in \mathbb{R}$. Then,

$$\begin{aligned}
\det \begin{bmatrix} \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_i - c\boldsymbol{r}_j \\ \vdots \\ \boldsymbol{r}_j \\ \vdots \\ \boldsymbol{r}_n \end{bmatrix} &= \det \begin{bmatrix} \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_i \\ \vdots \\ \boldsymbol{r}_j \\ \vdots \\ \boldsymbol{r}_n \end{bmatrix} - c \det \begin{bmatrix} \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_j \\ \vdots \\ \boldsymbol{r}_j \\ \vdots \\ \boldsymbol{r}_n \end{bmatrix} && \text{(Proposition 1.8.c)} \\
&= \det A - c(0) && \text{(Corollary 1.8.b)} \\
&= \det A.
\end{aligned}$$

For convenience, we denote this subtraction by $-c\boldsymbol{r}_j + \boldsymbol{r}_i \to \boldsymbol{r}_i$ ("adding $-c$ times the jth row to the ith row, and putting the result in the ith row"). This kind of notation will be useful in Section 2.

Remarks:

- This "rule" is usually used to create many zeros in a column, so that performing cofactor expansion along that column is simple.
- This also applies similarly for columns, by utilizing the corresponding properties for columns.

Example:

$$\begin{aligned}
\begin{vmatrix} 1 & 0 & 1 & 1 \\ 2 & 1 & 3 & 1 \\ 3 & 1 & -2 & 1 \\ -1 & 1 & 1 & 2 \end{vmatrix} &= \begin{vmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -3 \\ 0 & 1 & -5 & -2 \\ 0 & 1 & 2 & 3 \end{vmatrix} && (-2\boldsymbol{r}_1 + \boldsymbol{r}_2 \to \boldsymbol{r}_2,\ -3\boldsymbol{r}_1 + \boldsymbol{r}_3 \to \boldsymbol{r}_3, \text{ and } \boldsymbol{r}_1 + \boldsymbol{r}_4 \to \boldsymbol{r}_4) \\
&= 1 \begin{vmatrix} 1 & 1 & -3 \\ 1 & -5 & -2 \\ 1 & 2 & 3 \end{vmatrix} && \text{(cofactor expansion along the first column)} \\
&= \begin{vmatrix} 1 & 1 & -3 \\ 0 & -6 & 1 \\ 0 & 1 & 6 \end{vmatrix} && (-\boldsymbol{r}_1 + \boldsymbol{r}_2 \to \boldsymbol{r}_2 \text{ and } -\boldsymbol{r}_1 + \boldsymbol{r}_3 \to \boldsymbol{r}_3) \\
&= 1 \begin{vmatrix} -6 & 1 \\ 1 & 6 \end{vmatrix} && \text{(cofactor expansion along the first column)} \\
&= -36 - 1 = -37.
\end{aligned}$$

1.9 Matrix Inverses

1.9.1 The (multiplicative) *inverse* of a real number a is a real number b such that $ab = 1$, which is denoted by a^{-1}. [Note: The inverse may not exist. For example, 0 does not have an inverse.]

We have a similar notion for matrices.

1.9.2 An $n \times n$ matrix A is **invertible** (or **non-singular**[4]) if there exists an $n \times n$ matrix B such that $AB = BA = I_n$. The matrix B is is called the **inverse** of A, and is denoted by A^{-1}. A matrix with no inverse is called **non-invertible** (or **singular**).

Remarks:

- We only define invertibility for *square matrices*.
- Compared with the notion of inverse for real numbers, there is an extra condition: $AB = BA$ (which may not hold due to the non-commutativity of matrix multiplication). But it turns out that if we have either $AB = I_n$ or $BA = I_n$, then another one would automatically hold[5]). So, to prove invertibility we actually only need to show one of the equalities.

1.9.3 Like the case for real numbers, the matrix inverse is unique (if exists).

Proposition 1.9.a. Let A be an $n \times n$ matrix. Then, the inverse of A, if exists, must be unique.

Proof. Suppose that B and C are inverses of A. Then, by definition we have

$$AB = BA = AC = CA = I_n.$$

This implies

$$B = BI_n = B(AC) = (BA)C = I_nC = C,$$

establishing the uniqueness. □

1.9.4 It turns out that there is a special relationship between *invertibility* and *determinant*. One main result we would like to prove in Section 1.9 is that a matrix A is invertible *if and only if* $\det A \neq 0$.

1.9.5 Proving the "only if" direction is not too hard:

Proposition 1.9.b. Let A be an invertible $n \times n$ matrix. Then, $\det A \neq 0$. Furthermore, we have

$$\det\left(A^{-1}\right) = \frac{1}{\det A}.$$

Proof. Since A is invertible, we have $AA^{-1} = I_n$. Now, taking determinant gives

$$\det\left(AA^{-1}\right) = \det I_n = 1 \implies (\det A)(\det\left(A^{-1}\right)) = 1.$$

This implies $\det A \neq 0$ (otherwise the product would be 0, rather than 1). Hence, by rearranging the equation we have

$$\det\left(A^{-1}\right) = \frac{1}{\det A}.$$

□

1.9.6 On the other hand, proving the "if" direction is much more involved. We first define a related notion: *adjugate matrix*. Let A be an $n \times n$ matrix. Then, the **adjugate** of A, denoted by $\operatorname{adj} A$, is the *transpose* of the cofactor matrix of A: $C = [C_{ij}]$ with $C_{ij} = (-1)^{i+j} \det \widetilde{A}_{ij}$ for any $i, j = 1, \ldots, n$, i.e.,

$$\operatorname{adj} A = [C_{ij}]^T.$$

[4]Note that "invertible" corresponds to "non-singular" rather than "singular". We have this terminology since a matrix together with its inverse is like a "couple", so if a matrix *has* inverse, then it is not "singular".

[5]This is asserted by the *invertible matrix theorem*, which gives a series of statements equivalent to invertibility.

1.9.7 An important result for the adjugate matrix is as follows.

Theorem 1.9.c. Let $A = [a_{ij}]$ be an $n \times n$ matrix. Then,

$$A(\operatorname{adj} A) = (\det A)I_n = (\operatorname{adj} A)A.$$

Proof. We prove only the first equality since the second equality can be proved similarly (row $\leftrightarrow$ column, etc.). By definition of matrix multiplication, the (i, j)-entry of $A \operatorname{adj} A$ is

$$a_{i1}C_{j1} + \cdots + a_{1n}C_{jn}.$$

When $i = j$, this equals $\det A$ by the cofactor expansion theorem (Theorem 1.7.a). Now consider the case where $i \neq j$. Let A' be the matrix obtained from A by replacing its jth row by its ith row, i.e.,

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & \ddots & \vdots \\ a_{j1} & \cdots & a_{jn} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \to A' = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & \ddots & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}.$$

Since A' has two identical rows, we have $\det A' = 0$. On the other hand, by considering cofactor expansion of A' along jth row (which equals the original ith row of A, yet positioned at jth row), we see that the (i, j)-entry of $A \operatorname{adj} A$, namely $a_{i1}C_{j1} + \cdots + a_{1n}C_{jn}$, is indeed $\det A' = 0$. Thus, we can conclude that the (i, j)-entry of $A \operatorname{adj} A$ is 0 when $i \neq j$.

Hence, we have $A \operatorname{adj} A = (\det A)I_n$. □

1.9.8 The following corollary shows the "if" direction.

Corollary 1.9.d. Let A be an $n \times n$ matrix with $\det A \neq 0$. Then, A is invertible and

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

Proof. By Theorem 1.9.c, we have

$$A(\operatorname{adj} A) = (\det A)I_n = (\operatorname{adj} A)A.$$

Since $\det A \neq 0$, we can rewrite this as

$$A\left(\frac{1}{\det A} \operatorname{adj} A\right) = I_n = \left(\frac{1}{\det A} \operatorname{adj} A\right)A.$$

By definition, this means that A is invertible and

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

□

1.9.9 With Proposition 1.9.b and Corollary 1.9.d, we can prove our desired result about matrix invertibility and determinant:

Theorem 1.9.e. An $n \times n$ matrix A is invertible if and only if $\det A \neq 0$.

Proof. It follows from Proposition 1.9.b ("only if") and Corollary 1.9.d ("if"). □

1.9.10 Lastly, we introduce some properties regarding matrix inverse.

Proposition 1.9.f. Let A and B be invertible $n \times n$ matrices. Let $c \neq 0$. Then,

(a) $(AB)^{-1} = B^{-1}A^{-1}$;

(b) $(cA)^{-1} = c^{-1}A^{-1}$;

(c) $(A^T)^{-1} = (A^{-1})^T$;

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

Proof.

(a) Note that
$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n.$$

(b) Note that
$$(c^{-1}A^{-1})(cA) = c^{-1}cA^{-1}A = (1)I_n = I_n.$$

(c) Note that
$$(A^{-1})^TA^T = (AA^{-1})^T = I_n.$$

(d) Note that
$$A(A^{-1}) = I_n,$$
so A serves as the inverse of A^{-1}.

□

2 Systems of Linear Equations

2.1 Basic Notions and Methods for Systems of Linear Equations

2.1.1 A **system of m linear equations in n unknowns** (or **variables**) $x_1, , \dots, x_n$ is a family of equations of the form

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

where a_{ij}'s and b_k's are some real constants.

2.1.2 For the system in [2.1.1], the $m \times n$ matrix $[a_{ij}]$ is called the **coefficient matrix** of the system, while the matrix

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

is called the **augmented matrix** of the system.

[Note: The vertical line only serves for decorational purpose (entries on its right are the values appearing on the right of "=" in the system), and it does not affect the nature of the matrix, i.e., the vertical line can be ignored when interpreting the matrix.]

2.1.3 Writing $A = [a_{ij}]$, $\boldsymbol{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, and $\boldsymbol{b} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$, the system in [2.1.1] can be rewritten simply as

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

Then, we can observe that solving the system is just the same as solving this matrix equation. Hence, a *solution* to the system is just a column vector $\boldsymbol{v} \in \mathbb{R}^m$ such that $A\boldsymbol{v} = \boldsymbol{b}$. The **solution set** of the system is the set $\{\boldsymbol{v} \in \mathbb{R}^m : A\boldsymbol{v} = \boldsymbol{b}\}$, i.e., the set of all solutions to the system.

2.1.4 Next, we will introduce two approaches for solving a system of linear equations. The first one is related to the matrix inverse, and is applicable when the coefficient matrix A is an *invertible square matrix.*

To solve the system $A\boldsymbol{v} = \boldsymbol{b}$, multiplying both sides by A^{-1} gives

$$\boldsymbol{x} = A^{-1}A\boldsymbol{x} = \boxed{A^{-1}\boldsymbol{b}}.$$

This suggests a way of solving the system. Furthermore, we have the following result which guarantees the *uniqueness* of the solution in this case.

Proposition 2.1.a. Let A be an $n \times n$ *invertible* matrix and let $\boldsymbol{b} \in \mathbb{R}^n$ be a column vector. Then, the system of linear equations $A\boldsymbol{x} = \boldsymbol{b}$ must have a unique solution.

Proof. This follows from the uniqueness of matrix inverse. Particularly, the unique solution is given by $\boldsymbol{x} = A^{-1}\boldsymbol{b}$. □

2.1.5 Another approach for solving a system of linear equations is also only applicable when A is an invertible square matrix. However, it often requires fewer computations than the matrix inverse approach, and so is more frequently used. It is known as *Cramer's rule*:

Theorem 2.1.b (Cramer's rule)**.** Let A be an $n \times n$ invertible matrix and let $\boldsymbol{b} \in \mathbb{R}^n$ be a column vector. Then, the (unique) solution of the system

$$A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \boldsymbol{b}$$

is given by

$$x_i = \frac{\det A_i}{\det A}$$

where A_i is the matrix obtained by replacing the ith column of A by $\boldsymbol{b}$, for any $i = 1, \dots, n$.

Proof. By Corollary 1.9.d, we have

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

We also know that the solution of the system is $\boldsymbol{x} = A^{-1}\boldsymbol{b}$, so it suffices to show that for any $i = 1, \dots, n$,

$$\frac{\det A_i}{\det A} = \left(\frac{1}{\det A} (\operatorname{adj} A)\boldsymbol{b} \right)_{i1},$$

or

$$\det A_i = [(\operatorname{adj} A)\boldsymbol{b}]_{i1},$$

where RHS denotes the $(i, 1)$-entry of the $n \times 1$ matrix $(\operatorname{adj} A)\boldsymbol{b}$.

First fix any $i = 1, \dots, n$. By the definition of matrix multiplication,

$$[(\operatorname{adj} A)\boldsymbol{b}]_{i1} = C_{1i}b_1 + \cdots + C_{ni}b_n$$

where $C_{ji} = (-1)^{j+i}\widetilde{A}_{ji}$ is the (j, i)-cofactor of A. On the other hand, performing cofactor expansion for $\det A_i$ along the ith column gives also

$$\det A_i = b_1 C_{1i} + \cdots + b_n C_{ni}.$$

This shows the desired equality. ∎

2.2 Elementary Row Operations

2.2.1 To motivate the concept of *elementary row operations*. Consider the following system:

$$\begin{cases} x_1 + x_2 = 3 \\ \phantom{x_1 + {}} x_2 = 2 \end{cases}$$

It is straightforward to solve this system since we can simply put $x_2 = 2$ into the first equation to get $x_1 = 1$. However, a system is generally not that easy to solve, and this leads us to consider some systematic methods to "transform" an arbitrary system into a "simple" system like the above one. It turns out that it is possible by performing the so-called *elementary row operations*.

2.2.2 There are three types of **elementary row operations** (EROs) to be performed on a matrix:

- **type I ERO**: interchanging two different rows
- **type II ERO**: multiply a row by a *nonzero* scalar
- **type III ERO**: adding a scalar multiple of a row to another row

Here, we shall use $\boldsymbol{r}_1, \boldsymbol{r}_2, \dots, \boldsymbol{r}_m$ to denote the m rows of an $m \times n$, from top to bottom. We have the following notations for the three types of EROs:

- (type I) $\boldsymbol{r}_i \leftrightarrow \boldsymbol{r}_j$: interchanging the ith and the jth row ("putting $\boldsymbol{r}_i$ to the jth row $\boldsymbol{r}_j$, and putting $\boldsymbol{r}_j$ to the ith row $\boldsymbol{r}_i$")
- (type II) $k\boldsymbol{r}_i \to \boldsymbol{r}_i$: multiplying the ith row by a *nonzero* scalar k ("putting $k\boldsymbol{r}_i$ back to the ith row $\boldsymbol{r}_i$")
- (type III) $k\boldsymbol{r}_j + \boldsymbol{r}_i \to \boldsymbol{r}_i$: adding k times the jth row to the ith row ("putting $k\boldsymbol{r}_j + \boldsymbol{r}_i$ to the ith row $\boldsymbol{r}_i$")

2.3 Elementary Matrices

2.3.1 To utilize the results for *matrices* in Section 1 for EROs, we need to find a way to associate each ERO with a *matrix*. It turns out that *elementary matrices* are able to capture the essence of EROs.

2.3.2 An **elementary matrix** is a square matrix obtained by performing *exactly one* ERO on an identity matrix. An elementary matrix is of type I, II, or III if the ERO performed on the identity matrix is of type I, II, or III respectively.

Examples:

- $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is a type I elementary matrix.
- $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is a type II elementary matrix.
- $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ is a type III elementary matrix.

2.3.3 The following theorem suggests the connection between elementary matrix and ERO:

Theorem 2.3.a. Let A be an $m \times n$ matrix. If B is obtained from A by performing an ERO, then there exists an $m \times m$ elementary matrix E such that $B = EA$, and the matrix E can be obtained by performing the same ERO on I_m.

Conversely, if E is an $m \times m$ elementary matrix, then EA is the matrix obtained from A by performing the ERO corresponding to E.

2.3.4 An important property of elementary matrix is *invertibility*:

Proposition 2.3.b. Elementary matrices are invertible. Furthermore, the inverse of an elementary matrix is an elementary matrix of the same type.

Proof. It follows from Theorem 2.3.a and the property that the effect from any ERO can be cancelled out by performing an ERO of the same type. More explicitly, the reverse processes of all kinds of ERO are given as follows.

- The reverse process of $\boldsymbol{r}_i \leftrightarrow \boldsymbol{r}_j$ is $\boldsymbol{r}_i \leftrightarrow \boldsymbol{r}_j$.
- The reverse process of $c\boldsymbol{r}_i \to \boldsymbol{r}_i$ is $\frac{1}{c}\boldsymbol{r}_i \to \boldsymbol{r}_i$. (Note that $c \neq 0$.)
- The reverse process of $c\boldsymbol{r}_j + \boldsymbol{r}_i \to \boldsymbol{r}_i$ is $-c\boldsymbol{r}_j + \boldsymbol{r}_i \to \boldsymbol{r}_i$.

$\square$

2.4 (Reduced) Row Echelon Form

2.4.1 Recall the simple-to-solve system in [2.2.1]:

$$\begin{cases} x_1 + x_2 = 3 \\ \phantom{x_1 + {}} x_2 = 2 \end{cases}$$

In augmented matrix form, it can be expressed as

$$\left[\begin{array}{cc|c} 1 & 1 & 3 \\ 0 & 1 & 2 \end{array}\right].$$

Consider yet another simple-to-solve system of three equations:

$$\begin{cases} x_1 \qquad + 2x_3 = 3 \\ \qquad x_2 + \ \ x_3 = 2 \\ \qquad\qquad\quad x_3 = 1 \end{cases}.$$

The corresponding augmented matrix is

$$\left[\begin{array}{ccc|c} 1 & 0 & 2 & 3 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 \end{array}\right].$$

A common feature for these augmented matrices of these simple-to-solve systems is that there appears to be a "triangle of zeros" located at the lower left corner. We can observe that if the augmented matrix of a system has this kind of nice "format", then the system is quite easy to solve.

2.4.2 To formalize this notion, we introduce the concept of *row echelon form*. A matrix is said to be in **row echelon form** (REF) if the following conditions are all satisfied:

- All rows having only zero entries (called **zero rows**), if any, lie at the bottom of the matrix (i.e., below every nonzero row).
- The **leading entry** (i.e., the leftmost nonzero entry) in a nonzero row is on the right of the leading entry of every row above.

Examples and non-examples:

- $\left[\begin{array}{cc|c} 1 & 1 & 3 \\ 0 & 1 & 2 \end{array}\right]$ is in REF.
- $\left[\begin{array}{ccc|c} 1 & 0 & 2 & 3 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 \end{array}\right]$ is in REF.
- $\left[\begin{array}{cc|c} 1 & 1 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{array}\right]$ is in REF.
- $\left[\begin{array}{cc|c} 1 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 1 & 2 \end{array}\right]$ is *not* in REF. This is because the zero row (second row) is not at the bottom of the matrix.
- $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ is in REF.
- I_n and any zero matrix are in REF.
- $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ is *not* in REF. This is because the leading entry 1 in the third row is not on the right of the leading entry 2 in the second row.

2.4.3 Consider the following system

$$\begin{cases} x_1 \qquad\qquad = 3 \\ \qquad x_2 \qquad = 2 \\ \qquad\qquad x_3 = 1 \end{cases}.$$

Its augmented matrix is

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{array}\right].$$

It is very straightforward to obtain the solution to this system. Indeed, in this case we can even directly "read out" the solution. Hence, we would also like to introduce a notion to describe this kind of *very* easy-to-solve system. It is known as *reduced row echelon form*.

2.4.4 A matrix is said to be in **reduced row echelon form** (RREF) if it is in REF with the following additional conditions satisfied:

- The leading entry of every nonzero row is 1 (called **leading one**).
- For each leading one, all other entries in the same column are 0.

Examples and non-examples:

- $\left[\begin{array}{ccc|c} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{array}\right]$ is in RREF.
- $\left[\begin{array}{cc|c} 1 & 1 & 3 \\ 0 & 1 & 2 \end{array}\right]$ is *not* in RREF.
- $\begin{bmatrix} 1 & 2 & 0 & 4 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ is in RREF.
- $\begin{bmatrix} 1 & 0 & 3 \\ 0 & 0 & 1 \end{bmatrix}$ is *not* in RREF.
- I_n and any zero matrix are in RREF.

2.4.5 Apart from the practical application of solving systems of linear equations, the concept of RREF is also useful *theoretically*. It turns that for a square matrix in RREF, there are some extra criteria for matrix invertibility:

Theorem 2.4.a. Let A be an $n \times n$ matrix in RREF. Then the following statements are equivalent.

(a) A is invertible.

(b) A has n leading ones.

(c) $A = I_n$.

Proof. To prove statements of this form, a method is to prove a "cycle of implications" (logically speaking). Here we will prove that (a) $\implies$ (b) $\implies$ (c) $\implies$ (a).

<u>(a) $\implies$ (b)</u>: Assume that A is invertible. Then, there must be no zero row in A; otherwise, performing cofactor expansion along the zero row suggests that $\det A = 0$, which means A is not invertible, contradiction. Hence, each row must have a leading one, and so A has n leading ones in total.

<u>(b) $\implies$ (c)</u>: Assume that A has n leading ones. Since A has n rows, it implies that each row of A has a leading one. Now, as A is in RREF, the leading ones have to occupy all the diagonal entries, thus all non-diagonal entries are zero. So, A must be I_n.

<u>(c) $\implies$ (a)</u>: It follows from the fact that I_n is invertible. $\square$

2.5 Gaussian Elimination

2.5.1 As noted previously, one can solve a system whose augmented matrix is in RREF very easily. It turns out that there is a systematic method for "converting"/"reducing" *any* system of linear equations into a system whose augmented matrix is in RREF. This is known as *Gaussian elimination*, which is an important tool for solving a system of linear equation.

2.5.2 But before discussing Gaussian elimination, we first introduce a preliminary notion: *row equivalence*. For two $m \times n$ matrices A and B, the matrix A is said to be **row equivalent** to B if there exist elementary matrices $E_1, \ldots, E_k$ such that $E_k \cdots E_1 A = B$ (or equivalently, B can be obtained from A by performing some EROs).

2.5.3 Row equivalence is indeed an *equivalence relation* in mathematical sense. To see this, consider the following. (A, B, and C denote arbitrary matrices below.)

- reflexive: A is row equivalent to A. For example, we can interchange two rows of A twice to get back A.
- symmetric: Suppose that A is row equivalent to B, i.e., $E_k \cdots E_1 A = B$ for some elementary matrices $E_1, \ldots, E_k$. Since the inverse of any elementary matrix exists and is also elementary, by writing
$$A = E_1^{-1} \cdots E_k^{-1} B,$$
we see that B is row equivalent to A.
- transitive: Assume that A is row equivalent to B, and B is row equivalent to C. Then, we have
$$E_k \cdots E_1 A = B \quad \text{and} \quad F_\ell \cdots F_1 B = C$$
for some elementary matrices $E_1, \ldots, E_k, F_1, \ldots, F_\ell$. But then we can write
$$F_\ell \cdots F_1 E_k \cdots E_1 A = C,$$
so A is row equivalent to C.

2.5.4 An important result that serves as the foundation for the Gaussian elimination is the following.

Theorem 2.5.a. Let $A\boldsymbol{x} = \boldsymbol{b}$ and $A'\boldsymbol{x} = \boldsymbol{b}'$ be two systems of linear equations with the same number of equations and the same number of variables. If the augmented matrices $[A|\boldsymbol{b}]$ and $[A'|\boldsymbol{b}']$ are *row equivalent*, then the two systems have the same solution set.

Proof. By row equivalence, there exist elementary matrices $E_1, \ldots, E_k$ such that
$$E_k \cdots E_1 [A|\boldsymbol{b}] = [A'|\boldsymbol{b}'].$$
By block multiplication, we can write
$$[E_k \cdots E_1 A | E_k \cdots E_1 \boldsymbol{b}] = [A'|\boldsymbol{b}'],$$
which implies that $A' = E_k \cdots E_1 A$ and $\boldsymbol{b}' = E_r \cdots E_1 \boldsymbol{b}$.

To prove that the two systems have the same solution set, it suffices to prove the logical equivalence $A\boldsymbol{v} = \boldsymbol{b} \iff A'\boldsymbol{v} = \boldsymbol{b}'$.

"$\Rightarrow$": Assume that $A\boldsymbol{v} = \boldsymbol{b}$. Then, multiplying $E_k \cdots E_1$ on both sides gives
$$E_k \cdots E_1 A\boldsymbol{v} = E_k \cdots E_1 \boldsymbol{b},$$
thus $A'\boldsymbol{v} = \boldsymbol{b}'$.

"$\Leftarrow$": Assume that $A'\boldsymbol{v} = \boldsymbol{b}'$. Then, we have
$$E_k \cdots E_1 A\boldsymbol{v} = E_k \cdots E_1 \boldsymbol{b}.$$
Since elementary matrices are invertible, we have
$$E_1^{-1} \cdots E_k^{-1} E_k \cdots E_1 A\boldsymbol{v} = E_1^{-1} \cdots E_k^{-1} E_k \cdots E_1 \boldsymbol{b},$$
which implies $A\boldsymbol{v} = \boldsymbol{b}$. □

2.5.5 A corollary of Theorem 2.5.a is the following *column correspondence property*. Loosely, it suggests that there are identical "linear relationships" between *columns* for two row equivalent matrices.

Corollary 2.5.b (Column correspondence property)**.** Let A and B be two $m \times n$ matrices that are row equivalent. Write $A = \begin{bmatrix} \boldsymbol{a}_1 & \cdots & \boldsymbol{a}_n \end{bmatrix}$ and $B = \begin{bmatrix} \boldsymbol{b}_1 & \cdots & \boldsymbol{b}_n \end{bmatrix}$. Then,

$$c_1\boldsymbol{a}_1 + \cdots + c_n\boldsymbol{a}_n = \mathbf{0} \iff c_1\boldsymbol{b}_1 + \cdots + c_n\boldsymbol{b}_n = \mathbf{0}$$

where $c_1, \ldots, c_n$ are some constants.

Proof. It follows from Theorem 2.5.a with $\boldsymbol{b} = \boldsymbol{b}' = \mathbf{0}$ and $B = A'$. □

2.5.6 Given a matrix A, the **RREF of A** is a matrix in RREF that is row equivalent to A.

Due to Theorem 2.5.a, our main goal here is to find a RREF of the given augmented matrix, so that solving the underlying system is easy afterwards. *Gaussian elimination* provides a method for finding it systematically.

2.5.7 The **Gaussian elimination** is a standard procedure for obtaining RREF of a matrix as follows.

(1) Identify the leftmost nonzero column.

(2) Make the top entry of this column (called the **pivot position**) nonzero by a type I ERO (if needed).

(3) Make the entries below the pivot position zero by type III EROs (if needed).

(4) Ignore the row containing the pivot position and all rows above, and focus on the submatrix remaining.

(5) Repeat (1)–(4) as long as there is a nonzero row in the remained submatrix.

(6) Make the last pivot position 1 by a type II ERO (if needed).

(7) Make all entries in the same column as this pivot position 0 by type III EROs (if needed).

(8) Repeat (6)–(7) with the rows above, until all rows have been handled.

2.5.8 Example of Gaussian elimination: Consider an augmented matrix $A = \left[\begin{array}{ccc|c} 0 & 0 & 1 & 2 \\ 2 & 2 & 4 & 6 \\ 1 & 0 & 1 & 1 \end{array}\right]$.

$$\left[\begin{array}{ccc|c} 0 & 0 & 1 & 2 \\ 2 & 2 & 4 & 6 \\ 1 & 0 & 1 & 1 \end{array}\right]$$

$$(1) \quad \left[\begin{array}{ccc|c} 0 & 0 & 1 & 2 \\ 2 & 2 & 4 & 6 \\ 1 & 0 & 1 & 1 \end{array}\right]$$

$$(2) \quad \xrightarrow{\boldsymbol{r}_1 \leftrightarrow \boldsymbol{r}_2} \left[\begin{array}{ccc|c} 2 & 2 & 4 & 6 \\ 0 & 0 & 1 & 2 \\ 1 & 0 & 1 & 1 \end{array}\right]$$

$$(3) \quad \xrightarrow{-\frac{1}{2}\boldsymbol{r}_1 + \boldsymbol{r}_3 \to \boldsymbol{r}_3} \left[\begin{array}{ccc|c} 2 & 2 & 4 & 6 \\ 0 & 0 & 1 & 2 \\ 0 & -1 & -1 & -2 \end{array}\right]$$

$$(4) \quad \left[\begin{array}{ccc|c} 2 & 2 & 4 & 6 \\ 0 & 0 & 1 & 2 \\ 0 & -1 & -1 & -2 \end{array}\right]$$

$$(1) \quad \left[\begin{array}{ccc|c} 2 & 2 & 4 & 6 \\ 0 & 0 & 1 & 2 \\ 0 & -1 & -1 & -2 \end{array}\right]$$

$$(2) \quad \xrightarrow{\boldsymbol{r}_2 \leftrightarrow \boldsymbol{r}_3} \left[\begin{array}{ccc|c} 2 & 2 & 4 & 6 \\ 0 & -1 & -1 & -2 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

$$(3) \quad \left[\begin{array}{ccc|c} 2 & 2 & 4 & 6 \\ 0 & -1 & -1 & -2 \\ 0 & 0 & 1 & 2 \end{array}\right] \checkmark$$

$$(4) \quad \left[\begin{array}{ccc|c} 2 & 2 & 4 & 6 \\ 0 & -1 & -1 & -2 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

$$(1) \quad \left[\begin{array}{ccc|c} 2 & 2 & 4 & 6 \\ 0 & -1 & -1 & -2 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

$$(4) \quad \left[\begin{array}{ccc|c} 2 & 2 & 4 & 6 \\ 0 & -1 & -1 & -2 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

$$(6) \qquad \left[\begin{array}{ccc|c} 2 & 2 & 4 & 6 \\ 0 & -1 & -1 & -2 \\ 0 & 0 & 1 & 2 \end{array}\right] \checkmark$$

$$(7) \qquad \xrightarrow{\substack{-4\boldsymbol{r}_3+\boldsymbol{r}_1\to\boldsymbol{r}_1 \\ \boldsymbol{r}_3+\boldsymbol{r}_2\to\boldsymbol{r}_2}} \left[\begin{array}{ccc|c} 2 & 2 & 0 & -2 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

$$\left[\begin{array}{ccc|c} 2 & 2 & 0 & -2 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

$$(6) \qquad \xrightarrow{-\boldsymbol{r}_2\to\boldsymbol{r}_2} \left[\begin{array}{ccc|c} 2 & 2 & 0 & -2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

$$(7) \qquad \xrightarrow{-2\boldsymbol{r}_2+\boldsymbol{r}_3\to\boldsymbol{r}_3} \left[\begin{array}{ccc|c} 2 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

$$\left[\begin{array}{ccc|c} 2 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

$$(6) \qquad \xrightarrow{\frac{1}{2}\boldsymbol{r}_1\to\boldsymbol{r}_1} \left[\begin{array}{ccc|c} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{array}\right].$$

Hence, the RREF of A is given by:

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{array}\right].$$

This suggests that the solution to the underlying system is given by $x_1 = -2$, $x_2 = 0$, and $x_3 = 2$.

2.5.9 Gaussian elimination ensures the *existence* of RREF of any given matrix A, since this standard procedure can be applied to any matrix A to obtain a matrix in RREF that is row equivalent to A. Expressing this fact using elementary matrices, we can say that there always exist elementary matrices $E_1, \ldots, E_k$ such that

$$R = E_k \cdots E_1 A$$

where R is a RREF of A. Naturally, one would then ask whether such RREF of A is *unique*. It turns out that it is indeed unique:

Theorem 2.5.c. Every $m \times n$ matrix A has a unique RREF.

Proof. (Sketch) The existence of RREF of A is guaranteed by Gaussian elimination. So it suffices to prove the uniqueness part.

We may prove this by induction on n (the number of columns). The result holds when $n = 1$, since there are only two possible $m \times 1$ matrices in RREF:

$$\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Note that the leading one must be at the first row for the former matrix, so that all zero rows lie at the bottom of the matrix. It is then not hard to see that the unique RREF of any nonzero $m \times 1$ matrix is the former one, and the unique RREF of the zero $m \times 1$ matrix is the latter one (itself).

Now, assume the result holds when $n = k$, for some $k \in \mathbb{N}$. Let R_1 and R_2 be two RREFs of A. Let A', R_1', and R_2' denote the matrix obtained by removing the last column of A, R_1, and R_2 respectively.

Claim: R_1' and R_2' are two RREFs of A'.

Proof. First of all, it is easy to see that R_1' and R_2' are both row equivalent to A', since R_1' and R_2' can be obtained by the respective EROs performed to get R_1 and R_2 from A.

It then suffices to show that R_1' and R_2' are in RREF. WLOG, we focus on R_1'. When R is in RREF, we have the following cases.

- Case 1: All the leading ones are *not* at the last column of R.
  In this case, removing the last column still retains all leading ones, and every zero row (if exists) still remains as a zero row. The leading ones still satisfy with the requirements imposed by RREF as they are not affected by the removal.
- Case 2: The last column of R contains a leading one.
  Since R is in RREF, every row below the row with leading one at the last column (if exists) must be zero row. So, after removing the last column, the original row with leading one at the last column becomes a zero row (and of course every original zero row, if exists, is still a zero row). Similarly, the other leading ones are not affected by the removal, and so still satisfy the requirements from RREF.

$\square$

Then, the induction hypothesis implies that $R_1' = R_2'$. Next, we can show that the last columns of R_1 and R_2 are also the same by using Corollary 2.5.b. $\square$

2.5.10 The RREF of a square matrix can provide information on the invertibility of the square matrix, as suggested by the following result.

Proposition 2.5.d. Let A be an $n \times n$ matrix. Then A is invertible iff the RREF of A is invertible.

Proof. Let R be the RREF of A. Then, we can write

$$R = E_k \cdots E_1 A$$

for some elementary matrices $E_1, \ldots, E_k$. Now we consider *determinant*. Since elementary matrices are invertible, $\det E_i \neq 0$ for any $i = 1, \ldots, k$. Thus, by multiplicativity of determinant we have

$$\det R = (\text{nonzero constant}) \times \det A.$$

This then suggests that $\det A = 0$ iff $\det R = 0$, so the desired result follows. $\square$

2.5.11 Since Gaussian elimination allows us to convert an arbitrary matrix to its RREF, it gives us a general and systematic algorithm for solving a system of linear equations (*assuming that the system has a solution*) as follows.

(a) Given a system of linear equations $A\boldsymbol{x} = \boldsymbol{b}$, consider its associated augmented matrix $[A|\boldsymbol{b}]$. Using Gaussian elimination, we can find its RREF, denoted by $[A'|\boldsymbol{b}']$. [Note: By the claim in the proof of Theorem 2.5.c, A' is indeed the RREF of A.]

(b) Every variable in the system corresponding to a leading entry of $[A'|\boldsymbol{b}']$ is called a **leading variable** (or **basic variable**). Every other variable in the system is known as **free variable**.

(c) Set the free variables (if any) as arbitrary values, and then obtain the solutions for leading variables based on the RREF $[A'|\boldsymbol{b}']$, possibly in terms of the free variables.

[Note: The solution set obtained is sometimes called the **general solution** of the system (especially when some free variables are involved).]

2.6 Number of Solutions for Systems of Linear Equations

2.6.1 In [2.5.11], we have assumed the system has a solution. But in general, a system of linear equations may have no solution, e.g.

$$\begin{cases} 0x_1 + 0x_2 = 1 \\ \ \ x_1 + \ \ x_2 = 2 \end{cases}$$

has no solution. So, we are interested in finding some ways to determine the number of solutions for a system.

2.6.2 A system of linear equations is **consistent** if it has at least one solution. Otherwise, the system is called **inconsistent**. The following theorem provides a criterion of (in)consistency, using the notion of RREF.

Theorem 2.6.a. *A system of linear equations $A\boldsymbol{x} = \boldsymbol{b}$ is inconsistent iff the RREF of the augmented matrix $[A|\boldsymbol{b}]$ has a leading one in the last column.*

Proof. "$\Leftarrow$": When the RREF has a leading one in the last column, it means that a certain row of the RREF is

$$\begin{bmatrix} 0 & 0 & \cdots & 0|1 \end{bmatrix},$$

which implies that there is no solution.

"$\Rightarrow$": We prove by contrapositive. Assume that the RREF of $[A|\boldsymbol{b}]$ does not have any leading one in the last column. Then, for every row with a leading one, we can obtain an expression for the corresponding leading variable (possibly in terms of free variables).[6] After setting the free variables (if any) as arbitrary values, we would obtain a solution for the system, so the system is consistent. ☐

2.6.3 When we know the exact distribution of leading ones, we can say even more.

Corollary 2.6.b. *A system of linear equations $A\boldsymbol{x} = \boldsymbol{b}$ has a unique solution iff the RREF of the augmented matrix $[A|\boldsymbol{b}]$ has a leading one in each column except the last one.*

Proof. "$\Leftarrow$": Assume that the RREF has a leading one in each column except the last one. Then by Theorem 2.6.a, the system is consistent. Furthermore, by having a leading one in each column except the last one, there must be no free variable, so the solution is unique.

"$\Rightarrow$": Assume that the system has a unique solution. Then, the system is consistent, thus there is no leading one in the last column by Theorem 2.6.a. Furthermore, due to the uniqueness of solution, the system cannot possibly have any free variable. Hence, every other column must have a leading one. ☐

2.6.4 After deducing that a system is consistent, we would like to know the *number* of solutions it has. Of course when the coefficient matrix is invertible or when the RREF of the augmented matrix has a leading one in each column except the last one, the system would have a unique solution, by Proposition 2.1.a or Corollary 2.6.b respectively.

But this is not necessarily the case, and it is possible to have *infinitely many* solutions. For example, the system

$$\begin{cases} \ \ x_1 + \ \ x_2 = 0 \\ 2x_1 + 2x_2 = 0 \end{cases}$$

has infinitely many solutions. The solution set is $\{(t, -t) : t \in \mathbb{R}\}$, which is infinite.

2.6.5 To study the case with infinitely many solutions, an useful notion is *homogeneity*. A system of linear equations $A\boldsymbol{x} = \boldsymbol{b}$ is called **homogeneous** if $\boldsymbol{b} = \boldsymbol{0}$. Note that a homogeneous system is *always* consistent since the zero vector $\boldsymbol{x} = \boldsymbol{0}$ is always a solution (known as **trivial solution**). Every other solution of a homogeneous system, if exists, is called **non-trivial solution**.

[6] Note that such expression would not contain other leading variables since by definition of RREF, all other entries in the same column as leading one are zero.

2.6.6 The following result provides a sufficient condition for a homogeneous system to have infinitely many solutions.

Proposition 2.6.c. Let $A\boldsymbol{x} = \mathbf{0}_n$ be a homogeneous system of m linear equations in n variables. If the number of variables (n) exceeds that of equations (m), then the system has infinitely many solutions.

Proof. Since the augmented matrix of the system is $[A|\mathbf{0}_n]$, its RREF would be of the form $[A'|\mathbf{0}_n]$ for some $m \times n$ matrix A. As $n > m$ and A' can have at most m leading entries, there must be at least one free variable, which must lead to infinitely many solutions (since the system is consistent). □

2.6.7 Utilizing Proposition 2.6.c, we can show a more general result that applies to any consistent system.

Proposition 2.6.d. Let $A\boldsymbol{x} = \boldsymbol{b}$ be a system of m linear equations in n variables. Suppose that $n > m$ and the system is consistent. Let $\boldsymbol{x}_p$ be a *particular solution* of the system, i.e., it satisfies $A\boldsymbol{x}_p = \boldsymbol{b}$. Then, the solution set for the system $A\boldsymbol{x} = \boldsymbol{b}$ is

$$\{\boldsymbol{x}_p + \boldsymbol{y} \in \mathbb{R}^m : A\boldsymbol{y} = \mathbf{0}\}.$$

[Note: Since there are infinitely many $\boldsymbol{y}$ satisfying $A\boldsymbol{y} = \mathbf{0}$ in such case by Proposition 2.6.c, the solution set is infinite, thus the system $A\boldsymbol{x} = \boldsymbol{b}$ has infinitely many solutions as well.]

Proof. Let S be the solution set for the system $A\boldsymbol{x} = \boldsymbol{b}$, i.e., $S = \{\boldsymbol{x} \in \mathbb{R}^m : A\boldsymbol{x} = \boldsymbol{b}\}$. We shall prove the two subset inclusions separately.

$\underline{S \supseteq \{\boldsymbol{x}_p + \boldsymbol{y} \in \mathbb{R}^m : A\boldsymbol{y} = \mathbf{0}\}}$: Fix any $\boldsymbol{x}' \in \{\boldsymbol{x}_p + \boldsymbol{y} \in \mathbb{R}^m : A\boldsymbol{y} = \mathbf{0}\}$. Then, $\boldsymbol{x}' = \boldsymbol{x}_p + \boldsymbol{y}$ for some $\boldsymbol{y}$ satisfying $A\boldsymbol{y} = \mathbf{0}$. Hence,

$$A\boldsymbol{x}' = A(\boldsymbol{x}_p + \boldsymbol{y}) = A\boldsymbol{x}_p + A\boldsymbol{y} = \boldsymbol{b} + \mathbf{0} = \boldsymbol{b},$$

which implies that $\boldsymbol{x}' \in S$.

$\underline{S \subseteq \{\boldsymbol{x}_p + \boldsymbol{y} \in \mathbb{R}^m : A\boldsymbol{y} = \mathbf{0}\}}$: Fix any $\boldsymbol{x}' \in S$. Then, we have $A\boldsymbol{x}' = \boldsymbol{b}$, thus $A(\boldsymbol{x}' - \boldsymbol{x}_p) = \boldsymbol{b} - \boldsymbol{b} = \mathbf{0}$. Hence,

$$\boldsymbol{x}' = \boldsymbol{x}_p + (\boldsymbol{x}' - \boldsymbol{x}_p) \in \{\boldsymbol{x}_p + \boldsymbol{y} \in \mathbb{R}^m : A\boldsymbol{y} = \mathbf{0}\}.$$

□

2.6.8 So far we have seen systems with unique solution or infinitely many solutions. A natural follow-up question is then whether it is possible to have more than one solution but still *finitely* many solutions. It turns out that this is impossible, as suggested by the following result.

Proposition 2.6.e. If a system of linear equations $A\boldsymbol{x} = \boldsymbol{b}$ has more than one solution, then it must have infinitely many solutions.

Proof. Assume that $A\boldsymbol{x} = \boldsymbol{b}$ has more than one solution. Let $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ be two different solutions. Then, we have $A\boldsymbol{x}_1 = \boldsymbol{b}$ and $A\boldsymbol{x}_2 = \boldsymbol{b}$. It follows that $A(\boldsymbol{x}_1 - \boldsymbol{x}_2) = \boldsymbol{b} - \boldsymbol{b} = \mathbf{0}$. Thus, *for any* $t \in \mathbb{R}$, we have

$$A[\boldsymbol{x}_1 + t(\boldsymbol{x}_1 - \boldsymbol{x}_2)] = \boldsymbol{b} + t\mathbf{0} = \boldsymbol{b},$$

so $\boldsymbol{x}_1 + t(\boldsymbol{x}_1 - \boldsymbol{x}_2)$ is also a solution of the system. This then suggests that the system has infinitely many solutions. □

2.6.9 The next result concerns with a homogeneous system with the same numbers of variables and equations.

Proposition 2.6.f. Let A be an $n \times n$ matrix. Then, the following statements are equivalent.

(a) The system $A\boldsymbol{x} = \mathbf{0}$ has a non-trivial solution.

(b) The system $A\boldsymbol{x} = \mathbf{0}$ has infinitely many solutions.

(c) A is *not* invertible.

Proof. Here we will prove that (a) $\implies$ (c) $\implies$ (b) $\implies$ (a).

(a) $\implies$ (c): We prove by contrapositive. Assume that A is invertible. Then by Proposition 2.1.a, the system $A\boldsymbol{x} = \mathbf{0}$ has a *unique* solution. Since the trivial solution must be a solution of the homogeneous system $A\boldsymbol{x} = \mathbf{0}$, it follows that it is the *only* one, thus the system does *not* have a non-trivial solution.

(c) $\implies$ (b): Assume that A is not invertible. Then, the RREF of A, denoted by R, is also *not* invertible by Proposition 2.5.d. Note that the RREF of the augmented matrix $[A|\mathbf{0}]$ can be written as $[R|\mathbf{0}]$. For the "R" part, it follows from the claim in the proof of Theorem 2.5.c. The RHS is still $\mathbf{0}$ since any ERO would have no impact on the column of zeros.

Now, by Theorem 2.4.a, since the $n \times n$ matrix R (in RREF) is not invertible, it must have *less than* n leading ones. This means there are less than n leading entries, implying the existence of *free variable*. It then follows that the system must have infinitely many solutions, as a free variable can take arbitrary values.

(b) $\implies$ (a): It is clear since having infinitely many solutions implies that there are solutions other than the trivial solution, i.e., there is a non-trivial solution. □

2.6.10 Recall that Proposition 2.1.a suggests that invertibility of A implies unique solution. With the help of Proposition 2.6.f, we can prove also the converse, i.e., unique solution implies invertibility of A, provided that A is square.

Proposition 2.6.g. Let A be an $n \times n$ matrix and $\boldsymbol{b} \in \mathbb{R}^n$ be a column vector. If the system $A\boldsymbol{x} = \boldsymbol{b}$ has a unique solution, then A is invertible.

Proof. Assume to the contrary that $A\boldsymbol{x} = \boldsymbol{b}$ has a unique solution $\boldsymbol{x}_0$ while A is not invertible. Then, by Proposition 2.6.f, we know that $A\boldsymbol{x} = \mathbf{0}$ has a non-trivial solution, and we call it $\boldsymbol{y} \neq \mathbf{0}$.

Since $A\boldsymbol{y} = \mathbf{0}$, we would have

$$A(\boldsymbol{x}_0 + \boldsymbol{y}) = A\boldsymbol{x}_0 + A\boldsymbol{y} = \boldsymbol{b} + \mathbf{0} = \boldsymbol{b},$$

implying that $\boldsymbol{x}_0 + \boldsymbol{y} \neq \boldsymbol{x}_0$ is also a solution to the system, in addition to $\boldsymbol{x}_0$. This contradicts the uniqueness. □

2.6.11 Consequently, we obtain yet another criterion for matrix invertibility, in terms of the uniqueness of solution to a system of linear equations.

Proposition 2.6.h. Let A be an $n \times n$ matrix and $\boldsymbol{b} \in \mathbb{R}^n$ be a column vector. The matrix A is invertible iff the system $A\boldsymbol{x} = \boldsymbol{b}$ has a unique solution.

Proof. Combine Proposition 2.1.a and Proposition 2.6.g. □

2.7 Finding Matrix Inverses via Elementary Row Operations

2.7.1 It turns out that EROs are not only useful for solving system of linear equations, but also helpful for *finding matrix inverses*. Indeed, when the sizes of the matrices involved are large, often this ERO-based approach is more computationally feasible than the formula in Corollary 1.9.d.

2.7.2 Before introducing the methods of finding matrix inverses based on EROs, we first prove some theoretical results. The first one provides yet another criterion for invertibility.

Proposition 2.7.a. Let A be an $n \times n$ matrix. Then A is invertible iff the RREF of A is I_n.

Proof. Note that

$$\begin{aligned} & A \text{ is invertible} \\ \iff & \text{RREF of } A \text{ is invertible} && \text{(Proposition 2.5.d)} \\ \iff & \text{RREF of } A \text{ is } I_n && \text{(Theorem 2.4.a).} \end{aligned}$$

□

2.7.3 The next result relates invertible matrix and elementary matrices.

Corollary 2.7.b. Every invertible matrix A is a product of elementary matrices.

Proof. Since A is invertible, by Proposition 2.7.a, the RREF of A is I_n. Then, due to the row equivalence of A and I_n (which is a *symmetric* relation), we have

$$A = E_r \cdots E_1 I_n = E_r \cdots E_1$$

for some elementary matrices $E_1, \ldots, E_r$, as desired. □

2.7.4 Now, we are ready to introduce the method of finding matrix inverse via EROs.

Theorem 2.7.c. Let A be an invertible $n \times n$ matrix. Then the RREF of the $n \times 2n$ augmented matrix $[A|I_n]$ is $[I_n|A^{-1}]$.

Proof. Assume that A is invertible. Then the RREF of A is I_n by Proposition 2.7.a. Hence, we have

$$E_r \cdots E_1 A = I_n \tag{1}$$

for some elementary matrices $E_1, \ldots, E_r$.

Using matrix block multiplication, we have

$$E_r \cdots E_1 [A|I_n] = [E_r \cdots E_1 A | E_r \cdots E_1 I_n] = [I_n | E_r \cdots E_1]$$

From Equation (1), we can further write

$$A = E_1^{-1} \cdots E_r^{-1},$$

so $A^{-1} = E_r \cdots E_1$ by Proposition 1.9.f, as desired. □

<u>Remarks</u>:

- Practically, to get from $[A|I_n]$ to $[I_n|A^{-1}]$, we typically use *Gaussian elimination* on the $n \times 2n$ augmented matrix $[A|I_n]$. (It is not hard to see that $[I_n|A^{-1}]$ is the RREF of $[A|I_n]$.)
- The proof of this result also tells us how to express an invertible matrix as a product of elementary matrices implicitly.

  We first perform Gaussian elimination on $[A|I_n]$ and record the EROs performed. Then, by considering the reverse processes of the EROs (corresponding to the inverses of elementary matrices, which are also elementary), we can write
  $$A = E_1^{-1} \cdots E_r^{-1}.$$

3 Vector Spaces

3.1 Vector Spaces and Vector Subspaces

3.1.1 In Section 3, we will start studying a main object of interest in linear algebra: *vector space*, which *abstractizes* the properties we know in $\mathbb{R}^n$.

3.1.2 A **vector space** over $\mathbb{R}$ (or simply *real* vector space) is a nonempty set V on which two operations, called **vector addition** and **scalar multiplication** are defined such that for any elements $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$ (called **vectors** in V) and any scalars $a, b \in \mathbb{R}$, (i) the sum $\boldsymbol{u}+\boldsymbol{v}$ and the scalar multiple $a\boldsymbol{v}$ are unique elements of V, and (ii) the following axioms hold.

(1) (commutativity) $\boldsymbol{v}+\boldsymbol{u}=\boldsymbol{u}+\boldsymbol{v}$.
(2) (associativity) $(\boldsymbol{u}+\boldsymbol{v})+\boldsymbol{w}=\boldsymbol{u}+(\boldsymbol{v}+\boldsymbol{w})$.
(3) (zero vector) There exists an element $\mathbf{0} \in V$ such that $\boldsymbol{v}+\mathbf{0}=\boldsymbol{v}$.
(4) (additive inverse) There exists an element $-\boldsymbol{v} \in V$ such that $\boldsymbol{v}+(-\boldsymbol{v})=\mathbf{0}$.
(5) $1\boldsymbol{v}=\boldsymbol{v}$.
(6) $(ab)\boldsymbol{v}=a(b\boldsymbol{v})$.
(7) $a(\boldsymbol{u}+\boldsymbol{v})=a\boldsymbol{u}+a\boldsymbol{v}$.
(8) $(a+b)\boldsymbol{v}=a\boldsymbol{v}+b\boldsymbol{v}$.

[Note: In general, we can define a vector space over a *field* K, where the scalars are elements of the *field* K. But here we shall focus on real vector spaces. See MATH2102 for more details about this more general notion of vector space.]

3.1.3 With these axioms, we can deduce the following "natural" properties.

Proposition 3.1.a. Let $\boldsymbol{v}$ be a vector in a vector space V. Then, the following hold.

(a) The zero vector $\mathbf{0}$ in axiom (3) is unique.
(b) The scalar multiple $0\boldsymbol{v}$ is the zero vector.
(c) The additive inverse $-\boldsymbol{v}$ in axiom (4) equals $(-1)\boldsymbol{v}$ (and thus is uniquely determined by $\boldsymbol{v}$).
(d) For any $a \in \mathbb{R}$, we have $a\mathbf{0}=\mathbf{0}$.

Proof.

(a) Assume that there are two zero vectors $\mathbf{0}$ and $\mathbf{0}'$ satisfying axiom (3). Then, by applying axioms (1) and (3), we have

$$\mathbf{0}' \stackrel{(3)}{=} \mathbf{0}'+\mathbf{0} \stackrel{(1)}{=} \mathbf{0}+\mathbf{0} \stackrel{(3)}{=} \mathbf{0}.$$

(b) Using the axioms (5) and (8), we have

$$0\boldsymbol{v}+\boldsymbol{v} \stackrel{(5)}{=} 0\boldsymbol{v}+1\boldsymbol{v} \stackrel{(8)}{=} (0+1)\boldsymbol{v}=1\boldsymbol{v} \stackrel{(5)}{=} \boldsymbol{v}.$$

Adding additive inverse $-\boldsymbol{v}$ on both sides, we get

$$(0\boldsymbol{v}+\boldsymbol{v})+(-\boldsymbol{v})=\boldsymbol{v}+(-\boldsymbol{v}) \stackrel{(2),\,(4)}{\Longrightarrow} 0\boldsymbol{v}+\mathbf{0}=\mathbf{0} \stackrel{(3)}{\Longrightarrow} 0\boldsymbol{v}=\mathbf{0}.$$

(c) Consider:

$$\begin{aligned}
&\boldsymbol{v}+(-\boldsymbol{v})=\mathbf{0} && (4)\\
\Longrightarrow\ &(-1)\boldsymbol{v}+[\boldsymbol{v}+(-\boldsymbol{v})]=(-1)\boldsymbol{v}+\mathbf{0} &&\\
\Longrightarrow\ &[(-1)\boldsymbol{v}+\boldsymbol{v}]+(-\boldsymbol{v})=(-1)\boldsymbol{v} && (2),\ (3)\\
\Longrightarrow\ &[(-1)\boldsymbol{v}+1\boldsymbol{v}]+(-\boldsymbol{v})=(-1)\boldsymbol{v} && (5)\\
\Longrightarrow\ &0\boldsymbol{v}+(-\boldsymbol{v})=(-1)\boldsymbol{v} && (8)\\
\Longrightarrow\ &-\boldsymbol{v}=(-1)\boldsymbol{v} && (b),\ (1),\ (3).
\end{aligned}$$

(d) Setting $\boldsymbol{v} = \mathbf{0}$ in (b), we have $0\mathbf{0} = \mathbf{0}$. Hence,

$$a\mathbf{0} = a(0\mathbf{0}) = (a0)\mathbf{0} = 0\mathbf{0} = \mathbf{0}.$$

□

3.1.4 Some examples of vector space (the vector addition and scalar multiplication are naturally defined in the usual way for the following):

(a) The set of $\mathbb{R}^n$ of column vectors.

(b) The set of $m \times n$ matrices, denoted by $M_{m\times n}(\mathbb{R})$. [Note: The zero vector in this vector space is the *zero matrix* $O_{m\times n}$.]

(c) The set of all functions from $\mathbb{R}$ to $\mathbb{R}$. [Note: The zero vector in this vector space is the constant zero function, i.e., function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 0$ for any $x \in \mathbb{R}$.]

3.1.5 Just like a set can have *subsets*, a vector space can have (vector) *subspaces*. The idea is that we want to extract a "part" of a vector space such that the part is still a valid vector space on its own.

3.1.6 Let V be a vector space. A *nonempty* subset W of V is a **vector subspace** (or simply **subspace**) of V if for any $\boldsymbol{u}, \boldsymbol{v} \in W$ and any scalar $a \in \mathbb{R}$,

(a) (closed under addition) $\boldsymbol{u} + \boldsymbol{v} \in W$.

(b) (closed under scalar multiplication) $a\boldsymbol{v} \in W$.

[Warning: Do not forget the condition that the set needs to be nonempty! In practice, this can be verified conveniently by showing that $\mathbf{0} \in W$.]

3.1.7 The following property is useful for showing that a given set is *not* a vector subspace.

Proposition 3.1.b. Let W be a vector subspace of a vector space V. Then, the zero vector $\mathbf{0}$ in V belongs also to W.

Proof. Consider any $\boldsymbol{v} \in W \subseteq V$, which exists since W is nonempty. Then note that

$$\mathbf{0} = -\boldsymbol{v} + \boldsymbol{v} = (-1)\boldsymbol{v} + \boldsymbol{v} \in W$$

where the last "$\in$" follows from the closedness under addition and scalar multiplication. □

From this result, we know that if a subset W of a vector space V does *not* contain the zero vector $\mathbf{0}$ in V, then it cannot possibly be a vector subspace.

3.1.8 The following result justifies that a vector subspace is indeed a vector space.

Proposition 3.1.c. Let W be a vector subspace of a vector space V. Then W is also a vector space, with the vector addition and scalar multiplication from V.

Proof. Firstly, closedness under addition and scalar multiplication guarantees that vector addition and scalar multiplication must yield unique elements in W. So it remains to check the axioms of vector space. In fact, we only need to check axioms (3) and (4) since other axioms must hold due to the fact that $W \subseteq V$ and V is a vector space.

Axiom (3) follows from Proposition 3.1.b. Axiom (4) holds by noting that, for any $\boldsymbol{v} \in W$, there exists $(-1)\boldsymbol{v} \in W$ such that

$$\boldsymbol{v} + (-1)\boldsymbol{v} = (1-1)\boldsymbol{v} = 0\boldsymbol{v} = \mathbf{0}.$$

□

3.1.9 Some examples of vector subspaces:

(a) A vector space V is always a vector subspace of itself.

(b) Given any vector space V, the subset of V containing only the zero vector ($\{\mathbf{0}\}$) is a vector subspace of V. It is called the **zero subspace** of V.

(c) The set of all diagonal $n \times n$ matrices is a vector subspace of the vector space $M_{n\times n}(\mathbb{R})$.

(d) The set of all real polynomials is a vector subspace of the vector space of all functions from $\mathbb{R}$ to $\mathbb{R}$.

3.2 Spanning Sets

3.2.1 Consider a fixed vector $\boldsymbol{v} \in \mathbb{R}^n$. Note that the set $\{c\boldsymbol{v} : c \in \mathbb{R}\}$ is a vector subspace of $\mathbb{R}^n$. Here, we use a single vector to "yield" a vector subspace.

Next, consider two vectors $\boldsymbol{i}$ and $\boldsymbol{j}$ in $\mathbb{R}^2$. Note that the set $\{a\boldsymbol{i} + b\boldsymbol{j} : a, b \in \mathbb{R}\}$ is indeed just $\mathbb{R}^2$. So it turns out that the whole vector space $\mathbb{R}^2$ can be obtained by using just two vectors. They may be seen as "cores" of $\mathbb{R}^2$.

3.2.2 We have used the notion of *linear combination* above, which is defined in [1.3.6] in the context of vector space $\mathbb{R}^n$. Here, we will define it more generally as follows.

Let S be a nonempty subset of V. A vector $\boldsymbol{v} \in V$ is a **linear combination of vectors in S** if there exist a *finite* number of vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in S$ and scalars $a_1, \ldots, a_n \in \mathbb{R}$ such that

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

In such case, we call $\boldsymbol{v}$ as a **linear combination of vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$**.

3.2.3 Some examples of linear combination:

(a) In $\mathbb{R}^3$, $\begin{bmatrix}1\\2\\3\end{bmatrix}$ is a linear combination of $\begin{bmatrix}1\\0\\0\end{bmatrix}$, $\begin{bmatrix}0\\1\\0\end{bmatrix}$, and $\begin{bmatrix}0\\0\\1\end{bmatrix}$.

(b) In $M_{2\times 2}(\mathbb{R})$, $\begin{bmatrix}1&3\\2&0\end{bmatrix}$ is a linear combination of $\begin{bmatrix}1&3\\0&0\end{bmatrix}$, $\begin{bmatrix}0&0\\2&-1\end{bmatrix}$, and $\begin{bmatrix}0&0\\2&1\end{bmatrix}$ since

$$\begin{bmatrix}1&3\\2&0\end{bmatrix} = \begin{bmatrix}1&3\\0&0\end{bmatrix} + \frac{1}{2}\begin{bmatrix}0&0\\2&-1\end{bmatrix} + \frac{1}{2}\begin{bmatrix}0&0\\2&1\end{bmatrix}.$$

(c) In the vector space of all polynomials, $1 + 2x - 6x^5$ is a linear combination of $1 + 3x$ and $x + 6x^5$ since

$$1 + 2x - 6x^5 = (1 + 3x) - (x + 6x^5).$$

3.2.4 Let S be a nonempty subset of a vector space V. The **span** of S, denoted by $\operatorname{span}(S)$, is the set of all linear combinations of the vectors in S, i.e.,

$$\operatorname{span}(S) = \left\{\sum_{i=1}^{k} a_i\boldsymbol{v}_i : a_1, \ldots, a_k \in \mathbb{R}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in S, k \in \mathbb{N}\right\}$$

Conventionally, we define $\operatorname{span}(\varnothing) = \{\boldsymbol{0}\}$. [Intuition 💡: The span of empty set is like a set containing an "empty sum", which should naturally be the zero vector $\boldsymbol{0}$ (representing "nothing").]

3.2.5 It turns out that spanning always results in a vector subspace.

Proposition 3.2.a. Let V be a vector space and S be any subset of V. Then, $\operatorname{span}(S)$ is a vector subspace of V.

Proof. If $S = \varnothing$, then there is nothing to prove as $\operatorname{span}(S) = \{\boldsymbol{0}\}$ is simply the zero subspace in this case. Henceforth assume that $S \neq \varnothing$. Fix any $\boldsymbol{u}, \boldsymbol{v} \in \operatorname{span}(S)$. Then we can write

$$\boldsymbol{u} = a_1\boldsymbol{u}_1 + \cdots + a_r\boldsymbol{u}_r,$$

for some $a_1, \ldots, a_r \in \mathbb{R}$ and $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r \in S$. Also, we can write

$$\boldsymbol{v} = b_1\boldsymbol{v}_1 + \cdots + b_s\boldsymbol{v}_s,$$

for some $b_1, \ldots, b_s \in \mathbb{R}$ and $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s \in S$.

Now, it remains to check that $\boldsymbol{u} + \boldsymbol{v} \in \operatorname{span}(S)$ and $c\boldsymbol{v} \in \operatorname{span}(S)$ for any $c \in \mathbb{R}$.

$\underline{\boldsymbol{u}+\boldsymbol{v}\in\operatorname{span}(S)}$: Note that

$$\boldsymbol{u}+\boldsymbol{v}=(a_1\boldsymbol{u}_1+\cdots+a_r\boldsymbol{u}_r)+(b_1\boldsymbol{v}_1+\cdots+b_s\boldsymbol{v}_s)$$

is a linear combination of vectors $\boldsymbol{u}_1,\dots,\boldsymbol{u}_r,\boldsymbol{v}_1,\dots,\boldsymbol{v}_s$ in S. Thus, $\boldsymbol{u}+\boldsymbol{v}\in\operatorname{span}(S)$.

$\underline{c\boldsymbol{v}\in\operatorname{span}(S)\text{ for any }c\in\mathbb{R}}$: Note that for any $c\in\mathbb{R}$,

$$c\boldsymbol{v}=c(b_1\boldsymbol{v}_1+\cdots+b_s\boldsymbol{v}_s)=(cb_1)\boldsymbol{v}_1+\cdots+(cb_s)\boldsymbol{v}_s$$

is a linear combination of vectors in S, hence $c\boldsymbol{v}\in\operatorname{span}(S)$. □

3.2.6 A special kind of vector subspace obtained by spanning is the *column space*, which can be got by spanning the *columns* of a matrix.

Let A be an $m\times n$ matrix and let $\boldsymbol{v}_1,\dots,\boldsymbol{v}_n$ be the columns of A. Then,

$$\operatorname{col}(A)=\operatorname{span}(\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_n\})$$

is called the **column space** of A.

3.2.7 By definition of matrix-vector product, we can show that

$$\operatorname{col}(A)=\{A\boldsymbol{x}\in\mathbb{R}^n:\boldsymbol{x}\in\mathbb{R}^m\}.$$

Proof. "$\subseteq$": Fix any $\boldsymbol{u}\in\operatorname{col}(A)$. Then, we have

$$\boldsymbol{u}=x_1\boldsymbol{v}_1+\cdots+x_n\boldsymbol{v}_n$$

for some scalars $x_1,\dots,x_n\in\mathbb{R}$. But then we can just express it as

$$\boldsymbol{u}=A\boldsymbol{x}$$

where $\boldsymbol{x}=\begin{bmatrix}x_1&\cdots&x_n\end{bmatrix}^T\in\mathbb{R}^m$ by definition of matrix-vector product.

"$\supseteq$": Fix any $\boldsymbol{u}\in\{A\boldsymbol{x}\in\mathbb{R}^n:\boldsymbol{x}\in\mathbb{R}^m\}$. Then, $\boldsymbol{u}=A\boldsymbol{x}$ for some $\boldsymbol{x}\in\mathbb{R}^m$. Then, applying the definition of matrix-vector product again, writing $\boldsymbol{x}=\begin{bmatrix}x_1&\cdots&x_n\end{bmatrix}^T$, we have

$$\boldsymbol{u}=x_1\boldsymbol{v}_1+\cdots+x_n\boldsymbol{v}_n,$$

which means that $\boldsymbol{u}\in\operatorname{span}(\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_n\})$. □

3.2.8 A subset S of a vector space V is said to **span** V, or is a **spanning set** of V, if $\operatorname{span}(S)=V$.

Since every linear combination of vectors in $S\subseteq V$ belongs to V by the definition of vector space, we always have $\operatorname{span}(S)\subseteq V$. Hence, to show that S spans V, it actually suffices to show that $\operatorname{span}(S)\supseteq V$, i.e., *every vector in V is a linear combination of vectors in S.*

3.2.9 It turns that the concept of *solving system of linear equations* we have studied in Section 2 is useful for showing this.

For example, consider $V=\mathbb{R}^m$ and $S=\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_n\}\subseteq V$. Then, for any $\boldsymbol{u}=\begin{bmatrix}u_1&\cdots&u_m\end{bmatrix}^T\in\mathbb{R}^m$, we need to investigate whether the following equation, with unknowns $x_1,\dots,x_n$, has any solution:

$$x_1\boldsymbol{v}_1+\cdots+x_n\boldsymbol{v}_n=\boldsymbol{u}.$$

Writing $\boldsymbol{v}_j=\begin{bmatrix}v_{1j}\\ \vdots\\ v_{mj}\end{bmatrix}$ for any $j=1,\dots,n$, we can write the equation above more explicitly as a system of m linear equations in n unknowns:

$$\begin{cases}v_{11}x_1+\cdots+v_{1n}x_n=u_1,\\ v_{21}x_1+\cdots+v_{2n}x_n=u_2,\\ \qquad\vdots\\ v_{m1}x_1+\cdots+v_{mn}x_n=u_m.\end{cases}$$

Its augmented matrix is

$$\left[\begin{array}{cccc|c} v_{11} & v_{12} & \cdots & v_{1n} & u_1 \\ v_{21} & v_{22} & \cdots & v_{2n} & u_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} & u_m \end{array}\right].$$

Then, we know that S spans V iff the system is *consistent*. So methods for determining consistency in Section 2.6 can be utilized to determine whether S spans V or not.

3.3 Linear Independence

3.3.1 While *spanning set* is about the *existence* of solution to a system, *linear independence* is about the *uniqueness* of solution to a system.

3.3.2 A subset S of a vector space V is called **linearly dependent** if there exist distinct vectors $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n \in S$, and scalars $a_1, \dots, a_n \in \mathbb{R}$ which are *not all zero* such that

$$a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n = \mathbf{0},$$

for some $n \in \mathbb{N}$. [Intuition 💡: This means that we can express a vector in S as a linear combination of some other vectors in the same set S, so some vectors in S are "related linearly" ➔ "linearly dependent".

The equality would hold if the scalars were all zero, *regardless* of what S is. So we would like to exclude this "boring" case.]

3.3.3 A subset S of a vector space V is called **linearly independent** if S is *not* linearly dependent, i.e., for any $n \in \mathbb{N}$, the only scalars $a_1, \dots, a_n \in \mathbb{R}$ satisfying

$$a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n = \mathbf{0}, \quad \text{where } \boldsymbol{v}_1, \dots, \boldsymbol{v}_n \in S \text{ are distinct},$$

are the trivial one: $a_1 = \cdots = a_n = 0$, i.e., symbolically,

$$a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n = \mathbf{0} \implies a_1 = \cdots = a_n = 0.$$

In other words, for any finitely many distinct $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n \in S$, the homogeneous system (with unknowns $a_1, \dots, a_n$)

$$\begin{bmatrix} \boldsymbol{v}_1 & \cdots & \boldsymbol{v}_n \end{bmatrix} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

only has the trivial solution $a_1 = \cdots = a_n = 0$. Since a homogeneous system always has the trivial solution, this is equivalent to saying that the homogeneous system has a *unique* solution. So again the methods discussed in Section 2.6 are useful for determining linear independence.

[Note: If we have $S = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$, sometimes we say "$\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ are linearly (in)dependent" to mean "S is linearly (in)dependent".]

3.3.4 We can have a more "intuitive" equivalent definition for linear dependence when we focus on a set of two nonzero vectors.

Consider a subset $S = \{\boldsymbol{u}, \boldsymbol{v}\}$ of a vector space V, where $\boldsymbol{u}$ and $\boldsymbol{v}$ are nonzero. Then S is linearly dependent iff $\boldsymbol{u} = a\boldsymbol{v}$ for some $a \neq 0$.

Proof. "$\Leftarrow$": Assume that $\boldsymbol{u} = a\boldsymbol{v}$ for some $a \neq 0$. Then, we can write

$$(1)\boldsymbol{u} + (-a)\boldsymbol{v} = \mathbf{0},$$

so S is linearly dependent.

"$\Rightarrow$": Assume that S is linearly dependent. Then there exist scalars $a_1, a_2 \in \mathbb{R}$, not all zero, such that

$$a_1\boldsymbol{u} + a_2\boldsymbol{v} = \mathbf{0}.$$

We claim that $a_1 \neq 0$. To prove this, assume to the contrary that $a_1 = 0$. Then, we have $a_2 \neq 0$ and also $a_2\boldsymbol{v} = \mathbf{0}$. This implies $\boldsymbol{v} = \mathbf{0}$, contradiction. Similarly, we can show that $a_2 \neq 0$.

Hence, we can write

$$\boldsymbol{u} = \underbrace{\frac{-a_2}{a_1}}_{\neq 0}\boldsymbol{v}$$

as desired. □

3.3.5 Let V be a vector space and let $S_1 \subseteq S_2 \subseteq V$. Then, the following hold.

(a) If S_2 is linearly independent, then S_1 is also linearly independent.

(b) If S_1 is linearly dependent, then S_2 is also linearly dependent.

Proof.

(a) Assume that S_2 is linearly independent. Then for any $n \in \mathbb{N}$ and any distinct vectors $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n \in S_2$, we have

$$a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n = \mathbf{0} \implies a_1 = \cdots = a_n = 0.$$

But as $S_1 \subseteq S_2$, this implication must also hold for arbitrary distinct vectors in S_1.

(b) The statement is just the contrapositive of (a), and hence is true also.

□

However, the converse does *not* hold in general. WLOG, we focus on the converse of (a): "If S_1 is linearly independent, then S_2 is linearly independent." Take any $S_1 \subseteq V$ which is linearly independent and take $S_2 = S_1 \cup \{\mathbf{0}\}$. Then, $S_2 \supseteq S_1$ but S_2 is always linearly dependent.

3.4 Bases

3.4.1 The next concept to be discussed is *basis*, which neatly connects the concepts of *spanning set* and *linear independence*. A **basis** for a vector space V is a *linearly independent* subset of V which also *spans* V.

[Intuition 💡: A basis can be seen as a "minimal" spanning set for V, without "redundancy".]

3.4.2 To illustrate why a basis can be seen as a "minimal" spanning set for V, consider the following results. Let β be a basis for a vector space V.

(a) If S is a proper subset of β, then $\text{span}(S) \neq V$.

Proof. Assume that S is a proper subset of β. Then, there exists $\boldsymbol{v} \in \beta \subseteq V$ with $\boldsymbol{v} \notin S$. Now, suppose on the contrary that $\boldsymbol{v} \in \text{span}(S)$. Then, we can write

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

where $a_1, \dots, a_n \in \mathbb{R}$, $v_1, \dots, v_n \in S$, and $n \in \mathbb{N}$. This implies that

$$a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n + (-1)\boldsymbol{v} = \mathbf{0},$$

thus $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n, \boldsymbol{v}\} \subseteq \beta$ is *not* linearly independent, which would imply that β is *not* linearly independent also by [3.3.5], contradiction. This means $\boldsymbol{v} \notin \text{span}(S)$, so we have found an element in V *not* in $\text{span}(S)$, meaning that $\text{span}(S) \neq V$. □

[Intuition 💡: This means that there is not "smaller" spanning set for V than the "minimal" one.]

(b) If β is a proper subset of a set $S \subseteq V$, then S is not linearly independent.

Proof. Assume that β is a proper subset of $S \subseteq V$. Then there exists $\boldsymbol{v} \in S \subseteq V$ with $\boldsymbol{v} \notin \beta$. Since $\beta = \{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\}$ spans V, we can write

$$\boldsymbol{v} = a_1\boldsymbol{b}_1 + \cdots + a_n\boldsymbol{b}_n$$

for some scalars $a_1, \ldots, a_n \in \mathbb{R}$. But since β is a proper subset of S, we have $S \supseteq \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n, \boldsymbol{v}\}$. By writing the equation above as

$$a_1\boldsymbol{b}_1 + \cdots + a_n\boldsymbol{b}_n + (-1)\boldsymbol{v} = \boldsymbol{0},$$

we note that the latter set $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n, \boldsymbol{v}\}$ is *not* linearly independent, so do S (by [3.3.5]). $\square$

[Intuition 💡: Note that S also spans V since β is a proper subset of S. However, as a set "larger" than the "minimal" spanning set, it would contain some "redundancy" ➔ not linearly independent.]

3.4.3 Consider the vector space $\mathbb{R}^n$. A standard example of basis of $\mathbb{R}^n$ is the set $\beta = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$, where the elements are the standard vectors. It is called the **standard basis** for $\mathbb{R}^n$.

Proof. We can prove that the standard basis is indeed a basis for $\mathbb{R}^n$.

Firstly, we show that it spans $\mathbb{R}^n$. For any $\boldsymbol{v} = \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix}^T \in \mathbb{R}^n$, we can write

$$\boldsymbol{v} = v_1\boldsymbol{e}_1 + \cdots + v_n\boldsymbol{e}_n,$$

so $\boldsymbol{v} \in \operatorname{span}(\beta)$. This implies that $\operatorname{span}(\beta) = \mathbb{R}^n$.

Next, to show the linear independence of β, consider first the equation

$$x_1\boldsymbol{e}_1 + \cdots + x_n\boldsymbol{e}_n = \boldsymbol{0}.$$

It can be rewritten as a homogeneous system

$$I_n \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix},$$

which clearly has the unique solution $x_1 = \cdots = x_n = 0$. $\square$

3.4.4 Note that basis is *not unique*. For example, for the vector space $\mathbb{R}^2$, two possible bases are the standard basis $\{\boldsymbol{i}, \boldsymbol{j}\}$, and the set $\{2\boldsymbol{i}, 2\boldsymbol{j}\}$.

3.4.5 Let V be a vector space and S be any linearly independent subset of V. Then, S is a basis for its span $\operatorname{span}(S)$.

Proof. Linear independence of S follows from assumption, and by definition S must be a spanning set of $\operatorname{span}(S)$, where $\operatorname{span}(S)$ is considered as a vector space. $\square$

As a special case, if $V = \{\boldsymbol{0}\}$, then the only linearly independent subset of V is $\varnothing$, so the empty set $\beta = \varnothing$ is a basis for $\operatorname{span}(\varnothing) = \{\boldsymbol{0}\} = V$.

3.4.6 The main result about *basis* is the following.

Theorem 3.4.a. Let V be a nonzero vector space and β be a subset of V. Then, β is a basis for V iff for any vector $\boldsymbol{u} \in V$, $\boldsymbol{u}$ can be uniquely written as a linear combination of vectors in β, i.e.,

$$\boldsymbol{u} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$$

for some *unique* scalars $a_1, \ldots, a_n \in \mathbb{R}$, with $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$.

[Intuition 💡: The spanning property of basis corresponds to the *existence* of such linear combination, and the linear independence of basis corresponds to the *uniqueness* of such linear combination.]

Proof. "$\Rightarrow$": Assume that β is a basis for V, and fix any vector $\boldsymbol{u} \in V$.

<u>Existence</u>: Since β spans V, there exist scalars $a_1, \ldots, a_n \in \mathbb{R}$ such that

$$\boldsymbol{u} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n.$$

Uniqueness: Suppose that we can also write $\boldsymbol{u} = b_1\boldsymbol{v}_1 + \cdots + b_n\boldsymbol{v}_n$ for some scalars $b_1, \ldots, b_n$. Then, we have

$$\boldsymbol{u} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n = b_1\boldsymbol{v}_1 + \cdots + b_n\boldsymbol{v}_n,$$

which implies

$$(a_1 - b_1)\boldsymbol{v}_1 + \cdots + (a_n - b_n)\boldsymbol{v}_n = \mathbf{0}.$$

By linear independence of β, it follows that

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

which means $a_1 = b_1, \ldots, a_n = b_n$.

"$\Leftarrow$": Assume that for any $\boldsymbol{u} \in V$, we can write

$$\boldsymbol{u} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$$

for some *unique* scalars $a_1, \ldots, a_n \in \mathbb{R}$, with $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$. This immediately shows that $\operatorname{span}(\beta) = V$. So it remains to prove that β is linearly independent. Consider the equation

$$c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n = \mathbf{0} = 0\boldsymbol{v}_1 + \cdots + 0\boldsymbol{v}_n.$$

By the uniqueness, we must have $c_1 = \cdots = c_n = 0$, as desired. □

3.5 Dimensions

3.5.1 From now on, we shall focus on vector spaces with *finite* bases unless otherwise specified. Vector spaces with *infinite* bases are studied in *functional analysis*, which is a much more advanced topic. (See MATH4404 for more details.)

3.5.2 In Section 3.5, we shall discuss a "famous" concept: *dimension*. Most of us should have some intuitive idea about it, but here we will try to formalize this notion mathematically (in the context of linear algebra).

3.5.3 Before discussing the concept of dimension, we shall first consider several preliminary results.

Proposition 3.5.a. Let β be a basis for a vector space V. If β' is a linearly independent subset of V, then $|\beta'| \le |\beta|$. (Here $|\cdot|$ denotes cardinality.)

Proof. Firstly, if V is the zero vector space $\{\mathbf{0}\}$, this result is trivial since the only linearly independent subset of V is the empty set $\varnothing$. Thus, henceforth we suppose that V is a nonzero vector space.

Let $m = |\beta|$ and $n = |\beta'|$. Then, we write $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ and $\beta' = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$.

Since β spans V and β' is a subset of V, for any $j = 1, \ldots, n$, we can write

$$\boldsymbol{u}_j = a_{1j}\boldsymbol{v}_1 + \cdots + a_{mj}\boldsymbol{v}_m$$

for some scalars $a_{1j}, \ldots, a_{mj}$.

Now, we set

$$x_1\boldsymbol{u}_1 + \cdots + x_n\boldsymbol{u}_n = 0,$$

which can be rewritten as

$$\sum_{i=1}^{m}(a_{i1}x_1 + \cdots + a_{in}x_n)\boldsymbol{v}_i = 0.$$

By linear independence of $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$, we obtain the following homogeneous system of linear equations

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \qquad\qquad\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0. \end{cases}$$

Now, assume to the contrary that $n > m$. In such case, by Proposition 2.6.c, this system would have a non-trivial solution, contradicting to the linear independence of $\beta' = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$. $\square$

3.5.4 Using Proposition 3.5.a, we can show the following relationship between any two bases for a vector space V.

Corollary 3.5.b. Let β_1 and β_2 be any two bases of a vector space V. Then, β_1 and β_2 contain the same number of vectors.

Proof. Setting $\beta = \beta_1$ and $\beta' = \beta_2$ in Proposition 3.5.a gives $|\beta_2| \leq |\beta_1|$. On the other hand, setting $\beta = \beta_2$ and $\beta' = \beta_1$ in Proposition 3.5.a gives $|\beta_1| \leq |\beta_2|$. Hence, we have $|\beta_1| = |\beta_2|$. $\square$

3.5.5 From Corollary 3.5.b, we see that the *cardinality of basis* is independent from the choice of basis. It only depends on the underlying vector space. This suggests the notion of *dimension*. The number of vectors in a basis for a vector space V is called the **dimension** of V, denoted by $\dim(V)$.

[Note: Roughly speaking, dimension may be seen as the number of "degrees of freedom" or "independent parameters".]

Examples:

- The dimension of $\mathbb{R}^n$ is n (as expected) since the standard basis $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ of $\mathbb{R}^n$ has n vectors.
- The dimension of the zero vector space $V = \{\boldsymbol{0}\}$ is 0 since a basis (in fact, the only basis) for V is $\varnothing$. Indeed, the zero vector space is the only vector space with zero dimension.

3.5.6 To close Section 3.5, we give some results regarding dimension.

(a) Let S be a finite linearly independent subset of a vector space V. Then, $\dim(\operatorname{span}(S)) = |S|$.
Proof. Since S is a spanning set of $\operatorname{span}(S)$ (where $\operatorname{span}(S)$ is considered as a vector space) and S is linearly independent, S serves as a basis for $\operatorname{span}(S)$. Thus, its dimension is $\dim(\operatorname{span}(S)) = |S|$. $\square$

(b) Let W be a vector subspace of a vector space V. Then, $\dim(W) \leq \dim(V)$.
Proof. Let β_W and β_V be bases of W and V respectively. Then β_W is a linearly independent subset of W. Since $W \subseteq V$, β_W is also a linearly independent subset of V. Hence, by Proposition 3.5.a, we have $|\beta_W| \leq |\beta_V|$. Thus, $\dim(W) \leq \dim(V)$. $\square$

3.6 Constructing Bases: Extension and Reduction

3.6.1 So far we have seen some examples of bases, but we do not yet have a systematic method for obtaining bases. Thus we will introduce two important approaches for constructing bases in Section 3.6, namely *extension* and *reduction*.

3.6.2 The intuitive idea behind *extension* and *reduction* is related to [3.4.2]a and [3.4.2]b:

- *Extension:* From [3.4.2]a we know that if the cardinality of a subset S of V is less than $\dim(V)$, then $\operatorname{span}(S) \neq V$. The idea is thus as follows:
  (a) Start with a certain linearly independent subset S of V (which may not span V).
  (b) Keep adding vectors to S to form larger and larger *linearly independent* sets, until its cardinality reaches $\dim(V)$ ➔ "extending" the set S.
- *Reduction:* From [3.4.2]b we know that if the cardinality of a subset S of V is greater than $\dim(V)$, then S must not be linearly independent. The idea is thus as follows:
  (a) Start with a spanning set S of V (which may not be linearly independent).
  (b) Keep removing vectors from S while ensuring it still spans V, until its cardinality reaches $\dim(V)$ ➔ "reducing" the set S

3.6.3 To justify these two approaches mathematically, we shall utilize some theorems below.

Theorem 3.6.a. Let S be a linearly independent subset of a vector space V, and let $\boldsymbol{v} \in V$. If $\boldsymbol{v} \notin \operatorname{span}(S)$, then $S \cup \{\boldsymbol{v}\}$ is also linearly independent.

Proof. The result is vacuously true if $V = \{\mathbf{0}\}$, since the only linear independent subset of V is $\varnothing$, and $\mathbf{0} \in \operatorname{span}(\varnothing) = \{\mathbf{0}\}$ always. Thus we never have $\boldsymbol{v} \notin \operatorname{span}(S)$ in this case.

Now, assume that V is a nonzero vector space. Write $S = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$. Then, consider the equation

$$x_1\boldsymbol{v}_1 + \cdots + x_m\boldsymbol{v}_m + x_{m+1}\boldsymbol{v} = 0. \tag{2}$$

Case 1: $x_{m+1} \neq 0$.

In such case, we can rewrite Equation (2) as

$$\boldsymbol{v} = -\frac{x_1}{x_{m+1}}\boldsymbol{v}_1 - \cdots - \frac{x_m}{x_{m+1}}\boldsymbol{v}_m,$$

meaning that $\boldsymbol{v}$ is a linear combination of vectors in S, thus $\boldsymbol{v} \in \operatorname{span}(S)$, contradiction. So case 1 cannot happen.

Case 2: $x_{m+1} = 0$.

In this case, we can simplify Equation (2) as

$$x_1\boldsymbol{v}_1 + \cdots + x_m\boldsymbol{v}_m = 0,$$

which implies $x_1 = \cdots = x_m = 0$ by the linear independence of S. Thus, the only solution to Equation (2) is

$$x_1 = \cdots = x_m = x_{m+1} = 0,$$

which means that $S \cup \{\boldsymbol{v}\}$ is linearly independent. □

3.6.4 Theorem 3.6.a suggests how we can add vectors to a linearly independent set while preserving its linear independence. But only this is not enough for fully justifying the extension approach. We also need the following result which guarantees that a basis must be obtained when the cardinality of set reaches the dimension during the extension process.

Theorem 3.6.b. Let m be the dimension of a vector space V. If S is a linearly independent subset of V with m vectors, then S is a basis for V.

Proof. Assume to the contrary that $\operatorname{span}(S) \neq V$. Then there exists $\boldsymbol{v} \in V$ such that $\boldsymbol{v} \notin \operatorname{span}(S)$. Next, using Theorem 3.6.a, the set $S \cup \{\boldsymbol{v}\}$ is linearly independent. This contradicts Proposition 3.5.a since its cardinality is $|S \cup \{\boldsymbol{v}\}| = m + 1 > m = \dim(V)$[7]. □

3.6.5 Next, we consider theorems that justify *reduction*. Likewise two theorems are needed for fully justifying the reduction approach.

Theorem 3.6.c. Let S be a spanning set of a vector space V. If S is linearly *dependent*, then there exists $\boldsymbol{v} \in S$ such that $\operatorname{span}(S \setminus \{\boldsymbol{v}\}) = \operatorname{span}(S) = V$.

Proof. When $V = \{\mathbf{0}\}$, this result again holds vacuously since the only spanning set for V is the empty set $\varnothing$, which must be linearly independent.

Now assume that V is nonzero. Write $S = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$. Since S is linearly dependent, there exist scalars $a_1, \ldots, a_m$, not all zero, such that

$$a_1\boldsymbol{v}_1 + \cdots + a_m\boldsymbol{v}_m = 0.$$

Choose an $i \in \{1, \ldots, n\}$ with $a_i \neq 0$. Then rewrite the equation as

$$\boldsymbol{v}_i = -\frac{a_1}{a_i}\boldsymbol{v}_1 - \cdots - \frac{a_{i-1}}{a_i}\boldsymbol{v}_{i-1} - \frac{a_{i+1}}{a_i}\boldsymbol{v}_{i+1} - \cdots - \frac{a_m}{a_i}\boldsymbol{v}_m.$$

[7] When $\boldsymbol{v} \notin \operatorname{span}(S)$, it implies in particular that $\boldsymbol{v} \notin S$. Thus, $|S \cup \{\boldsymbol{v}\}|$ is indeed $m + 1$.

Thus, $\boldsymbol{v}_i \in \operatorname{span}(S \setminus \{\boldsymbol{v}_i\})$, and so

$$\operatorname{span}(S \setminus \{\boldsymbol{v}_i\}) = \operatorname{span}(S) = V.$$

□

[Note: The proof implicitly suggests that how we can find such vector $\boldsymbol{v}$ to be removed from the linearly dependent set S. We just pick a vector in S that is a linear combination of the other vectors in S, which is guaranteed to exist by Theorem 3.6.c.]

3.6.6 Next, we have a result that is analogous to Theorem 3.6.b. But before proving it, we need the following lemma.

Lemma 3.6.d. Let S be a finite subset of a vector space V with $m \in \mathbb{N}_0$ (distinct) nonzero vectors. Then there exists a subset β of S such that β is a basis for $\operatorname{span}(S)$.

Proof. We will prove by induction on the cardinality of S: m.

Firstly, the case $m = 0$ trivially holds since in such case we have $\operatorname{span}(S) = \operatorname{span}(\varnothing) = \{\mathbf{0}\}$, and thus we can just choose $\beta = S = \varnothing$ to be a basis for the zero vector space.

Assume for induction that the case $m = k$ holds for a $k \in \mathbb{N}_0$. Now, consider any finite subset S of V with $k + 1$ nonzero vectors.

Case 1: S is linearly independent.

Then we can simply choose $\beta = S$ to be a basis for $\operatorname{span}(S)$.

Case 2: S is linearly dependent.

Since S is a spanning set for $\operatorname{span}(S)$, by Theorem 3.6.c, there exists $\boldsymbol{v} \in S$ such that $\operatorname{span}(S \setminus \{\boldsymbol{v}\}) = \operatorname{span}(S)$. Applying the induction hypothesis on the set $S \setminus \{\boldsymbol{v}\}$ (with k nonzero vectors), there exists $\beta \subseteq S \setminus \{\boldsymbol{v}\} \subseteq S$ such that β is a basis for $\operatorname{span}(S \setminus \{\boldsymbol{v}\}) = \operatorname{span}(S)$.

Thus, the case $m = k + 1$ holds, and so the result follows by induction. □

3.6.7 Now, we can prove the desired theorem.

Theorem 3.6.e. Let m be the dimension of a vector space V. If S is a spanning set of V with m vectors, then S is a basis for V.

Proof. Assume to the contrary that S is not a basis for V. Then by Lemma 3.6.d, there exists a subset β of S such that β is a basis for $\operatorname{span}(S) = V$. Since S is *not* a basis for V, the subset inclusion must be proper and it must be the case that $|\beta| < |S| = m$. This implies that $\dim(V) = |\beta| < m$, contradiction. □

3.7 Column Spaces

3.7.1 Let A be an $m \times n$ matrix and let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ be the columns of A. Recall that the column space of A is defined as $\operatorname{col}(A) = \operatorname{span}(\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\})$. By [3.2.7], we can write

$$\operatorname{col}(A) = \{A\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{x} \in \mathbb{R}^m\}.$$

3.7.2 Considering the columns of an $n \times n$ matrix A, we can obtain some more criteria for matrix invertibility. The criteria are collected below.

Theorem 3.7.a. Let A be an $n \times n$ matrix with columns $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$. Then the following are equivalent.

(a) A is invertible.

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

(c) For any $\boldsymbol{b} \in \mathbb{R}^n$, $A\boldsymbol{x} = \boldsymbol{b}$ has a unique solution.

(d) $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is a basis for $\mathbb{R}^n$.

(e) $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is linearly independent.

Proof. (a) $\iff$ (b): It follows from Theorem 1.9.e.

(a) $\iff$ (c): It follows from Proposition 2.6.h.

(a) $\iff$ (e): Note that

$$\begin{aligned} & \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} \text{ is linearly independent} \\ \iff & \text{the homogeneous system } A\boldsymbol{x} = \boldsymbol{0} \text{ only has the trivial solution} \\ \iff & A \text{ is invertible} \qquad \text{(by Proposition 2.6.f).} \end{aligned}$$

It then suffices to prove that (d) $\iff$ (e).

(d) $\implies$ (e): Immediate since a basis must be linearly independent.

(e) $\implies$ (d): It follows from Theorem 3.6.b since $\dim(\mathbb{R}^n) = n$. □

3.7.3 Next, we would like to find *bases* and *dimensions* of column spaces. We start by considering the following result about the preservation of linear independence after multiplication by an invertible matrix.

Theorem 3.7.b. Let P be an invertible $n \times n$ matrix. Then $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ is linearly independent in $\mathbb{R}^n$ iff $\{P\boldsymbol{v}_1, \ldots, P\boldsymbol{v}_k\}$ is linearly independent in $\mathbb{R}^n$.

[Note: Here we focus on the vector space $\mathbb{R}^n$ so that $P\boldsymbol{v}_i$ is well-defined for every $i = 1, \ldots, k$.]

Proof. "$\Rightarrow$": Assume that $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ are linearly independent. Consider

$$x_1(P\boldsymbol{v}_1) + \cdots + x_k(P\boldsymbol{v}_k) = 0$$

where $x_1, \ldots, x_k \in \mathbb{R}$ are unknowns. Since P is invertible, we can multiply both sides by P^{-1} to get

$$x_1\boldsymbol{v}_1 + \cdots + x_k\boldsymbol{v}_k = 0,$$

which implies that $x_1 = \cdots = x_k = 0$ by the linear independence of $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$.

"$\Leftarrow$": Similar to the "$\Rightarrow$" direction except that we multiply both sides of the equation by matrix P instead of P^{-1}. □

3.7.4 By definition, we have $\text{col}(A) = \text{span}(\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\})$, so $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is a spanning set for $\text{col}(A)$, when considered as a vector space. Then, by the *reduction* approach in Section 3.6, we know that there is a subset of $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ that forms a basis for $\text{col}(A)$. Here we will provide a systematic method for obtaining such a basis in Theorem 3.7.e. But before that, we need the following preparatory result, which suggests the preservation of *dimension* of column space after multiplication by an invertible matrix.

Theorem 3.7.c. Let A be an $m \times n$ matrix and P be an invertible $m \times m$ matrix. Then, $\dim(\text{col}(PA)) = \dim(\text{col}(A))$.

Proof. Let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ be the columns of A. We know that a subset of $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ forms a basis for $\text{col}(A)$, and we denote it by $\{\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_k}\}$. We want to show that $\{P\boldsymbol{v}_{i_1}, \ldots, P\boldsymbol{v}_{i_k}\}$ (having the same cardinality as $\{\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_k}\}$) is a basis for $\text{col}(PA)$, and therefore $\dim(\text{col}(PA)) = \dim(\text{col}(A))$.

Its linear independence follows from Theorem 3.7.b, so it suffices to prove that $\text{span}(\{P\boldsymbol{v}_{i_1}, \ldots, P\boldsymbol{v}_{i_k}\}) = \text{col}(PA)$. Firstly, by block multiplication we can write $PA = \begin{bmatrix} P\boldsymbol{v}_1 & \cdots & P\boldsymbol{v}_n \end{bmatrix}$, thus

$$\text{span}(\{P\boldsymbol{v}_1, \ldots, P\boldsymbol{v}_n\}) = \text{col}(PA).$$

Since $\{\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_k}\}$ is a basis (and thus a spanning set) for $\text{col}(A)$, for every $j = 1, \ldots, n$, we can write $\boldsymbol{v}_j$ as a linear combination of $\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_k}$, so we can also write $P\boldsymbol{v}_j$ as a linear combination of $P\boldsymbol{v}_{i_1}, \ldots, P\boldsymbol{v}_{i_k}$. This implies that

$$\text{span}(\{P\boldsymbol{v}_{i_1}, \ldots, P\boldsymbol{v}_{i_k}\}) = \text{span}(\{P\boldsymbol{v}_1, \ldots, P\boldsymbol{v}_n\}) = \text{col}(PA).$$

□

3.7.5 If the condition that P is invertible is dropped in Theorem 3.7.c, we would only have a weaker result where the equality becomes an inequality, as suggested below.

Proposition 3.7.d. Let A be an $m \times n$ matrix and P be an $m \times m$ matrix. Then, $\dim(\mathrm{col}(PA)) \leq \dim(\mathrm{col}(A))$.

Proof. Let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ be the columns of A, and consider a basis $\{\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_k}\}$ for $\mathrm{col}(A)$. Using the same argument as the proof for Theorem 3.7.c, we can show that $S = \{P\boldsymbol{v}_{i_1}, \ldots, P\boldsymbol{v}_{i_k}\}$ is a spanning set for $\mathrm{col}(PA)$, when considered as a vector space.

Then, by the *reduction* approach in Section 3.6, a basis for $\mathrm{col}(PA)$ can be obtained by removing vectors in the spanning set S, if necessary. This implies that $\dim(\mathrm{col}(PA)) \leq |S| = \dim(\mathrm{col}(A))$. ☐

3.7.6 Now, we give the systematic method for obtaining a basis for column space as follows.

Theorem 3.7.e. Let A be an $m \times n$ matrix and R be the RREF of A. Then, the columns of A corresponding to the columns containing the leading ones in R form a basis for $\mathrm{col}(A)$.

Proof. Let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ be the columns of A. By Gaussian elimination, $R = E_r \cdots E_1 A$ for some elementary matrices $E_1, \ldots, E_r$. Let $E = E_r \cdots E_1$. Then we can write

$$R = EA = \begin{bmatrix} E\boldsymbol{v}_1 & \cdots E\boldsymbol{v}_n \end{bmatrix}$$

by block multiplication.

Denote the columns in R with leading ones by $E\boldsymbol{v}_{i_1}, \ldots, E\boldsymbol{v}_{i_k}$. It is not hard to see that the homogeneous system

$$\begin{bmatrix} E\boldsymbol{v}_{i_1} & \cdots & E\boldsymbol{v}_{i_k} \end{bmatrix} \boldsymbol{x} = \boldsymbol{0}$$

has only the trivial solution, by considering the definition of RREF. So, $\{E\boldsymbol{v}_{i_1}, \ldots, E\boldsymbol{v}_{i_k}\}$ is linearly independent.

By the definition of RREF, all entries in the rows of R without leading ones are zero. Thus, every column of R that does not contain any leading one in R can be expressed as a linear combination of $E\boldsymbol{v}_{i_1}, \ldots, E\boldsymbol{v}_{i_n}$. Consequently,

$$\mathrm{col}(R) = \mathrm{span}\left(\{E\boldsymbol{v}_{i_1}, \ldots, E\boldsymbol{v}_{i_k}\}\right).$$

So, we know that $\{E\boldsymbol{v}_{i_1}, \ldots, E\boldsymbol{v}_{i_k}\}$ is a basis for $\mathrm{col}(R)$, thus $\dim(\mathrm{col}(R)) = k$.

Since E is invertible, we know that $\{\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_k}\}$ is linearly independent by Theorem 3.7.b, and $\dim(\mathrm{col}(A)) = \dim(\mathrm{col}(EA)) = \dim(\mathrm{col}(R)) = k$ by Theorem 3.7.c. Thus, $\{\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_k}\}$ is a basis for $\mathrm{col}(A)$ by Theorem 3.6.b. ☐

Corollary 3.7.f. Let A be an $m \times n$ matrix. Then $\dim(\mathrm{col}(A))$ is the number of leading ones in the RREF of A.

Proof. It follows from Theorem 3.7.e, by noting the number of columns of A corresponding to the leading ones in R is just the number of leading ones in R, where R is the RREF of A. ☐

3.8 Row Spaces

3.8.1 After discussing column space, we will discuss *row space*. Let A be an $m \times n$ matrix with *rows* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$ (as row vectors). The **row space** of A is defined as $\mathrm{row}(A) = \mathrm{span}\left(\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}\right)$. Likewise, we would like to find bases and dimensions of row spaces.

3.8.2 The first result suggests that multiplication of an invertible matrix preserves the whole row space (not just the dimension!).

Theorem 3.8.a. Let A be an $m \times n$ matrix and P be an invertible $m \times m$ matrix. Then, $\mathrm{row}(PA) = \mathrm{row}(A)$.

Proof. Let $\boldsymbol{u}_1, \dots, \boldsymbol{u}_m$ be the rows of A, and $\boldsymbol{w}_1, \dots, \boldsymbol{w}_m$ be the rows of PA. Write $P = [p_{ij}]$. Then, by block multiplication, we have

$$PA = \begin{bmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mm} \end{bmatrix} \begin{bmatrix} \boldsymbol{u}_1 \\ \vdots \\ \boldsymbol{u}_m \end{bmatrix} = \begin{bmatrix} p_{11}\boldsymbol{u}_1 + \cdots + p_{1m}\boldsymbol{u}_m \\ \vdots \\ p_{m1}\boldsymbol{u}_1 + \cdots + p_{mm}\boldsymbol{u}_m \end{bmatrix}$$

This shows that for every row w_i of PA is a linear combination of $\boldsymbol{u}_1, \dots, \boldsymbol{u}_m$. Hence every linear combination of $\boldsymbol{w}_1, \dots, \boldsymbol{w}_m$ is also a linear combination of $\boldsymbol{u}_1, \dots, \boldsymbol{u}_m$. It follows that

$$\operatorname{row}(PA) = \operatorname{span}(\{\boldsymbol{w}_1, \dots, \boldsymbol{w}_m\}) \subseteq \operatorname{span}(\{\boldsymbol{u}_1, \dots, \boldsymbol{u}_m\}) = \operatorname{row}(A).$$

So now we have proved that $\operatorname{row}(QB) \subseteq \operatorname{row}(B)$ for any $m \times n$ matrix B and $m \times m$ (invertible) matrix Q. By setting $B = PA$ and $Q = P^{-1}$, we get

$$\operatorname{row}(A) = \operatorname{row}(P^{-1}(PA)) \subseteq \operatorname{row}(PA),$$

so the result follows. □

3.8.3 If the condition that P is invertible is dropped in Theorem 3.8.a, we would only have a weaker result about *inequality* of *dimensions*, as suggested below.

Proposition 3.8.b. Let A be an $m \times n$ matrix and P be an $m \times m$ matrix. Then, $\dim(\operatorname{row}(PA)) \leq \dim(\operatorname{row}(A))$.

Proof. Using the same argument as the first part of the proof for Theorem 3.8.a, we can show that $\operatorname{row}(PA) \subseteq \operatorname{row}(A)$, thus $\operatorname{row}(PA)$ is a vector subspace of $\operatorname{row}(A)$, even without the assumption that P is invertible. Then, by [3.5.6]b, we have $\dim(\operatorname{row}(PA)) \leq \dim(\operatorname{row}(A))$. □

3.8.4 The next result suggests how we can find a basis for row space.

Theorem 3.8.c. Let A be an $m \times n$ matrix and R be the RREF of A. Let $\boldsymbol{w}_1, \dots, \boldsymbol{w}_k$ be the non-zero rows in the RREF of A. Then, $\{\boldsymbol{w}_1, \dots, \boldsymbol{w}_k\}$ is a basis for $\operatorname{row}(A)$.

Proof. First of all, by Gaussian elimination, we can write $R = E_r \cdots E_1 A$ for some elementary matrices $E_1, \dots, E_r$. Write $E = E_r \cdots E_1$ and note that it is invertible. Thus, by Theorem 3.8.a, $\operatorname{row}(R) = \operatorname{row}(EA) = \operatorname{row}(A)$, so it suffices to show that $\{\boldsymbol{w}_1, \dots, \boldsymbol{w}_k\}$ is a basis for $\operatorname{row}(R)$.

Since adding zero (row) vectors into the set $\{\boldsymbol{w}_1, \dots, \boldsymbol{w}_k\}$ does not change its span, we see that $\operatorname{span}(\{\boldsymbol{w}_1, \dots, \boldsymbol{w}_k\}) = \operatorname{row}(R)$. Also, by the definition of RREF, the nonzero rows contain the leading ones at different positions. From this we can observe that $\{\boldsymbol{w}_1, \dots, \boldsymbol{w}_k\}$ is linearly independent. Thus, $\{\boldsymbol{w}_1, \dots, \boldsymbol{w}_k\}$ is a basis for $\operatorname{row}(R)$, as desired. □

Corollary 3.8.d. Let A be an $m \times n$ matrix. Then $\dim(\operatorname{row}(A))$ is the number of leading ones in the RREF of A.

Proof. It follows from Theorem 3.8.c, by noting the number of nonzero rows in R is just the number of leading ones in R, where R is the RREF of A. □

3.9 Matrix Rank

3.9.1 A fundamental result in linear algebra that connects row and column spaces is the following. It suggests that row and column spaces of the same matrix must always have the same dimension.

Theorem 3.9.a. Let A be an $m \times n$ matrix. Then $\dim(\operatorname{row}(A)) = \dim(\operatorname{col}(A))$.

Proof. Let R be the RREF of A. Then, we can write $R = E_r \cdots E_1 A$ for some elementary matrices $E_1, \ldots, E_r$. Let $E = E_r \cdots E_1$, and note that E is invertible. Thus, by Theorems 3.7.c and 3.8.a, we have

$$\dim(\text{col}(A)) = \dim(\text{col}(R))$$

and

$$\dim(\text{row}(A)) = \dim(\text{row}(R))$$

By Corollaries 3.7.f and 3.8.d, we then have

$$\dim(\text{col}(R)) = \dim(\text{row}(R)) = \text{number of leading ones in } R,$$

which implies that $\dim(\text{row}(A)) = \dim(\text{col}(A))$. □

3.9.2 The common value of the dimensions of row and column spaces of a matrix is said to be the rank of that matrix. Symbolically, the **rank** of an $m \times n$ matrix A is $\text{rank}(A) = \dim(\text{col}(A))$ $(= \dim(\text{row}(A)))$.

3.9.3 Since taking matrix transpose is essentially just interchanging rows and columns, it does not change the rank.

Corollary 3.9.b. Let A be an $m \times n$ matrix. Then $\text{rank}(A) = \text{rank}(A^T)$.

Proof. Note that $\text{rank}(A) = \dim(\text{col}(A)) = \dim(\text{row}(A^T)) = \text{rank}(A^T)$. □

3.9.4 Intuitively, rank measures the "magnitude" of non-invertibility of a matrix. The *lower* the rank of a matrix is, the "*more* non-invertible" the matrix is. Examples:

- The rank of every zero matrix is 0 (the lowest possible rank), so zero matrix is "very non-invertible".
- The rank of every invertible $n \times n$ matrix is n (the highest possible rank for an $n \times n$ matrix).

  Proof. Let A be any invertible matrix. By Proposition 2.7.a, the RREF of A is I_n, so there exist elementary matrices $E_1, \ldots, E_r$ such that $I_n = E_r \cdots E_1 A$. Let $E = E_r \cdots E_1$, which is invertible. Then, we have

  $$\text{rank}(A) = \dim(\text{col}(A)) = \dim(\text{col}(EA)) = \dim(\text{col}(I_n)) = \dim(\mathbb{R}^n) = n.$$

  □

  Hence, as expected, an *invertible* matrix has no degree of non-invertibility.
- The 3×3 matrix $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ has rank 2 since its RREF is $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$, which has two nonzero rows. While this matrix is not invertible, its rank suggests that its "degree of non-invertibility" is not very high.

3.10 Null Spaces

3.10.1 So far we have introduced two kinds of spaces that are related to a matrix: column and row spaces. We will introduce the third kind here, which is about the concept of the system of linear equations.

3.10.2 Let A be an $m \times n$ matrix. Then the **null space** of A is given by $\text{null}(A) = \{\boldsymbol{x} \in \mathbb{R}^n : A\boldsymbol{x} = \mathbf{0}\}$, i.e., the solution set of the homogeneous system $A\boldsymbol{x} = \mathbf{0}$.

3.10.3 The following result suggests that null space is indeed a vector subspace of $\mathbb{R}^n$.

Theorem 3.10.a. Let A be an $m \times n$ matrix. Then, the null space $\text{null}(A)$ is a vector subspace of $\mathbb{R}^n$.

Proof. Fix any $\boldsymbol{u}, \boldsymbol{v} \in \text{null}(A)$. Then, $A\boldsymbol{u} = A\boldsymbol{v} = \boldsymbol{0}$.

<u>Closed under addition</u>: We have $A(\boldsymbol{u}+\boldsymbol{v}) = A\boldsymbol{u} + A\boldsymbol{v} = \boldsymbol{0}+\boldsymbol{0} = \boldsymbol{0}$, thus $\boldsymbol{u}+\boldsymbol{v} \in \text{null}(A)$.

<u>Closed under scalar multiplication</u>: For any $a \in \mathbb{R}$, $A(a\boldsymbol{v}) = aA\boldsymbol{v} = a\boldsymbol{0} = \boldsymbol{0}$, thus $a\boldsymbol{v} \in \text{null}(A)$. ☐

3.10.4 Like column and row spaces, we would like to find dimensions and bases of null spaces. They can be found as suggested by the following result.

Theorem 3.10.b. Let A be an $m \times n$ matrix and R be the RREF of A.

(a) The dimension $\dim(\text{null}(A))$, called the **nullity** of A and denoted by $\text{nullity}(A)$, equals the number of free variables in the system $A\boldsymbol{x} = \boldsymbol{0}$, or equivalently, $R\boldsymbol{x} = \boldsymbol{0}$.

(b) Let $s_1, \ldots, s_r$ be the parameters assigned to the free variables. Express the null space of A, i.e., the solution set of the homogeneous system $A\boldsymbol{x} = \boldsymbol{0}$, as $\{s_1\boldsymbol{v}_1 + \cdots + s_r\boldsymbol{v}_r : s_1, \ldots, s_r \in \mathbb{R}\}$, where $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r \in \mathbb{R}^n$.[8] Then, the set $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}$ is a basis for $\text{null}(A)$.

Proof. Note that (b) implies (a) by the definition of dimension. So it suffices to prove (b).

Firstly, we observe from the above expression of null space that

$$\text{null}(A) = \{s_1\boldsymbol{v}_1 + \cdots + s_r\boldsymbol{v}_r : s_1, \ldots, s_r \in \mathbb{R}\} = \text{span}\left(\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}\right).$$

This shows $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}$ spans $\text{null}(A)$.

Next, note that for every $i = 1, \ldots, r$, the vector $\boldsymbol{v}_i$ has (i) a nonzero entry at the position for the corresponding free variable in each solution from the solution set, and (ii) zero entries at the positions for the rest of the free variables. Thus, $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}$ is linearly independent. ☐

3.10.5 Example: Let $A = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$. Then the solution set of $A\boldsymbol{x} = \boldsymbol{0}$ is $\text{null}(A) = \{(x_1, x_2, x_3, x_4)^T : x_1 + x_2 + x_3 + x_4 = 0\}$. We can write

$$\text{null}(A) = \left\{ \begin{bmatrix} -s-t-u \\ s \\ t \\ u \end{bmatrix} \in \mathbb{R}^4 : s, t, u \in \mathbb{R} \right\} = \left\{ s\begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + t\begin{bmatrix} -1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + u\begin{bmatrix} -1 \\ 0 \\ 0 \\ 1 \end{bmatrix} : s, t, u \in \mathbb{R} \right\},$$

thus a basis for $\text{null}(A)$ is $\left\{ \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right\}$.

[8] This is always possible for a *homogeneous* system. Each solution in the general solution is a vector involving free variables $s_1, \ldots, s_r$ *without* constant term due to the homogeneity. Then, each general solution can be "split" into $s_1\boldsymbol{v}_1, \ldots, s_r\boldsymbol{v}_r$.

4 Linear Transformations

4.0.1 We have mentioned in Sections 1.4 and 1.5 that matrix-vector product and matrix multiplication are actually related to the concept of *linear transformation*. As we have mentioned at the very beginning of this notes, linear transformation is another central concept in linear algebra, apart from vector space. So we will investigate linear transformations in Section 4.

4.1 Linear Transformations

4.1.1 Given two vector spaces, we can define many functions by treating one of them as domain as another as codomain. However, not all such functions are said to be *linear transformations*. To qualify as a linear transformation, we impose an additional constraint: The operations on vector spaces, namely vector addition and scalar multiplication, should be preserved.

4.1.2 Let V and W be vector spaces. A function $T: V \to W$ is a **linear transformation** from V to W if for any $\boldsymbol{u}, \boldsymbol{v} \in V$ and any scalar $c \in \mathbb{R}$,

(a) (preserving vector addition) $T(\boldsymbol{u}+\boldsymbol{v}) = T(\boldsymbol{u}) + T(\boldsymbol{v})$;

(b) (preserving scalar multiplication) $T(c\boldsymbol{v}) = cT(\boldsymbol{v})$.

Examples:

- A function $T: \mathbb{R}^2 \to \mathbb{R}^2$ defined by $T\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = 3\begin{bmatrix} x \\ y \end{bmatrix}$ is a linear transformation.

  Proof. Exercise. □

- A function $T: \mathbb{R}^n \to \mathbb{R}$ defined by $T\left(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}\right) = x_1 + \cdots + x_n$ is a linear transformation.

  Proof. Exercise. □

- A function $T: \mathbb{R}^3 \to \mathbb{R}^2$ defined by $T\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\right) = \begin{bmatrix} x_1 + x_2 \\ x_2 - 2x_3 \end{bmatrix}$ is a linear transformation.

  Proof. Fix any $\boldsymbol{u} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ and $\boldsymbol{v} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$ in $\mathbb{R}^3$. Then,

$$\begin{aligned} T(\boldsymbol{u}+\boldsymbol{v}) &= T\left(\begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{bmatrix}\right) \\ &= \begin{bmatrix} x_1 + y_1 + x_2 + y_2 \\ x_2 + y_2 - 2(x_3 + y_3) \end{bmatrix} \\ &= \begin{bmatrix} x_1 + x_2 \\ x_2 - 2x_3 \end{bmatrix} + \begin{bmatrix} y_1 + y_2 \\ y_2 - 2y_3 \end{bmatrix} \\ &= T\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\right) + T\left(\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}\right) \\ &= T(\boldsymbol{u}) + T(\boldsymbol{v}). \end{aligned}$$

  Next, for any $c \in \mathbb{R}$, we have

$$T(c\boldsymbol{v}) = T\left(c\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\right) = T\left(\begin{bmatrix} cx_1 \\ cx_2 \\ cx_3 \end{bmatrix}\right) = \begin{bmatrix} cx_1 + cx_2 \\ cx_2 - 2cx_3 \end{bmatrix} = c\begin{bmatrix} x_1 + x_2 \\ x_2 - 2x_3 \end{bmatrix} = cT\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\right) = cT(\boldsymbol{v}).$$

  □

4.1.3 To connect the concepts of matrix-vector product and linear transformation, consider the following. Let A be an $m \times n$ matrix, and $L_A : \mathbb{R}^n \to \mathbb{R}^m$ be defined by $L_A(\boldsymbol{v}) = A\boldsymbol{v}$ for any $\boldsymbol{v} \in \mathbb{R}^n$. Then L_A is a linear transformation.

Proof. Fix any $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^n$. Firstly, we have $L_A(\boldsymbol{u}+\boldsymbol{v}) = A(\boldsymbol{u}+\boldsymbol{v}) = A\boldsymbol{u} + A\boldsymbol{v} = L_A(\boldsymbol{u}) + L_A(\boldsymbol{v})$. Next, for any $c \in \mathbb{R}$, we have $L_A(c\boldsymbol{v}) = A(c\boldsymbol{v}) = c(A\boldsymbol{v}) = cL_A(\boldsymbol{v})$. □

4.1.4 Two special kinds of linear transformations are as follows. Let V and W be vector spaces.

- The identity function $\mathrm{id}_V : V \to V$, defined by $\mathrm{id}_V(\boldsymbol{v}) = \boldsymbol{v}$ for any $\boldsymbol{v} \in V$, is a linear transformation. It is called the **identity transformation**.

  Proof. To prove that it is a linear transformation, first fix any $\boldsymbol{u}, \boldsymbol{v} \in V$. Then,

  $$\mathrm{id}_V(\boldsymbol{u}+\boldsymbol{v}) = \boldsymbol{u}+\boldsymbol{v} = \mathrm{id}_V(\boldsymbol{u}) + \mathrm{id}_V(\boldsymbol{v})$$

  and for any $c \in \mathbb{R}$, we have

  $$\mathrm{id}_V(c\boldsymbol{v}) = c\boldsymbol{v} = c\,\mathrm{id}_V(\boldsymbol{v}).$$

  □

- The zero function $T_0 : V \to W$, defined by $T_0(\boldsymbol{v}) = \mathbf{0}$[9] for any $\boldsymbol{v} \in V$, is a linear transformation. It is called the **zero transformation**.

  Proof. Again first fix any $\boldsymbol{u}, \boldsymbol{v} \in V$. Then,

  $$T_0(\boldsymbol{u}+\boldsymbol{v}) = \mathbf{0} = \mathbf{0} + \mathbf{0} = T_0(\boldsymbol{u}) + T_0(\boldsymbol{v})$$

  and for any $c \in \mathbb{R}$, we have

  $$T_0(c\boldsymbol{v}) = \mathbf{0} = c\mathbf{0} = cT_0(\boldsymbol{v}).$$

  □

For the identity transformation, if $V = \mathbb{R}^n$, then it is indeed a special case of the linear transformation in [4.1.3] with $A = I_n$. For the zero transformation, if $V = \mathbb{R}^n$ and $W = \mathbb{R}^m$, then it is a special case of the linear transformation in [4.1.3] with $A = O_{m\times n}$. Note however that the identity and zero transformations can be defined for arbitrary vector spaces, not limited to $\mathbb{R}^n$.

4.1.5 The following result suggests that linear transformation also preserves *zero* and *linear combinations*.

Proposition 4.1.a. Let $T : V \to W$ be a linear transformation. Then:

(a) $T(\mathbf{0}) = \mathbf{0}$. [Note: The $\mathbf{0}$ in the LHS denotes the zero vector in V, while the $\mathbf{0}$ in the RHS denotes the zero vector in W.]

(b) Let n be any positive integer. For any $a_1, \ldots, a_n \in \mathbb{R}$ and any $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in V$,

$$T(a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n) = a_1T(\boldsymbol{v}_1) + \cdots + a_nT(\boldsymbol{v}_n).$$

Proof.

(a) Fix any $\boldsymbol{v} \in V$ and note that

$$T(\mathbf{0}) = T(0\boldsymbol{v}) = 0T(\boldsymbol{v}) = \mathbf{0},$$

by Proposition 3.1.a.

(b) We prove by induction. The case $n = 1$ follows immediately from the definition of linear transformation (preservation of scalar multiplication). Now assume that the case $n = k$ for a $k \in \mathbb{N}$, i.e.,

$$T(a_1\boldsymbol{v}_1 + \cdots + a_k\boldsymbol{v}_k) = a_1T(\boldsymbol{v}_1) + \cdots + a_kT(\boldsymbol{v}_k).$$

[9] Note that $\mathbf{0}$ is the zero vector in W.

Consider

$$\begin{aligned} T(a_1\boldsymbol{v}_1 + \cdots + a_k\boldsymbol{v}_k + a_{k+1}\boldsymbol{v}_{k+1}) &= T(a_1\boldsymbol{v}_1 + \cdots + a_k\boldsymbol{v}_k) + T(a_{k+1}\boldsymbol{v}_{k+1}) \\ &= a_1T(\boldsymbol{v}_1) + \cdots + a_kT(\boldsymbol{v}_k) + T(a_{k+1}\boldsymbol{v}_{k+1}) \\ &= a_1T(\boldsymbol{v}_1) + \cdots + a_kT(\boldsymbol{v}_k) + a_{k+1}T(\boldsymbol{v}_{k+1}), \end{aligned}$$

so the case $n = k + 1$ holds, hence the result follows by induction.

□

4.1.6 More advanced examples of linear transformations:

- Let V be the vector space of differentiable functions from $\mathbb{R}$ to $\mathbb{R}$. (It can be proved that V is a vector subspace of the vector space of all functions from $\mathbb{R}$ to $\mathbb{R}$.) Define a function $T : V \to V$ by $T(f) = f'$ for any $f \in V$. Then T is a linear transformation.

  Proof. Fix any $f_1, f_2 \in V$. Firstly, we have

  $$T(f_1 + f_2) = (f_1 + f_2)' = f_1' + f_2' = T(f_1) + T(f_2).$$

  Next, for any $c \in \mathbb{R}$, we have

  $$T(cf_1) = (cf_1)' = cf_1' = cT(f_1).$$

  □

- Let V be the vector space of all $m \times n$ matrices, P be an $m \times m$ matrix, and Q be an $n \times n$ matrix. Define a function $T : V \to V$ by $T(A) = PAQ$ for any $A \in V$. Then T is a linear transformation.

  Proof. Fix any $A, B \in V$. Firstly, we have

  $$T(A + B) = P(A + B)Q = P(AQ + BQ) = PAQ + PBQ = T(A) + T(B).$$

  Next, for any $c \in \mathbb{R}$, we have

  $$T(cA) + P(cA)Q = cPAQ = cT(A).$$

  □

4.1.7 The following is a non-example of linear transformation. Let V be the vector space of $n \times n$ matrices. Define $T : V \to V$ by $T(A) = A^2$. Then T is *not* a linear transformation since $T(2I_n) = (2I_n)^2 = 4I_n^2 = 4T(I_n) \neq 2T(I_n)$.

4.1.8 To obtain more examples of linear transformations, we can utilize the following result to construct linear transformations from *bases*.

Theorem 4.1.b. Let V and W be vector spaces. Let $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ be a basis for V and let $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n \in W$. Then there exists a unique linear transformation $T : V \to W$ such that $T(\boldsymbol{v}_i) = \boldsymbol{w}_i$ for every $i = 1, \ldots, n$.

[Note: This result does not say that $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$ is a basis for W.]

Proof. Existence: Fix any $\boldsymbol{v} \in V$. By Theorem 3.4.a, the vector $\boldsymbol{v}$ can be written as $a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$ for some unique scalars $a_1, \ldots, a_n \in \mathbb{R}$. Then define $T : V \to W$ by

$$T(\boldsymbol{v}) = a_1\boldsymbol{w}_1 + \cdots + a_n\boldsymbol{w}_n.$$

Note that for every $i = 1, \ldots, n$, we have $T(\boldsymbol{v}_i) = \boldsymbol{w}_i$ since the corresponding unique scalars are $a_i = 1$ and $a_j = 0$ for any $j \neq i$. We also claim that T is a linear transformation.

Proof. Addition: Fix any $\boldsymbol{v}, \boldsymbol{v}' \in V$. By Theorem 3.4.a, we can write

$$\boldsymbol{v} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n \quad \text{and} \quad \boldsymbol{v}' = a_1'\boldsymbol{v}_1 + \cdots + a_n'\boldsymbol{v}_n$$

for some unique scalars $a_1, \ldots, a_n, a'_1, \ldots, a'_n \in \mathbb{R}$. Note that

$$\boldsymbol{v} + \boldsymbol{v}' = (a_1 + a'_1)\boldsymbol{v}_1 + \cdots + (a_n + a'_n)\boldsymbol{v}_n,$$

thus

$$T(\boldsymbol{v}+\boldsymbol{v}') = (a_1 + a'_1)\boldsymbol{w}_1+\cdots+(a_n + a'_n)\boldsymbol{w}_n = (a_1\boldsymbol{w}_1+\cdots+a_n\boldsymbol{w}_n)+(a'_1\boldsymbol{w}_1+\cdots+a'_n\boldsymbol{w}_n) = T(\boldsymbol{v})+T(\boldsymbol{v}').$$

Scalar multiplication: Fix any $\boldsymbol{v} \in V$ and $c \in \mathbb{R}$. By Theorem 3.4.a, write $\boldsymbol{v} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$ for some unique scalars $a_1, \ldots, a_n \in \mathbb{R}$. Then we have $c\boldsymbol{v} = (ca_1)\boldsymbol{v}_1 + \cdots + (ca_n)\boldsymbol{v}_n$, thus

$$T(c\boldsymbol{v}) = (ca_1)\boldsymbol{w}_1 + \cdots + (ca_n)\boldsymbol{w}_n = c(a_1\boldsymbol{w}_1 + \cdots + a_n\boldsymbol{w}_n) = cT(\boldsymbol{v}).$$

□

Uniqueness: Let $T' : V \to W$ be another linear transformation satisfying $T'(\boldsymbol{v}_i) = \boldsymbol{w}_i$ for every $i = 1, \ldots, n$. Fix any $\boldsymbol{v} \in V$. Then there are unique scalars $a_1, \ldots, a_n$ such that $\boldsymbol{v} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$. Hence,

$$\begin{aligned}
T'(\boldsymbol{v}) &= T'(a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n) \\
&= a_1T'(\boldsymbol{v}_1) + \cdots + a_nT'(\boldsymbol{v}_n) \\
&= a_1\boldsymbol{w}_1 + \cdots + a_n\boldsymbol{w}_n \\
&= a_1T(\boldsymbol{v}_1) + \cdots + a_nT(\boldsymbol{v}_n) \\
&= T(a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n) \\
&= T(\boldsymbol{v}).
\end{aligned}$$

Since this holds for arbitrary $\boldsymbol{v} \in V$, we conclude that $T' = T$. □

4.2 Null Spaces and Ranges

4.2.1 Given an $m \times n$ matrix, we can obtain its corresponding null space and column space, as suggested in Sections 3.7 and 3.10. We can do similar things for a linear transformation, and consider its *null space* and *range*.

4.2.2 Let $T : V \to W$ be a linear transformation. The **null space** of T, denoted by $\text{null}(T)$, is given by $\{\boldsymbol{v} \in V : T(\boldsymbol{v}) = \boldsymbol{0}\}$. [Note: Here $\boldsymbol{0}$ denotes the zero vector in W.]

The **range** of T, denoted by $\text{ran}(T)$, is given by $\text{ran}(T) = \{T(\boldsymbol{v}) \in W : \boldsymbol{v} \in V\}$. [Note: This coincides with the usual definition of range for a function.]

4.2.3 Examples:

- Consider the zero transformation $T_0 : V \to W$, defined by $T_0(\boldsymbol{v}) = \boldsymbol{0}$ for any $\boldsymbol{v} \in V$. Then, $\text{null}(T_0) = V$ and $\text{ran}(T_0) = \{\boldsymbol{0}\}$.
- Consider the identity transformation $\text{id}_V : V \to V$, defined by $\text{id}_V(\boldsymbol{v}) = \boldsymbol{v}$ for any $\boldsymbol{v} \in V$. Then, $\text{null}(\text{id}_V) = \{\boldsymbol{0}\}$ and $\text{ran}(\text{id}_V) = V$.
- Let $T : \mathbb{R}^{2n} \to \mathbb{R}^n$ be defined by

$$T(\boldsymbol{v}) = \begin{bmatrix} I_n & O_{n\times n} \\ O_{n\times n} & O_{n\times n} \end{bmatrix}\boldsymbol{v}$$

for any $\boldsymbol{v} \in \mathbb{R}^{2n}$. Then,

$$\text{null}(T) = \left\{ \begin{bmatrix} 0 \\ \vdots \\ 0 \\ x_{n+1} \\ \vdots \\ x_{2n} \end{bmatrix} : x_{n+1}, \ldots, x_{2n} \in \mathbb{R} \right\}$$

and

$$\operatorname{ran}(T) = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \\ 0 \\ \vdots \\ 0 \end{bmatrix} : x_1, \ldots, x_n \in \mathbb{R} \right\}.$$

4.2.4 Let A be an $m \times n$ matrix and let $L_A : \mathbb{R}^n \to \mathbb{R}^m$ be the associated linear transformation, i.e., the one defined by $L_A(\boldsymbol{v}) = A\boldsymbol{v}$ for any $\boldsymbol{v} \in \mathbb{R}^n$.

The null space of L_A is

$$\operatorname{null}(L_A) = \{\boldsymbol{v} \in \mathbb{R}^n : L_A(\boldsymbol{v}) = \boldsymbol{0}\} = \{\boldsymbol{v} \in \mathbb{R}^n : A\boldsymbol{v} = \boldsymbol{0}\} = \operatorname{null}(A)$$

as expected. On the other hand, the range of L_A is

$$\operatorname{ran}(L_A) = \{L_A(\boldsymbol{v}) \in \mathbb{R}^m : \boldsymbol{v} \in \mathbb{R}^n\} = \{A\boldsymbol{v} \in \mathbb{R}^m : \boldsymbol{v} \in \mathbb{R}^n\} = \operatorname{col}(A).$$

From this, we can see that the notions of null space and range of a linear transformation can be seen as generalizations to the concepts of null space and column space for a matrix, respectively.

4.2.5 Like the null space and column space of a matrix, the null space and range of a linear transformation are vector subspaces.

Proposition 4.2.a. Let $T : V \to W$ be a linear transformation. Then $\operatorname{null}(T)$ and $\operatorname{ran}(T)$ are vector subspaces of V and W respectively.

Proof. First consider $\operatorname{null}(T)$. Closed under addition: For any $\boldsymbol{v}, \boldsymbol{w} \in \operatorname{null}(T)$, we have $T(\boldsymbol{v}) = T(\boldsymbol{w}) = \boldsymbol{0}$, thus $T(\boldsymbol{v} + \boldsymbol{w}) = T(\boldsymbol{v}) + T(\boldsymbol{w}) = \boldsymbol{0}$. Hence, $\boldsymbol{v} + \boldsymbol{w} \in \operatorname{null}(T)$.

Closed under scalar multiplication: For any $c \in \mathbb{R}$ and any $\boldsymbol{v} \in V$, we have $T(c\boldsymbol{v}) = cT(\boldsymbol{v}) = \boldsymbol{0}$, thus $c\boldsymbol{v} \in \operatorname{null}(T)$.

Next consider $\operatorname{ran}(T)$. Closed under addition: For any $\boldsymbol{v}', \boldsymbol{w}' \in \operatorname{ran}(T)$, $v' = T(\boldsymbol{v})$ and $\boldsymbol{w}' = T(\boldsymbol{w})$ for some $\boldsymbol{v}, \boldsymbol{w} \in V$. Thus, $\boldsymbol{v}' + \boldsymbol{w}' = T(\boldsymbol{v}) + T(\boldsymbol{w}) = T(\boldsymbol{v} + \boldsymbol{w}) \in \operatorname{ran}(T)$.

Closed under scalar multiplication: For any $c \in \mathbb{R}$ and any $v' \in \operatorname{ran}(T)$, we have $v' = T(\boldsymbol{v})$ for some $\boldsymbol{v} \in V$. Hence, $c\boldsymbol{v}' = cT(\boldsymbol{v}) = T(c\boldsymbol{v}) \in \operatorname{ran}(T)$. □

4.2.6 To find the range of a linear transformation, the following result can be of use.

Proposition 4.2.b. Let $T : V \to W$ be a linear transformation and $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ be a basis for V. Then

$$\operatorname{ran}(T) = \operatorname{span}(\{T(\boldsymbol{v}_1), \ldots, T(\boldsymbol{v}_n)\}).$$

Proof. "$\supseteq$": For any $\boldsymbol{w} \in \operatorname{span}(\{T(\boldsymbol{v}_1), \ldots, T(\boldsymbol{v}_n)\})$, we have for some $a_1, \ldots, a_n \in \mathbb{R}$,

$$\boldsymbol{w} = a_1 T(\boldsymbol{v}_1) + \cdots + a_n T(\boldsymbol{v}_n) = T(a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n) \in \operatorname{ran}(T).$$

"$\subseteq$": For any $\boldsymbol{w} \in \operatorname{ran}(T)$, we know $\boldsymbol{w} = T(\boldsymbol{v})$ for some $\boldsymbol{v} \in V$. By the spanning property of basis, $\boldsymbol{v} = b_1\boldsymbol{v}_1 + \cdots + b_n\boldsymbol{v}_n$ for some $b_1, \ldots, b_m \in \mathbb{R}$. Thus

$$\boldsymbol{w} = T(b_1\boldsymbol{v}_1 + \cdots + b_n\boldsymbol{v}_n) = b_1 T(\boldsymbol{v}_1) + \cdots + b_n T(\boldsymbol{v}_n) \in \operatorname{span}(\{T(\boldsymbol{v}_1), \ldots, T(\boldsymbol{v}_n)\}).$$

□

This result tells us that we can obtain the range of a linear transformation by first finding a basis for the domain V. Then, after applying the linear transformation on each vector in the basis, the range would just be the span of those transformed vectors.

4.2.7 Example: Let $T : \mathbb{R}^3 \to \mathbb{R}^2$ be defined by $T\left(\begin{bmatrix} x \\ y \\ z \end{bmatrix}\right) = \begin{bmatrix} x-y \\ y-z \end{bmatrix}$. Then, the null space and the range of T are given by:

- *null space:* We first solve the system of linear equations

$$\begin{cases} x - y \phantom{{}-z} = 0 \\ \phantom{x-{}} y - z = 0 \end{cases}.$$

The null space $\text{null}(T)$ is just the solution set $\{(t,t,t) \in \mathbb{R}^3 : t \in \mathbb{R}\}$.

- *range:* Consider the standard basis $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$ for $\mathbb{R}^3$. Then, by Proposition 4.2.b,

$$\text{ran}(T) = \text{span}\left(\{T(\boldsymbol{e}_1), T(\boldsymbol{e}_2), T(\boldsymbol{e}_3)\}\right) = \text{span}\left(\left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right\}\right) = \mathbb{R}^2,$$

where we get the last equality from the observation that $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ already span $\mathbb{R}^2$.

4.2.8 The concepts of null space and range of a linear transformation can be neatly related by an important result called *dimension formula*. Before stating that, we first introduce some preliminary notions. Let $T : V \to W$ be a linear transformation.

- The **nullity** of T, denoted by $\text{nullity}(T)$, is the dimension of $\text{null}(T)$.
- The **rank** of T, denoted by $\text{rank}(T)$, is the dimension of $\text{ran}(T)$.

By [4.2.4], given an $m \times n$ matrix A and letting $L_A : \mathbb{R}^n \to \mathbb{R}^m$ be defined by $L_A(\boldsymbol{v}) = A\boldsymbol{v}$ for any $\boldsymbol{v} \in \mathbb{R}^m$, we know that

- $\text{nullity}(L_A) = \dim(\text{null}(A)) = \text{nullity}(A)$.
- $\text{rank}(L_A) = \dim(\text{col}(A)) = \text{rank}(A)$.

4.2.9 The dimension formula is as follows.

Theorem 4.2.c (Dimension formula)**.** Let $T : V \to W$ be a linear transformation. Then

$$\text{nullity}(T) + \text{rank}(T) = \dim(V).$$

Proof. Let $k = \text{nullity}(T)$ and $m = \dim(V)$. Let $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_k\}$ be a basis for $\text{null}(T)$, which is linearly independent in V. By the extension approach in Section 3.6, we can find vectors $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{m-k}$ such that $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_k, \boldsymbol{u}_1, \dots, \boldsymbol{u}_{m-k}\}$ is a basis for V.

By Proposition 4.2.b,

$$\begin{aligned} \text{ran}(T) &= \text{span}\left(\{T(\boldsymbol{v}_1), \dots, T(\boldsymbol{v}_k), T(\boldsymbol{u}_1), \dots, T(\boldsymbol{u}_{m-k})\}\right) \\ &= \text{span}\left(\{\boldsymbol{0}, \dots, \boldsymbol{0}, T(\boldsymbol{u}_1), \dots, T(\boldsymbol{u}_{m-k})\}\right) \\ &= \text{span}\left(\{T(\boldsymbol{u}_1), \dots, T(\boldsymbol{u}_{m-k})\}\right). \end{aligned}$$

Next, we shall show that $\{T(\boldsymbol{u}_1), \dots, T(\boldsymbol{u}_{m-k})\}$ is linearly independent as well, thus forming a basis for $\text{ran}(T)$. Consider

$$a_1 T(\boldsymbol{u}_1) + \cdots + a_{m-k} T(\boldsymbol{u}_{m-k}) = \boldsymbol{0},$$

which implies $T(a_1\boldsymbol{u}_1 + \cdots + a_{m-k}\boldsymbol{u}_{m-k}) = \boldsymbol{0}$, thus $a_1\boldsymbol{u}_1 + \cdots + a_{m-k}\boldsymbol{u}_{m-k} \in \text{null}(T)$. Then, by the spanning property of the basis $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_k\}$ for $\text{null}(T)$, we know

$$a_1\boldsymbol{u}_1 + \cdots + a_{m-k}\boldsymbol{u}_{m-k} = b_1\boldsymbol{v}_1 + \cdots + b_k\boldsymbol{v}_k$$

for some $b_1, \dots, b_k \in \mathbb{R}$. Rearranging it gives

$$a_1\boldsymbol{u}_1 + \cdots + a_{m-k}\boldsymbol{u}_{m-k} - b_1\boldsymbol{v}_1 - \cdots - b_k\boldsymbol{v}_k = \mathbf{0}.$$

Since $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_k, \boldsymbol{u}_1, \dots, \boldsymbol{u}_{m-k}\}$ is a basis for V and hence linearly independent, we have

$$a_1 = \cdots = a_{m-k} = -b_1 = \cdots = -b_k = 0,$$

which in particular implies $a_1 = \cdots = a_{m-k} = 0$. So $\{T(\boldsymbol{u}_1), \dots, T(\boldsymbol{u}_{m-k})\}$ is linearly independent, and thus is a basis for $\operatorname{ran}(T)$. This shows $\operatorname{rank}(T) = \dim(\operatorname{ran}(T)) = m - k = \dim(V) - \operatorname{nullity}(T)$, as desired. $\square$

4.2.10 By setting T to be $L_A : \mathbb{R}^n \to \mathbb{R}^m$ defined by $L_A(\boldsymbol{v}) = A\boldsymbol{v}$ for any $\boldsymbol{v} \in \mathbb{R}^n$ where A is an $m \times n$ matrix, the equality in the dimension formula reduces to

$$\operatorname{nullity}(A) + \operatorname{rank}(A) = \dim(\mathbb{R}^n) = n = \text{number of columns of } A.$$

This special case is known as the *rank-nullity theorem*.

4.3 Injectivity and Surjectivity

4.3.1 Next, we will consider the injectivity and surjectivity of a linear transformation, which turn out to be related to the concepts of null space and range.

4.3.2 A criterion for injectivity based on null space is as follows.

Proposition 4.3.a. Let $T : V \to W$ be a linear transformation. Then T is injective iff $\operatorname{null}(T) = \{\mathbf{0}\}$.

Proof. "$\Rightarrow$": Assume T is injective. Fix any $\boldsymbol{v} \in \operatorname{null}(T)$ and we have $T(\boldsymbol{v}) = \mathbf{0} = T(\mathbf{0})$, where the last equality is a property of linear transformation. By the injectivity of T, it follows that $\boldsymbol{v} = \mathbf{0}$. This shows $\operatorname{null}(T) \subseteq \{\mathbf{0}\}$. But another subset inclusion is immediate as $T(\mathbf{0}) = \mathbf{0}$ always, thus $\mathbf{0} \in \operatorname{null}(T)$.

"$\Leftarrow$": Assume $\operatorname{null}(T) = \{\mathbf{0}\}$. Fix any $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ with $T(\boldsymbol{v}_1) = T(\boldsymbol{v}_2)$. Then,

$$\begin{aligned} & T(\boldsymbol{v}_1) - T(\boldsymbol{v}_2) = \mathbf{0} \\ \implies & T(\boldsymbol{v}_1 - \boldsymbol{v}_2) = \mathbf{0} \\ \implies & \boldsymbol{v}_1 - \boldsymbol{v}_2 = \mathbf{0} && \text{(since null}(T) = \{\mathbf{0}\}) \\ \implies & \boldsymbol{v}_1 = \boldsymbol{v}_2. \end{aligned}$$

This shows T is injective. $\square$

[Note: Practically, it suffices to only prove that $\operatorname{null}(T) \subseteq \{\mathbf{0}\}$ to show that T is injective, since the another subset inclusion is immediate from the property that $T(\mathbf{0}) = \mathbf{0}$.]

4.3.3 We can extend Proposition 4.3.a by utilizing the dimension formula (Theorem 4.2.c).

Theorem 4.3.b. Let $T : V \to W$ be a linear transformation. Then the following are equivalent.

(a) T is injective.
(b) $\operatorname{null}(T) = \{\mathbf{0}\}$.
(c) $\operatorname{rank}(T) = \dim(V)$.

Proof. (a) $\iff$ (b) follows from Proposition 4.3.a. So it suffices to show that (b) $\iff$ (c).

(b) $\implies$ (c): Assume $\operatorname{null}(T) = \{\mathbf{0}\}$. Then, we have $\operatorname{nullity}(T) = 0$ and by Theorem 4.2.c, $\operatorname{rank}(T) = \dim(V) - 0 = \dim(V)$.

(c) $\implies$ (b): Assume $\operatorname{rank}(T) = \dim(V)$. By Theorem 4.2.c, $\operatorname{nullity}(T) = \dim(V) - \operatorname{rank}(T) = \dim(V) - \dim(V) = 0$. This means $\dim(\operatorname{null}(T)) = 0$. But the only vector space with zero dimension is the zero vector space $\{\mathbf{0}\}$. Hence $\operatorname{null}(T) = \{\mathbf{0}\}$. $\square$

4.3.4 To show that a linear transformation is *not* injective, the following result provides a convenient tool.

Proposition 4.3.c. Let $T : V \to W$ be a linear transformation. If $\dim(V) > \dim(W)$, then T is not injective.

Proof. We prove by contrapositive. Suppose T is injective. Then by Theorem 4.3.b, $\operatorname{rank}(T) = \dim(\operatorname{ran}(T)) = \dim(V)$. But on the other hand, as $\operatorname{ran}(T)$ is a subspace of W, we have $\operatorname{rank}(T) = \dim(\operatorname{ran}(T)) \leq \dim(W)$. This shows $\dim(V) \leq \dim(W)$. □

4.3.5 After discussing injectivity, we shall also discuss surjectivity in the following result. It gives us a criterion for the bijectivity (i.e., both injectivity and surjectivity) of a linear transformation. Before proving it, we consider the following lemma.

Lemma 4.3.d. Let V be a vector space. If W is a subspace of V with $\dim(W) = \dim(V)$, then $W = V$.

Proof. Assume to the contrary that W is a proper subset of V while $\dim(W) = \dim(V)$. Then there exists $\boldsymbol{w} \in V \setminus W$. Let β be a basis for W. We know that $|\beta| = \dim(W) = \dim(V)$ and $\operatorname{span}(\beta) = W$. Since $\boldsymbol{w} \notin W = \operatorname{span}(\beta)$ and β is linearly independent in V, by Theorem 3.6.a, the union $\beta \cup \{\boldsymbol{w}\}$ is linearly independent in V. But then this contradicts Proposition 3.5.a as $|\beta \cup \{\boldsymbol{w}\}| > \dim(V)$. □

Theorem 4.3.e. Let $T : V \to W$ be a linear transformation. Then T is bijective iff $\operatorname{null}(T) = \{\mathbf{0}\}$ and $\dim(V) = \dim(W)$.

Proof. "$\Rightarrow$": Assume T is bijective. Then by the injectivity of T, we have $T = \{\mathbf{0}\}$, thus $\operatorname{nullity}(T) = 0$. On the other hand, by the surjectivity of T, we have by definition $\operatorname{ran}(T) = W$, so $\operatorname{rank}(T) = \dim(W)$. Finally, by Theorem 4.2.c, we have $\dim(V) = \operatorname{rank}(T) + \operatorname{nullity}(T) = \operatorname{rank}(T) = \dim(W)$.

"$\Leftarrow$" Assume $\operatorname{null}(T) = \{\mathbf{0}\}$ and $\dim(V) = \dim(W)$. The first condition implies that T is injective and $\operatorname{nullity}(T) = 0$. Next, by Theorem 4.2.c, $\dim(W) = \dim(V) = \operatorname{rank}(T) + \operatorname{nullity}(T) = \operatorname{rank}(T) = \dim(\operatorname{ran}(T))$. Since $\operatorname{ran}(T)$ is a subspace of W, we have $\operatorname{ran}(T) = W$ by Lemma 4.3.d.

Thus, T is surjective. Together with the injectivity of T shown before, we conclude that T is bijective. □

4.3.6 As a corollary, we can obtain several more criteria for bijectivity.

Corollary 4.3.f. Let $T : V \to W$ be a linear transformation. Then, the following are equivalent.

(a) T is bijective.
(b) T is injective and $\dim(V) = \dim(W)$.
(c) T is surjective and $\dim(V) = \dim(W)$.

Proof. <u>(a) $\iff$ (b)</u>:

$$\begin{aligned} & T \text{ is bijective} \\ \iff & \operatorname{null}(T) = \{\mathbf{0}\} \text{ and } \dim(V) = \dim(W) && \text{(Theorem 4.3.e)} \\ \iff & T \text{ is injective and } \dim(V) = \dim(W) && \text{(Proposition 4.3.a).} \end{aligned}$$

<u>(a) $\implies$ (c)</u>: Suppose that T is bijective. Then T is immediately surjective and it suffices to show that $\dim(V) = \dim(W)$. But this just follows from Theorem 4.3.e.

<u>(c) $\implies$ (a)</u>: Suppose that T is surjective and $\dim(V) = \dim(W)$. It then suffices to show that T is injective. Due to the surjectivity of T, we have $\operatorname{rank}(T) = \dim(\operatorname{ran}(T)) = \dim(W) = \dim(V)$. By dimension formula, we get

$$\operatorname{nullity}(T) = \dim(V) - \operatorname{rank}(T) = 0,$$

which forces $\operatorname{null}(T) = \{\mathbf{0}\}$, hence T is injective. □

4.3.7 A bijective linear transformation is said to be an **isomorphism**. Given two vector spaces V and W, if there exists an isomorphism from V to W, then we say that V is **isomorphic** to W. (Intuitively, this means that V and W have the same "structure" in a certain sense.)

4.4 Matrix Representations of Linear Transformations

4.4.1 From [4.1.3], we know that the concepts of matrices and linear transformations can be connected, by considering a linear transformation $L_A : \mathbb{R}^n \to \mathbb{R}^m$ associated to an $m \times n$ matrix A. More generally, we can have a *matrix representation* of any linear transformation, which is the main topic to be discussed in Section 4.4.

4.4.2 An **ordered basis** is a basis equipped with a specific order. For an ordered basis $\beta = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$ for a vector space V, we can say:

- $\boldsymbol{v}_1$ is the first one;
- $\boldsymbol{v}_2$ is the second one;
- ...
- $\boldsymbol{v}_n$ is the last one.

Example: Consider two ordered bases $\beta = \{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ and $\beta' = \{\boldsymbol{e}_2, \boldsymbol{e}_1\}$ for $\mathbb{R}^2$. Note that they are different ordered bases. Although we still use set notation, the order matters!

4.4.3 Before discussing matrix representation of a linear transformation, we shall first introduce matrix representation of a *vector*, as a preliminary notion. Let $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ be an ordered basis for a vector space V. By Theorem 3.4.a, for any $\boldsymbol{v} \in V$, we have

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

for some unique scalars $a_1, \ldots, a_n \in \mathbb{R}$. Using these unique scalars, we define the **coordinate vector of $\boldsymbol{v}$ with respect to β** by

$$[\boldsymbol{v}]_\beta = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

Through this, we represent a vector using an $n \times 1$ matrix.

In fact, the function $[\cdot]_\beta : V \to \mathbb{R}^n$ is a linear transformation.

Proof. Fix any $\boldsymbol{u}, \boldsymbol{v} \in V$. Suppose that we can write $\boldsymbol{u} = a_1'\boldsymbol{v}_1 + \cdots + a_n'\boldsymbol{v}_n$ and $\boldsymbol{v} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$.

Addition: Note that $\boldsymbol{u} + \boldsymbol{v} = (a_1' + a_1)\boldsymbol{v}_1 + \cdots + (a_n' + a_n)\boldsymbol{v}_n$. Thus,

$$[\boldsymbol{u} + \boldsymbol{v}]_\beta = \begin{bmatrix} a_1' + a_1 \\ \vdots \\ a_n' + a_n \end{bmatrix} = \begin{bmatrix} a_1' \\ \vdots \\ a_n' \end{bmatrix} + \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = [\boldsymbol{u}]_\beta + [\boldsymbol{v}]_\beta.$$

Scalar multiplication: For any $c \in \mathbb{R}$, $c\boldsymbol{v} = (ca_1)\boldsymbol{v}_1 + \cdots + (ca_n)\boldsymbol{v}_n$, thus

$$[c\boldsymbol{v}]_\beta = \begin{bmatrix} ca_1 \\ \vdots \\ ca_n \end{bmatrix} = c\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = c[\boldsymbol{v}]_\beta.$$

□

Furthermore, $[\cdot]_\beta$ is actually an *isomorphism*.

Proof. We shall use Theorem 4.3.e. It is immediate that $\dim(V) = \dim(\mathbb{R}^n) = n$, so it suffices to show that $\text{null}(T) = \{\boldsymbol{0}\}$. "$\supseteq$" is immediate, so we only need to show $\text{null}(T) \subseteq \{\boldsymbol{0}\}$. Fix any $\boldsymbol{v} \in \text{null}(T)$. Then we have $[\boldsymbol{v}]_\beta = \boldsymbol{0}$, which implies $\boldsymbol{v} = 0\boldsymbol{v}_1 + \cdots + 0\boldsymbol{v}_n = \boldsymbol{0}$. □

Consequently, any vector space V with dimension n is isomorphic to $\mathbb{R}^n$.

4.4.4 Examples:

- Let $\beta = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$ be an ordered basis for $\mathbb{R}^2$. Then, since $\boldsymbol{v} = \begin{bmatrix} 2 \\ 4 \end{bmatrix} = 3\begin{bmatrix} 1 \\ 1 \end{bmatrix} - 1\begin{bmatrix} 1 \\ -1 \end{bmatrix}$, we have
$$[\boldsymbol{v}]_\beta = \begin{bmatrix} 3 \\ -1 \end{bmatrix}.$$
- Let $\beta = \{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ be an ordered basis for $\mathbb{R}^2$. Then, since $\boldsymbol{v} = \begin{bmatrix} 2 \\ 4 \end{bmatrix} = 2\boldsymbol{e}_1 + 4\boldsymbol{e}_2$, we have
$$[\boldsymbol{v}]_\beta = \begin{bmatrix} 2 \\ 4 \end{bmatrix}.$$
- Let $\beta = \{\boldsymbol{e}_2, \boldsymbol{e}_1\}$ be an ordered basis for $\mathbb{R}^2$. Then, since $\boldsymbol{v} = \begin{bmatrix} 2 \\ 4 \end{bmatrix} = 4\boldsymbol{e}_2 + 2\boldsymbol{e}_1$, we have
$$[\boldsymbol{v}]_\beta = \begin{bmatrix} 4 \\ 2 \end{bmatrix}.$$
- Let $\mathcal{P}_3$ denote the vector space of all polynomials of degree at most 3, i.e., $\mathcal{P}_3 = \{a_0 + a_1x + a_2x^2 + a_3x^3 : a_0, a_1, a_2, a_3 \in \mathbb{R}\}$. Let $\beta = \{1, 1+x, x^2, x^2+x^3\}$ be an ordered basis for $\mathcal{P}_3$. Then, since $\boldsymbol{v} = 1 + x + x^2 + x^3 = 0(1) + 1(1+x) + 0(x^2) + 1(x^2+x^3)$, we have
$$[\boldsymbol{v}]_\beta = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

4.4.5 Let us now consider matrix representation of a linear transformation. Let $T : V \to W$ be a linear transformation. Since there are two vector spaces involved for a single linear transformation, the definition also involves two ordered bases. We let $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ be an ordered basis for V and $\gamma = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$ be an ordered basis for W. For every $j = 1, \ldots, n$, since $T(\boldsymbol{v}_j) \in W$, by Theorem 3.4.a, we have
$$T(\boldsymbol{v}_j) = a_{1j}\boldsymbol{w}_1 + \cdots + a_{mj}\boldsymbol{w}_m$$
for some unique scalars $a_{1j}, \ldots, a_{mj} \in \mathbb{R}$. From this we know that
$$[T(\boldsymbol{v}_1)]_\gamma = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix}, \quad [T(\boldsymbol{v}_2)]_\gamma = \begin{bmatrix} a_{12} \\ \vdots \\ a_{m2} \end{bmatrix}, \quad \ldots \quad , \quad [T(\boldsymbol{v}_n)]_\gamma = \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix}.$$
Combining all these column vectors into a matrix gives the matrix representation of T. More precisely, the **matrix representation of T relative to β and γ** is the $m \times n$ matrix
$$[T]_\beta^\gamma = \begin{bmatrix} [T(\boldsymbol{v}_1)]_\gamma & \cdots & [T(\boldsymbol{v}_n)]_\gamma \end{bmatrix} = [a_{ij}] = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}.$$
[Note: If $\beta = \gamma$, we sometimes write $[T]_\beta$ instead of $[T]_\beta^\beta$.]

4.4.6 Consider the special case where T is a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$ and we use the standard bases in the matrix representation. Let β and β' be the (ordered) standard bases for $\mathbb{R}^n$ and $\mathbb{R}^m$ respectively. Then $[T]_\beta^{\beta'}$ is called the **standard matrix representation** of T.

Example: Let $T : \mathbb{R}^4 \to \mathbb{R}^3$ be a linear transformation defined by
$$T\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}\right) = \begin{bmatrix} x_1 + x_3 \\ x_2 + x_3 \\ x_1 + x_4 \end{bmatrix}.$$

Then the standard matrix representation of T is

$$[T]_{\beta}^{\beta'} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix},$$

since:

- $T\left(\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = 1\boldsymbol{e}_1 + 0\boldsymbol{e}_2 + 1\boldsymbol{e}_3,$
- $T\left(\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = 0\boldsymbol{e}_1 + 1\boldsymbol{e}_2 + 0\boldsymbol{e}_3,$
- $T\left(\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = 1\boldsymbol{e}_1 + 1\boldsymbol{e}_2 + 0\boldsymbol{e}_3,$
- $T\left(\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = 0\boldsymbol{e}_1 + 0\boldsymbol{e}_2 + 1\boldsymbol{e}_3,$

where $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$ is the standard basis for $\mathbb{R}^3$.

4.4.7 Given a matrix representation of a linear transformation, we can recover its explicit form through matrix multiplication.

Theorem 4.4.a. Let $T : V \to W$ be a linear transformation. Let β and γ be ordered bases for V and W respectively. Then,

$$[T(\boldsymbol{v})]_{\gamma} = [T]_{\beta}^{\gamma}[\boldsymbol{v}]_{\beta}$$

for any $\boldsymbol{v} \in V$.

Proof. Let $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ and $\gamma = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$.

We first establish the result for the vectors in β. Firstly, note that $[T(\boldsymbol{v}_i)]_{\gamma}$ is the ith column of $[T]_{\beta}^{\gamma}$ and $[\boldsymbol{v}_i]_{\beta} = \boldsymbol{e}_i$ in $\mathbb{R}^m$[10]. Then, by definition of matrix multiplication, $[T]_{\beta}^{\gamma}\boldsymbol{e}_i$ is the ith column of $[T]_{\beta}^{\gamma}$. It follows that $[T(\boldsymbol{v}_i)]_{\gamma} = [T]_{\beta}^{\gamma}[\boldsymbol{v}_i]_{\beta}$.

Next, we will establish the result for general vector in V to complete the proof. For any $\boldsymbol{v} \in V$, we have $\boldsymbol{v} = a_1\boldsymbol{v}_1 + \cdots + a_m\boldsymbol{v}_m$ for some unique scalars $a_1, \ldots, a_m$. Then,

$$\begin{aligned} [T(\boldsymbol{v})]_{\gamma} &= [T(a_1\boldsymbol{v}_1 + \cdots + a_m\boldsymbol{v}_m)]_{\gamma} \\ &= [a_1T(\boldsymbol{v}_1) + \cdots + a_mT(\boldsymbol{v}_m)]_{\gamma} \\ &= a_1[T(\boldsymbol{v}_1)]_{\gamma} + \cdots + a_m[T(\boldsymbol{v}_m)]_{\gamma} \\ &= a_1[T]_{\beta}^{\gamma}\boldsymbol{e}_1 + \cdots + a_m[T]_{\beta}^{\gamma}\boldsymbol{e}_m \\ &= [T]_{\beta}^{\gamma}(a_1\boldsymbol{e}_1 + \cdots + a_m\boldsymbol{e}_m) \\ &= [T]_{\beta}^{\gamma}\begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix} \\ &= [T]_{\beta}^{\gamma}[\boldsymbol{v}]_{\beta}. \end{aligned}$$

□

[10]We can write $\boldsymbol{v}_i = 0\boldsymbol{v}_1 + \cdots + 0\boldsymbol{v}_{i-1} + 1\boldsymbol{v}_i + 0\boldsymbol{v}_{i+1} + \cdots + 0\boldsymbol{v}_m$.

4.4.8 Through matrix representations, we can establish some relationship between operations between linear transformations and the matrix operations. First we consider addition of linear transformations.

Let $T : V \to W$ and $T' : V \to W$ be two linear transformations. Then $T+T'$ is defined to be a function from V to W given by $(T+T')(\boldsymbol{v}) = T(\boldsymbol{v}) + T'(\boldsymbol{v})$. Note that $T+T'$ is also a linear transformation from V to W.

Proof. Addition: For any $\boldsymbol{u}, \boldsymbol{v} \in V$,

$$\begin{aligned}(T+T')(\boldsymbol{u}+\boldsymbol{v}) &= T(\boldsymbol{u}+\boldsymbol{v}) + T'(\boldsymbol{u}+\boldsymbol{v}) \\ &= T(\boldsymbol{u}) + T'(\boldsymbol{u}) + T(\boldsymbol{v}) + T'(\boldsymbol{v}) \\ &= (T+T')(\boldsymbol{u}) + (T+T')(\boldsymbol{v}).\end{aligned}$$

Scalar multiplication: For any $c \in \mathbb{R}$ and $\boldsymbol{v} \in V$,

$$(T+T')(c\boldsymbol{v}) = T(c\boldsymbol{v}) + T'(c\boldsymbol{v}) = c(T(\boldsymbol{v}) + T'(\boldsymbol{v})) = c(T+T')(\boldsymbol{v}).$$

□

4.4.9 As one may expect, addition of linear transformations corresponds to matrix addition.

Theorem 4.4.b. Let $T, T' : V \to W$ be two linear transformations. Let β and γ be ordered bases for V and W respectively. Then,

$$[T+T']^{\gamma}_{\beta} = [T]^{\gamma}_{\beta} + [T']^{\gamma}_{\beta}.$$

Proof. For any $\boldsymbol{v} \in V$,

$$\begin{aligned}[T+T']^{\gamma}_{\beta}[\boldsymbol{v}]_{\beta} &= [(T+T')(\boldsymbol{v})]_{\gamma} && \text{(Theorem 4.4.a)} \\ &= [T(\boldsymbol{v}) + T'(\boldsymbol{v})]_{\gamma} \\ &= [T(\boldsymbol{v})]_{\gamma} + [T'(\boldsymbol{v})]_{\gamma} \\ &= [T]^{\gamma}_{\beta}[\boldsymbol{v}]_{\beta} + [T']^{\gamma}_{\beta}[\boldsymbol{v}]_{\beta} && \text{(Theorem 4.4.a)} \\ &= ([T]^{\gamma}_{\beta} + [T']^{\gamma}_{\beta})[\boldsymbol{v}]_{\beta}.\end{aligned}$$

As this holds for arbitrary $\boldsymbol{v} \in V$, we conclude that

$$[T+T']^{\gamma}_{\beta} = [T]^{\gamma}_{\beta} + [T']^{\gamma}_{\beta}.$$

□

4.4.10 Next, we consider composition of linear transformations.

Let $T : V \to W$ and $T' : W \to X$ be two linear transformations. Then the composition of T and T' is the function $T' \circ T : V \to X$ given by

$$(T' \circ T)(\boldsymbol{v}) = T'(T(\boldsymbol{v}))$$

for any $\boldsymbol{v} \in V$. The composition $T' \circ T$ is a linear transformation from V to X.

Proof. Addition: For any $\boldsymbol{u}, \boldsymbol{v} \in V$,

$$(T' \circ T)(\boldsymbol{u}+\boldsymbol{v}) = T'(T(\boldsymbol{u}+\boldsymbol{v})) = T'(T(\boldsymbol{u}) + T(\boldsymbol{v})) = T'(T(\boldsymbol{u})) + T'(T(\boldsymbol{v})) = (T' \circ T)(\boldsymbol{u}) + (T' \circ T)(\boldsymbol{v}).$$

Scalar multiplication: For any $\boldsymbol{v} \in V$ and $c \in \mathbb{R}$,

$$(T' \circ T)(c\boldsymbol{v}) = T'(T(c\boldsymbol{v})) = T'(cT(\boldsymbol{v})) = cT'(T(\boldsymbol{v})) = c(T' \circ T)(\boldsymbol{v}).$$

□

4.4.11 It turns out that composition of linear transformations corresponds to matrix multiplication. This explains the seemingly strange definition of matrix multiplication.

Theorem 4.4.c. Let $T : V \to W$ and $T' : W \to X$ be two linear transformations. Let β, γ, and δ be ordered bases for V, W, and X respectively. Then,

$$[T' \circ T]_\beta^\delta = [T']_\gamma^\delta [T]_\beta^\gamma.$$

Proof. For any $\boldsymbol{v} \in V$,

$$\begin{aligned}
[T' \circ T]_\beta^\delta [\boldsymbol{v}]_\beta &= [(T' \circ T)(\boldsymbol{v})]_\delta && \text{(Theorem 4.4.a)} \\
&= [T'(T(\boldsymbol{v}))]_\delta \\
&= [T']_\gamma^\delta [T(\boldsymbol{v})]_\gamma && \text{(Theorem 4.4.a)} \\
&= [T']_\gamma^\delta [T]_\beta^\gamma [\boldsymbol{v}]_\beta && \text{(Theorem 4.4.a).}
\end{aligned}$$

As this holds for arbitrary $\boldsymbol{v} \in V$, we conclude that

$$[T' \circ T]_\beta^\delta = [T']_\gamma^\delta [T]_\beta^\gamma.$$

□

4.4.12 Apart from operations, there are also some correspondence in the properties between linear transformations and their matrix representations. The first one is invertibility.

4.4.13 Let $T : V \to W$ be a linear transformation. T is said to be **invertible** if the inverse of T exists, i.e., there exists a function $T^{-1} : W \to V$ such that $T^{-1} \circ T = \mathrm{id}_V$ and $T \circ T^{-1} = \mathrm{id}_W$. T^{-1} is called the **inverse** of T. From MATH2012, we know that T is invertible iff T is bijective. So an invertible linear transformation is just the same as an isomorphism.

Note that the inverse of T, namely T^{-1}, is still a linear transformation.

Proof. Fix any $\boldsymbol{w}_1, \boldsymbol{w}_2 \in W$. By the bijectivity of T, there exist unique $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ such that $T(\boldsymbol{v}_1) = \boldsymbol{w}_1$ and $T(\boldsymbol{v}_2) = \boldsymbol{w}_2$. Furthermore, we have $\boldsymbol{v}_1 = T^{-1}(\boldsymbol{w}_1)$ and $\boldsymbol{v}_2 = T^{-1}(\boldsymbol{w}_2)$.

Addition: Consider

$$\begin{aligned}
T^{-1}(\boldsymbol{w}_1 + \boldsymbol{w}_2) &= T^{-1}(T(\boldsymbol{v}_1) + T(\boldsymbol{v}_2)) \\
&= T^{-1}(T(\boldsymbol{v}_1)) + T^{-1}(T(\boldsymbol{v}_2)) \\
&= \boldsymbol{v}_1 + \boldsymbol{v}_2 \\
&= T^{-1}(\boldsymbol{w}_1) + T^{-1}(\boldsymbol{w}_2).
\end{aligned}$$

Scalar multiplication: For any $c \in \mathbb{R}$, consider

$$T^{-1}(c\boldsymbol{w}_1) = T^{-1}(cT(\boldsymbol{v}_1) = T^{-1}(T(c\boldsymbol{v}_1)) = c\boldsymbol{v}_1 = cT^{-1}(\boldsymbol{w}_1).$$

□

4.4.14 As one may expect, invertibility of a linear transformation corresponds to the invertibility of its matrix representation.

Theorem 4.4.d. Let $T : V \to W$ be a linear transformation. Let β and γ be ordered bases for V and W respectively. Then T is invertible iff $[T]_\beta^\gamma$ is invertible.

Proof. Let $m = \dim(V)$.

"$\Rightarrow$": Assume that T is invertible. Then $\dim(W) = \dim(V) = m$. So both β and γ contain m vectors. Thus, we have $[T^{-1}]_\gamma^\beta [T]_\beta^\gamma = [T^{-1} \circ T]_\beta^\beta = [\mathrm{id}_V]_\beta^\beta = I_m$, and similarly, $[T]_\beta^\gamma [T^{-1}]_\gamma^\beta = [\mathrm{id}_W]_\gamma^\gamma = I_m$. This shows that $[T]_\beta^\gamma$ is invertible (and its inverse is given by $[T^{-1}]_\gamma^\beta$).

"$\Leftarrow$" Assume that $[T]_\beta^\gamma$ is invertible. Let $A=[T]_\beta^\gamma$. Fix any $\boldsymbol{w}\in W$. Write

$$A^{-1}[\boldsymbol{w}]_\gamma=\begin{bmatrix}a_1\\ \vdots\\ a_m\end{bmatrix}.$$

Also write the ordered bases as $\beta=\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_m\}$ and $\gamma=\{\boldsymbol{w}_1,\dots,\boldsymbol{w}_m\}$. To construct the inverse of T, we define $U:W\to V$ by $U(\boldsymbol{w})=a_1\boldsymbol{v}_1+\cdots+a_m\boldsymbol{v}_m$. Note that by construction,

$$[U(\boldsymbol{w})]_\beta=\begin{bmatrix}a_1\\ \vdots\\ a_m\end{bmatrix}=A^{-1}[\boldsymbol{w}]_\gamma.$$

We claim that $U=T^{-1}$. To see this, note first that

$$[U]_\gamma^\beta=\begin{bmatrix}[U(\boldsymbol{w}_1)]_\beta & \cdots & [U(\boldsymbol{w}_m)]_\beta\end{bmatrix}=\begin{bmatrix}A^{-1}[\boldsymbol{w}_1]_\gamma & \cdots & A^{-1}[\boldsymbol{w}_m]_\gamma\end{bmatrix}=\begin{bmatrix}A^{-1}\boldsymbol{e}_1 & \cdots & A^{-1}\boldsymbol{e}_m\end{bmatrix}=A^{-1}$$

where $\boldsymbol{e}_1,\dots,\boldsymbol{e}_m$ are standard vectors in $\mathbb{R}^m$. By Theorem 4.4.c,

$$[U\circ T]_\beta^\beta=\big[U\big]_\gamma^\beta\big[T\big]_\beta^\gamma=A^{-1}A=I_m.$$

Then by Theorem 4.4.a, we have for any $\boldsymbol{v}\in V$,

$$[(U\circ T)(\boldsymbol{v})]_\beta=[U\circ T]_\beta^\beta[\boldsymbol{v}]_\beta=I_m[\boldsymbol{v}]_\beta=[\boldsymbol{v}]_\beta,$$

implying that $(U\circ T)(\boldsymbol{v})=\boldsymbol{v}$, i.e., $U\circ T=\mathrm{id}_V$. Similarly, we can show that $T\circ U=\mathrm{id}_W$. Hence, $U=T^{-1}$. □

4.4.15 As suggested in the proof of Theorem 4.4.d, if T is invertible, then the inverse of the matrix representation $[T]_\beta^\gamma$ is given by $[T^{-1}]_\gamma^\beta$, namely the matrix representation of T^{-1}. This provides us another way to compute matrix inverse.

4.4.16 Next, we consider rank and nullity. It turns that a linear transformation has the same rank and nullity as its matrix representation. [Note: The terms "rank" and "nullity" have different meanings when applied to linear transformations and matrices respectively.]

Theorem 4.4.e. Let T be a linear transformation from V to W. Let β and γ be ordered bases for V and W respectively. Then,

$$\mathrm{rank}(T)=\mathrm{rank}([T]_\beta^\gamma)\quad\text{and}\quad\mathrm{nullity}(T)=\mathrm{nullity}([T]_\beta^\gamma).$$

Proof. (Partial) Note that it suffices to prove that $\mathrm{rank}(T)=\mathrm{rank}([T]_\beta^\gamma)$, since it implies the latter by dimension formula (Theorem 4.2.c) and rank-nullity theorem ([4.2.10]).

Start with a basis $\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_r\}$ for $\mathrm{null}(T)$. By the extension approach, we can add some vectors to form a basis $\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_r,\boldsymbol{v}_{r+1},\dots,\boldsymbol{v}_n\}$ for V, denoted by β'.

By Proposition 4.2.b,

$$\begin{aligned}\mathrm{ran}(T)&=\mathrm{span}\left(\{T(\boldsymbol{v}_1),\dots,T(\boldsymbol{v}_r),T(\boldsymbol{v}_{r+1}),\dots,T(\boldsymbol{v}_n)\}\right)\\&=\mathrm{span}\left(\{\mathbf{0},\dots,\mathbf{0},T(\boldsymbol{v}_{r+1}),\dots,T(\boldsymbol{v}_n)\}\right)\\&=\mathrm{span}\left(\{T(\boldsymbol{v}_{r+1}),\dots,T(\boldsymbol{v}_n)\}\right).\end{aligned}$$

By dimension formula (Theorem 4.2.c), $\dim(\mathrm{ran}(T))=\mathrm{rank}(T)=\dim(V)-\mathrm{nullity}(T)=n-r$. Since $\{T(\boldsymbol{v}_{r+1}),\dots,T(\boldsymbol{v}_n)\}$ is a spanning set for $\mathrm{ran}(T)$ that contains $n-r$ vectors, it is a basis for $\mathrm{ran}(T)$ by Theorem 3.6.e.

Next, by the extension approach again, we can add some vectors to form a basis $\{T(\boldsymbol{v}_{r+1}),\dots,T(\boldsymbol{v}_n),\boldsymbol{w}_1,\dots,\boldsymbol{w}_s\}$ for W (with cardinality $n-r+s$), denoted by γ'.

Note that the matrix representation

$$\begin{aligned}[T]_{\beta'}^{\gamma'} &= \begin{bmatrix}[T(\boldsymbol{v}_1)]_{\gamma'} & \cdots & [T(\boldsymbol{v}_r)]_{\gamma'} & [T(\boldsymbol{v}_{r+1})]_{\gamma'} & \cdots & [T(\boldsymbol{v}_n)]_{\gamma'}\end{bmatrix} \\ &= \begin{bmatrix}[\mathbf{0}]_{\gamma'} & \cdots & [\mathbf{0}]_{\gamma'} & \boldsymbol{e}_1 & \cdots & \boldsymbol{e}_{n-r}\end{bmatrix} && (\boldsymbol{e}_1,\dots,\boldsymbol{e}_{n-r} \text{ are standard vectors in } \mathbb{R}^{n-r+s}) \\ &= \begin{bmatrix}\mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{e}_1 & \cdots & \boldsymbol{e}_{n-r}\end{bmatrix} \\ &= \begin{bmatrix}O_{(n-r)\times r} & I_{n-r} \\ O_{s\times r} & O_{s\times(n-r)}\end{bmatrix}.\end{aligned}$$

Note that the rank of the matrix $[T]_{\beta'}^{\gamma'}$ is $n-r$, since $\begin{bmatrix}O_{(n-r)\times r} & I_{n-r} \\ O_{s\times r} & O_{s\times(n-r)}\end{bmatrix}$ is in RREF and it has $n-r$ leading ones. This is the same as the rank of T, given by $\operatorname{rank}(T)=\dim(\operatorname{ran}(T))=n-r$ as well.

So far we have established the equality for a *specific* choice of bases for the matrix representation, namely β' and γ'. To prove the general case, we need to utilize the approach of *change of coordinates*, to be discussed in Section 4.5. So the proof is to be continued at [4.5.7]. $\square$

4.5 Change of Coordinates Matrix

4.5.1 Let β and β' be two ordered bases for a vector space V. Then the matrix $[\mathrm{id}_V]_{\beta}^{\beta'}$ is called a **change of coordinates matrix** from β to β'.

Example: With $\beta=\{\boldsymbol{e}_1,\boldsymbol{e}_2\}$ and $\beta'=\left\{\begin{bmatrix}1\\2\end{bmatrix},\begin{bmatrix}3\\4\end{bmatrix}\right\}$ being two ordered bases for $\mathbb{R}^2$, the change of coordinates matrix from β to β' is

$$[\mathrm{id}_{\mathbb{R}^2}]_{\beta}^{\beta'}=\begin{bmatrix}1 & 3\\ 2 & 4\end{bmatrix}.$$

4.5.2 The following result tells us how $[\mathrm{id}_V]_{\beta}^{\beta'}$ is related to "change of coordinates".

Theorem 4.5.a. Let β and β' be two ordered bases for a vector space V. Let $Q=[\mathrm{id}_V]_{\beta}^{\beta'}$. Then,

(a) Q is invertible.

(b) (change of coordinates) For any $\boldsymbol{v}\in V$, $[\boldsymbol{v}]_{\beta'}=Q[\boldsymbol{v}]_{\beta}$.

[Note: From the *change of coordinates* property, we see that multiplying the change of coordinates matrix Q does change the coordinate vector from $[\boldsymbol{v}]_{\beta}$ (with respect to β) to $[\boldsymbol{v}]_{\beta'}$ (with respect to β').]

Proof.

(a) Note that id_V is invertible, so by Theorem 4.4.d, the matrix representation $Q=[\mathrm{id}_V]_{\beta}^{\beta'}$ is invertible as well.

(b) For any $\boldsymbol{v}\in V$, we have $Q[\boldsymbol{v}]_{\beta}=[\mathrm{id}_V]_{\beta}^{\beta'}[\boldsymbol{v}]_{\beta}\overset{\text{thm. 4.4.a}}{=}[\mathrm{id}_V(\boldsymbol{v})]_{\beta'}=[\boldsymbol{v}]_{\beta'}$.

$\square$

4.5.3 Using change of coordinates matrix, we also change the matrix representation of a linear transformation.

Theorem 4.5.b. Let β and β' be two ordered bases for a vector space V. Let $T:V\to V$ be a linear transformation and let $Q=[\mathrm{id}_V]_{\beta}^{\beta'}$. Then,

$$[T]_{\beta}^{\beta}=Q^{-1}[T]_{\beta'}^{\beta'}Q.$$

[⚠ Warning: We do not have $[T]_{\beta'}^{\beta'} = Q^{-1}[T]_{\beta}^{\beta}Q$ with this definition of Q.]

Proof. Note first that $Q^{-1} = \left([\mathrm{id}_V]_{\beta}^{\beta'}\right)^{-1} = [\mathrm{id}_V]_{\beta'}^{\beta}$ by [4.4.15]. Then, consider:

$$\begin{aligned}
Q^{-1}[T]_{\beta'}^{\beta'}Q &= [\mathrm{id}_V]_{\beta'}^{\beta}[T]_{\beta'}^{\beta'}[\mathrm{id}_V]_{\beta}^{\beta'} \\
&= [\mathrm{id}_V]_{\beta'}^{\beta}[T \circ \mathrm{id}_V]_{\beta}^{\beta'} && \text{(Theorem 4.4.c)} \\
&= [\mathrm{id}_V]_{\beta'}^{\beta}[T]_{\beta}^{\beta'} \\
&= [\mathrm{id}_V \circ T]_{\beta}^{\beta} && \text{(Theorem 4.4.c)} \\
&= [T]_{\beta}^{\beta}.
\end{aligned}$$

□

4.5.4 Theorem 4.5.b is somehow related to the following definition about *similar* matrices. An $n \times n$ matrix A is said to be **similar** to an $n \times n$ matrix B if there exists an invertible matrix Q such that $B = Q^{-1}AQ$. In view of Theorems 4.5.a and 4.5.b, we know that the two matrix representations $[T]_{\beta'}^{\beta'}$ and $[T]_{\beta}^{\beta}$ are similar.

4.5.5 As one may expect, matrix similarity is an equivalence relation.

Proof. Write $A \sim B$ if A is similar to B.

Reflexive: For any $n \times n$ matrix A, we can write $A = I_n^{-1}AI_n$, so $A \sim A$.

Symmetric: For any $n \times n$ matrices A and B, we have

$$A \sim B \implies B = Q^{-1}AQ \implies A = QBQ^{-1} = (Q^{-1})^{-1}BQ^{-1} \implies B \sim A$$

where Q is an invertible matrix.

Transitive: For any $n \times n$ matrices A, B, and C, assume $A \sim B$ and $B \sim C$. Then, there exist invertible matrices P and Q such that $B = P^{-1}AP$ and $C = Q^{-1}BQ$. Then,

$$C = Q^{-1}(P^{-1}AP)Q = (PQ)^{-1}A(PQ),$$

so $A \sim C$. □

4.5.6 As suggested by the name, two similar matrices A and B indeed share a number of common properties:

(a) *same rank:* Note that

$$\begin{aligned}
\mathrm{rank}(B) &= \mathrm{rank}(Q^{-1}AQ) \\
&= \mathrm{rank}(AQ) && \text{(Theorem 3.7.c)} \\
&= \mathrm{rank}(Q^TA^T) \\
&= \mathrm{rank}(A^T) && \text{(Theorem 3.7.c)} \\
&= \mathrm{rank}(A) && \text{(Corollary 3.9.b)}.
\end{aligned}$$

(b) *same determinant:* Note that $\det B = \det\left(Q^{-1}AQ\right) = \det\left(Q^{-1}\right)\det A \det Q = (\det Q)^{-1}\det Q \det A = \det A$.

4.5.7 Using a similar idea as the proof of Theorem 4.5.b, we can complete the rest of the proof for Theorem 4.4.e:

Proof. (Continued) Given any ordered bases β and γ for V and W respectively, we have by Theorem 4.4.c,

$$[\mathrm{id}_W]_{\gamma}^{\gamma'}[T]_{\beta}^{\gamma}[\mathrm{id}_V]_{\beta'}^{\beta} = [T]_{\beta'}^{\gamma'}.$$

Since both $[\mathrm{id}_W]_{\gamma}^{\gamma'}$ and $[\mathrm{id}_V]_{\beta'}^{\beta}$ are invertible matrices (as identity transformation is invertible), $[T]_{\beta}^{\gamma}$ and $[T]_{\beta'}^{\gamma'}$ are similar. Thus, by [4.5.6]a, we have

$$\operatorname{rank}([T]_{\beta}^{\gamma}) = \operatorname{rank}([T]_{\beta'}^{\gamma'}).$$

So the general case follows from the proven specific case. $\square$

5 Diagonalization

5.0.1 Section 5 is related to the concept of matrix similarity. Given an $n \times n$ matrix A, we are trying to find a *diagonal* matrix D that is similar to A, just as suggested by the name "diagonalization". A reason for doing so is that diagonal matrices satisfy some nice properties and it is often convenient to work with them. With the matrix similarity, we can deduce some properties of A based on the properties of D.

5.1 Diagonalizability

5.1.1 An $n \times n$ matrix A is **diagonalizable** if there exists an invertible $n \times n$ matrix Q such that $Q^{-1}AQ$ is a diagonal matrix, i.e., A is similar to some diagonal matrix.

Given an $n \times n$ matrix A, the process of finding such matrix Q and the corresponding diagonal matrix is referred as the **diagonalization** of the matrix A.

5.1.2 Examples:

- $A = \begin{bmatrix} -4 & -2 \\ 28 & 11 \end{bmatrix}$ is diagonalizable since
$$Q^{-1}AQ = \begin{bmatrix} 3 & 0 \\ 0 & 4 \end{bmatrix}$$
where $Q = \begin{bmatrix} 2 & -1 \\ -7 & 4 \end{bmatrix}$ is invertible. [Note: This choice of Q and the diagonal matrix seems to be coming from nowhere, but as we will see, there is actually a systematic way to find such matrices.]
- Any diagonal matrix D is diagonalizable since $D = I_n^{-1} D I_n$.

5.1.3 Let A be an invertible $n \times n$ matrix. Then, A is diagonalizable iff A^{-1} is diagonalizable.

Proof. "$\Rightarrow$": Suppose A is diagonalizable. Then there exists an invertible $n \times n$ matrix Q such that $Q^{-1}AQ = D$ for some diagonal matrix D. Note that D must be invertible as $\det D = \det Q^{-1} \det A \det Q = (\det Q)^{-1} \det A (\det Q) = \det A \neq 0$. Hence, we have
$$Q^{-1}A^{-1}Q = (Q^{-1}AQ)^{-1} = D^{-1}$$
where D^{-1} is still a diagonal matrix [11]. Thus A^{-1} is diagonalizable.

"$\Leftarrow$": Interchange A and A^{-1} in the proof for "$\Rightarrow$". $\square$

5.1.4 Now we will introduce a systematic way to (i) determine if a matrix is diagonalizable and (ii) diagonalize a matrix (if possible). It utilizes the concepts of *eigenvalues* and *eigenvectors*.

5.1.5 Let A be an $n \times n$ matrix. A scalar $\lambda \in \mathbb{R}$ is an **eigenvalue** of A if there is a *nonzero* vector $\boldsymbol{v} \in \mathbb{R}^n$ such that $A\boldsymbol{v} = \lambda\boldsymbol{v}$. In such case, $\boldsymbol{v}$ is called a **λ-eigenvector** of A. A nonzero vector $\boldsymbol{v}$ is called an **eigenvector** of A if it is a λ-eigenvector of A for some $\lambda \in \mathbb{R}$.

Remarks:

- We consider only nonzero vector since we always have $A\mathbf{0} = \lambda\mathbf{0}$ for any $\lambda \in \mathbb{R}$, so it is not interesting to consider zero vector. On the other hand, the λ in the definition can be zero.
- Note that if $\boldsymbol{v}$ is a λ-eigenvector of A, the vector $c\boldsymbol{v}$ is a λ-eigenvector of A as well, for any $c \neq 0$. Thus, given an eigenvalue λ of A, there are indeed infinitely many λ-eigenvectors of A.

Geometrically, given an eigenvector $\boldsymbol{v}$ of A, the vectors $A\boldsymbol{v}$ and $\boldsymbol{v}$ are parallel. More specifically, $A\boldsymbol{v}$ is obtained by $\boldsymbol{v}$ through *scaling*.

[11] It can be obtained by taking the reciprocal of every diagonal entry of D. Note that every diagonal entry of D must be nonzero since $\det D \neq 0$.

5.1.6 In the special case where A is diagonal, we can easily obtain eigenvalues and eigenvectors.

Proposition 5.1.a. Let $D = \text{diag}(a_1, \ldots, a_n)$ (i.e., the diagonal matrix with diagonal entries $D_{11} = a_1, \ldots, D_{nn} = a_n$). Then, $a_1, \ldots, a_n$ are eigenvalues of A, and an a_i-eigenvector of A is $\boldsymbol{e}_i$ for any $i = 1, \ldots, n$.

Proof. Observe that $D\boldsymbol{e}_i = a_i\boldsymbol{e}_i$ for any $i = 1, \ldots, n$. □

5.1.7 Let A be an invertible $n \times n$ matrix. Then,

(a) any eigenvalue of A is nonzero.

(b) $\boldsymbol{v}$ is an eigenvector of A iff $\boldsymbol{v}$ is an eigenvector of A^{-1}.

(c) λ is an eigenvalue of A iff λ^{-1} is an eigenvalue of A^{-1}.

Proof.

(a) Assume to the contrary that $A\boldsymbol{v} = 0\boldsymbol{v} = \boldsymbol{0}$ for some nonzero $\boldsymbol{v}$. This means the homogeneous system $A\boldsymbol{x} = \boldsymbol{0}$ has a non-trivial solution, thus A is not invertible by Proposition 2.6.f.

(b) "$\Rightarrow$": Suppose $\boldsymbol{v}$ is an eigenvector of A. Then $A\boldsymbol{v} = \lambda\boldsymbol{v}$ for some $\lambda \neq 0$ (by (a)). Hence, $\boldsymbol{v} = A^{-1}\lambda\boldsymbol{v} = \lambda(A^{-1}\boldsymbol{v})$. Dividing both sides by λ gives $A^{-1}\boldsymbol{v} = \lambda^{-1}\boldsymbol{v}$.
"$\Leftarrow$": Interchange A and A^{-1} in the proof for "$\Rightarrow$".

(c) Similar to (b).

□

5.1.8 We will introduce a systematic approach for finding eigenvalues and eigenvectors of a general $n \times n$ matrix in Section 5.2. Before that, let us first investigate how eigenvalues and eigenvectors can help us diagonalize a matrix.

Theorem 5.1.b. Let $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ be a set of eigenvectors of an $n \times n$ matrix A. Let $Q = \begin{bmatrix}\boldsymbol{v}_1 & \cdots & \boldsymbol{v}_n\end{bmatrix}$ be an $n \times n$ matrix. If $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is a basis for $\mathbb{R}^n$, then $Q^{-1}AQ$ is a diagonal matrix with the diagonal entries being the eigenvalues of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ respectively.

Proof. We identify β as an ordered basis. Let λ_i be the corresponding eigenvalue of the eigenvector $\boldsymbol{v}_i$, for any $i = 1, \ldots, n$. Let β' be the standard ordered basis for $\mathbb{R}^n$.

Then, note that $Q = [\text{id}_{\mathbb{R}^n}]_{\beta}^{\beta'} = \begin{bmatrix}[\boldsymbol{v}_1]_{\beta'} & \cdots & [\boldsymbol{v}_n]_{\beta'}\end{bmatrix}$, the change of coordinates matrix from β to β'. By Theorem 4.5.a, $\boldsymbol{v}_i = Q\boldsymbol{e}_i$ and $\boldsymbol{e}_i = Q^{-1}\boldsymbol{v}_i$, for any $i = 1, \ldots, n$.

Hence, for any $i = 1, \ldots, n$,

$$(Q^{-1}AQ)\boldsymbol{e}_i = Q^{-1}A(Q\boldsymbol{e}_i) = Q^{-1}A\boldsymbol{v}_i = Q^{-1}\lambda_i\boldsymbol{v}_i = \lambda_i Q^{-1}\boldsymbol{v}_i = \lambda_i\boldsymbol{e}_i.$$

This implies that $Q^{-1}AQ$ is a diagonal matrix with diagonal entries being $\lambda_1, \ldots, \lambda_n$. □

5.1.9 Furthermore, eigenvalues and eigenvectors can help us determine the diagonalizability. The following gives a diagonalizability criterion based on eigenvectors.

Theorem 5.1.c. Let A be an $n \times n$ matrix. Then A is diagonalizable iff there exists a basis $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ for $\mathbb{R}^n$ such that $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ are eigenvectors of A.

Proof. "$\Leftarrow$": It follows from Theorem 5.1.b.

"$\Rightarrow$": Suppose A is diagonalizable. Then $D = Q^{-1}AQ$, or $A = QDQ^{-1}$, for some invertible matrix Q and diagonal matrix $D = \text{diag}(\lambda_1, \ldots, \lambda_n)$.

Then, construct eigenvectors by considering for each $i = 1, \ldots, n$,

$$A(Q\boldsymbol{e}_i) = QDQ^{-1}Q\boldsymbol{e}_i = Q(D\boldsymbol{e}_i) = Q(\lambda_i\boldsymbol{e}_i) = \lambda_i Q\boldsymbol{e}_i.$$

Since $Q\boldsymbol{e}_i \neq \boldsymbol{0}$ for any $i = 1, \ldots, n$, $Q\boldsymbol{e}_1, \ldots, Q\boldsymbol{e}_n$ are eigenvectors of A.

Since $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ is linearly independent in $\mathbb{R}^n$, $\{Q\boldsymbol{e}_1, \ldots, Q\boldsymbol{e}_n\}$ is linearly independent in $\mathbb{R}^n$ also, by Theorem 3.7.b. By Theorem 3.6.b, it is a basis for $\mathbb{R}^n$ as well. □

5.1.10 Example: Let $A = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$. It can be shown that $\begin{bmatrix} -3 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ are 1-eigenvector and 5-eigenvector of A respectively. Thus, by Theorem 5.1.b, letting $Q = \begin{bmatrix} -3 & 1 \\ 1 & 1 \end{bmatrix}$, we have

$$Q^{-1}AQ = \begin{bmatrix} 1 & 0 \\ 0 & 5 \end{bmatrix}.$$

(Verify this by carrying out the matrix multiplications directly.)

5.1.11 In the special case where the matrix A has only one eigenvalue, we can say even more.

Let A be an $n \times n$ matrix with only one eigenvalue λ. Then A is diagonalizable iff $A = \lambda I_n$.

Proof. "$\Leftarrow$": Since $\lambda I_n \boldsymbol{v} = \lambda \boldsymbol{v}$ for any nonzero $\boldsymbol{v} \in \mathbb{R}^n$, λI_n has only one eigenvalue λ. (So it makes sense for $A = \lambda I_n$.) Furthermore, λI_n, as a diagonal matrix itself, is diagonalizable.

"$\Rightarrow$": Suppose A is diagonalizable. Then $Q^{-1}AQ = D$ for some invertible matrix Q and diagonal matrix D. By Theorem 5.1.c, there exists a basis $\beta = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ of $\mathbb{R}^n$ whose elements are eigenvectors of A.

Since the eigenvalues of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ must all be λ by assumption, by Theorem 5.1.b, $D = Q^{-1}AQ$ is a diagonal matrix with all diagonal entries being λ. So, $Q^{-1}AQ = \lambda I_n$, which implies

$$A = Q\lambda I_n Q^{-1} = \lambda QQ^{-1} = \lambda I_n.$$

□

5.2 Finding Eigenvalues and Eigenvectors

5.2.1 Now we introduce a systematic approach to find eigenvalues and eigenvectors of a given matrix. A key concept that is involved is the *characteristic polynomial*.

5.2.2 Let A be an $n \times n$ matrix. The polynomial $\det(A - tI_n)$ in t is the **characteristic polynomial** of A.

Examples:

- The characteristic polynomial of $A = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$ is

$$\det(A - tI_2) = \det \begin{bmatrix} 2-t & 1 \\ 0 & 1-t \end{bmatrix} = (2-t)(1-t) = t^2 - 3t + 2.$$

- The characteristic polynomial of the diagonal matrix $A = \operatorname{diag}(a_1, \dots, a_n)$ is

$$\det(A - tI_n) = (a_1 - t) \cdots (a_n - t).$$

5.2.3 It turns out similar matrices share the same characteristic polynomial. Let A and B be two similar $n \times n$ matrices. Then the characteristic polynomials of A and B are the same.

Proof. By definition, we can write $B = Q^{-1}AQ$ for some invertible matrix Q. Then, note that

$$\begin{aligned}
\det(B - tI_n) &= \det\big(Q^{-1}AQ - Q^{-1}(tI_n)Q\big) \\
&= \det\big(Q^{-1}(A - tI_n)Q\big) \\
&= \det\big(Q^{-1}\big)\det(A - tI_n)\det Q \\
&= (\det Q)^{-1}\det(A - tI_n)\det Q \\
&= \det(A - tI_n).
\end{aligned}$$

□

5.2.4 The characteristic polynomial can be used to find eigenvalues of a matrix, as suggested by the following result.

Theorem 5.2.a. Let A be an $n\times n$ matrix. Then a scalar $\lambda \in \mathbb{R}$ is an eigenvalue of A iff $\det(A-\lambda I_n) = 0$.

Proof. "$\Rightarrow$": Suppose λ is an eigenvalue of A. Then there exists a nonzero $\boldsymbol{v} \in \mathbb{R}^n$ such that $A\boldsymbol{v} = \lambda\boldsymbol{v}$, or $(A-\lambda I_n)\boldsymbol{v} = \mathbf{0}$. Hence, there is a non-trivial solution for the homogeneous system $(A-\lambda I_n)\boldsymbol{x} = \mathbf{0}$, thus $A-\lambda I_n$ is not invertible by Proposition 2.6.f, so $\det(A-\lambda I_n) = 0$.

"$\Leftarrow$": Assume $\det(A-\lambda I_n) = 0$. Then, $A-\lambda I_n$ is not invertible, so by Proposition 2.6.f, there is a non-trivial solution for the homogeneous system $(A-\lambda I_n)\boldsymbol{x} = \mathbf{0}$. Calling that solution $\boldsymbol{v}$, we have

$$(A-\lambda I_n)\boldsymbol{v} = 0 \implies A\boldsymbol{v} = \lambda\boldsymbol{v},$$

thus λ is an eigenvalue of A. □

5.2.5 In view of Theorem 5.2.a, practically speaking, we can find all eigenvalues of a matrix by finding all the roots of its characteristic polynomial. Note however that the roots may not be real in general. *Fundamental theorem of algebra* tells us that some of the roots can be complex in general. For example, consider the matrix $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Its characteristic polynomial is $\det(A-tI_2) = t^2+1$, and the roots of this polynomial are i and $-i$, meaning that the eigenvalues of A are non-real complex numbers.

In such case, we can use matrices with *complex* entries to diagonalize A. However, in MATH2101 we shall focus on matrices with *real* entries only. So, by restricting our attention to these matrices, A is *not* diagonalizable. To distinguish between two kinds of diagonalizability, we say that A is not **diagonalizable over** $\mathbb{R}$ but **diagonalizable over** $\mathbb{C}$. Nonetheless, here we shall not focus too much on this kind of cases.

5.2.6 Due to Theorem 5.2.a, we can deduce some properties about the number of eigenvalues of a matrix based on its characteristic polynomial.

Proposition 5.2.b. An $n \times n$ matrix A has at most n distinct eigenvalues.

Proof. Write $A = [a_{ij}]$ and consider the characteristic polynomial of A: $\det(A-tI_n)$. Note that the diagonal entries of $A-tI_n$ are $a_{11}-t, \dots, a_{nn}-t$. By cofactor expansion, the determinant would (at least) include the term $(a_{11}-t)\cdots(a_{nn}-t)$, which in turn includes the term $(-1)^n t^n$. We also observe that there would not be any term involving t raised to a power higher than n from the cofactor expansion.

It follows that the characteristic polynomial is of degree n, hence has at most n distinct roots. This then means A has at most n distinct eigenvalues, by Theorem 5.2.a. □

5.3 Linear Independence of Eigenvectors

5.3.1 After discussing how to find eigenvalues and eigenvectors in Section 5.2, we will discuss the relationship between different eigenvectors. More specifically, we consider the linear independence of eigenvectors.

Theorem 5.3.a. Let A be an $n \times n$ matrix with m distinct eigenvalues $\lambda_1, \dots, \lambda_m$. Let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m$ be λ_1-,...,λ_m-eigenvectors of A respectively. Then, $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_m\}$ is linearly independent.

Proof. We shall prove this inductively. Firstly, consider the $m = 1$ case. Since $\boldsymbol{v}_1$ is λ_1-eigenvector of A, it must be nonzero. The linear independence of $\{\boldsymbol{v}_1\}$ is then immediate.

Now assume that the case $m = k$ holds, i.e., $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_k\}$ is linearly independent, for some $k \in \{1, \dots, n-1\}$. We want to prove that the case $m = k+1$ holds. Consider:

$$\begin{aligned} a_1\boldsymbol{v}_1 + \cdots + a_{k+1}\boldsymbol{v}_{k+1} &= \mathbf{0} \qquad (3) \\ \implies a_1A\boldsymbol{v}_1 + \cdots + a_{k+1}A\boldsymbol{v}_{k+1} &= \mathbf{0} \\ \implies a_1\lambda_1\boldsymbol{v}_1 + \cdots + a_{k+1}\lambda_{k+1}\boldsymbol{v}_{k+1} &= \mathbf{0}. \qquad (4) \end{aligned}$$

Multiplying Equation (3) by λ_{k+1} on both sides gives

$$a_1\lambda_{k+1}\boldsymbol{v}_1 + \cdots + a_k\lambda_k\boldsymbol{v}_k + a_{k+1}\lambda_{k+1}\boldsymbol{v}_{k+1}.$$

Subtracting this by Equation (4) gives

$$a_1(\lambda_{k+1}-\lambda_1)\boldsymbol{v}_1 + \cdots + a_k(\lambda_{k+1}-\lambda_k)\boldsymbol{v}_k.$$

By induction hypothesis (linear independence of $\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_k\}$), we have

$$a_1(\lambda_{k+1}-\lambda_1) = \cdots = a_k(\lambda_{k+1}-\lambda_k) = 0.$$

But since the eigenvalues $\lambda_1,\dots,\lambda_{k+1}$ are distinct (by the setting), we must have $a_1 = \cdots = a_k = 0$.

Putting this to Equation (3) gives $a_{k+1}\boldsymbol{v}_{k+1} = \mathbf{0}$. Since $\boldsymbol{v}_{k+1}$ is an eigenvector of A, it must be nonzero. Hence, we have $a_{k+1} = 0$ as well. This means that $\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_{k+1}\}$ is linearly independent. □

5.3.2 Based on Theorem 5.3.a, we can obtain a sufficient condition for diagonalizability.

Corollary 5.3.b. Let A be an $n\times n$ matrix. If A has n distinct eigenvalues, then A is diagonalizable.

Proof. Let $\lambda_1,\dots,\lambda_n$ be the n distinct eigenvalues of A, and $\boldsymbol{v}_1,\dots,\boldsymbol{v}_n$ be λ_1-,...,λ_n-eigenvectors of A respectively. Then by Theorem 5.3.a, $\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_n\}$ is linearly independent. Since $\dim(\mathbb{R}^n) = n$, $\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_n\}$ is indeed a basis for $\mathbb{R}^n$, by Theorem 3.6.b. It then follows by Theorem 5.1.c that A is diagonalizable. □

5.4 Algebraic and Geometric Multiplicities

5.4.1 In [5.1.11] and Corollary 5.3.b, we have introduced some criterion or sufficient condition for diagonalizability under some special cases. We would then like to obtain a more general and helpful criterion for diagonalizability, and it is related to the concepts of algebraic and geometric multiplicities.

5.4.2 We start with algebraic multiplicity. Let A be an $n\times n$ matrix and λ be an eigenvalue of A. The **algebraic multiplicity** (A.M.) of λ is the largest integer k such that $(t-\lambda)^k$ divides $\det(A-tI_n)$, i.e., we can write $\det(A-tI_n) = (t-\lambda)^kP(t)$ for some polynomial $P(t)$.

Example: Consider the matrix

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

The characteristic polynomial of A is

$$\det(A-tI_4) = \det\begin{bmatrix} 1-t & 2 & 3 & 4 \\ 0 & 2-t & 0 & 3 \\ 0 & 0 & 1-t & 0 \\ 0 & 0 & 0 & -1-t \end{bmatrix} = (1-t)^2(2-t)(-1-t).$$

(We can compute this by starting with cofactor expansion along the last row.) From this we know that the eigenvalues of A are 1, 2, and -1. Their A.M. are as follows:

Eigenvalue λ	A.M.
1	2
2	1
-1	1

5.4.3 Let A be an $n \times n$ matrix with eigenvalues $\lambda_1, \dots, \lambda_k$, where $a_1, \dots, a_k$ are the respective A.M. In general (assuming diagonalizability over $\mathbb{R}$), the characteristic polynomial can be written as

$$(-1)^n (t-\lambda_1)^{a_1} \cdots (t-\lambda_k)^{a_k}.$$

(To see this, consider cofactor expansion.)

5.4.4 Since the characteristic polynomial is of degree n, we must have $a_1 + \cdots + a_k = n$, i.e., the sum of A.M. of all the eigenvalues is always n.

5.4.5 Furthermore, for λ to be an eigenvalue of A, the A.M. of λ must be *at least one*, so that λ is a root of the characteristic polynomial.

On the other hand, since the sum of the A.M. of all eigenvalues of A is n, the maximum possible A.M. of an eigenvalue is n, which is achieved when A only has one eigenvalue.

5.4.6 Next, we consider geometric multiplicity. Let A be an $n \times n$ matrix and λ be an eigenvalue of A. The set containing all λ-eigenvectors of A and the zero vector, namely $E_\lambda = \{\boldsymbol{v} \in \mathbb{R}^n : A\boldsymbol{v} = \lambda \boldsymbol{v}\}$ or the null space $\text{null}(A - \lambda I_n)$, is said to be the **$\lambda$-eigenspace**.

By Theorem 3.10.a, every eigenspace is a vector subspace since it is a null space. So it makes sense to talk about the *dimension* of E_λ. This dimension $\dim(E_\lambda)$ is said to be the **geometric multiplicity** of λ.

5.4.7 For λ to be an eigenvalue of A, there must exist an nonzero vector $\boldsymbol{v}$ such that $A\boldsymbol{v} = \lambda\boldsymbol{v}$. Thus, the λ-eigenspace must contain some nonzero vector, which means that the G.M. of λ must be *at least one*.

5.4.8 Practically, finding G.M. of eigenvalues is a matter of solving systems of linear equations. This is because for each eigenvalue λ, we are essentially finding the dimension of null space, or the nullity of $A - \lambda I_n$, and Theorem 3.10.b tells us that this value is given by the number of free variables in the homogeneous system $(A - \lambda I_n)\boldsymbol{x} = \mathbf{0}$. In short, the G.M. of an eigenvalue λ is the number of free variables in the homogeneous system $(A - \lambda I_n)\boldsymbol{x} = \mathbf{0}$.

5.4.9 After introducing both A.M. and G.M., it is now time to investigate their relationship. One remarkable result is as follows.

Theorem 5.4.a (G.M. $\le$ A.M.)**.** Let A be an $n \times n$ matrix and λ be an eigenvalue of A. Then the geometric multiplicity of λ is less than or equal to the algebraic multiplicity of λ.

[Note: Coincidentally, we have another important result in mathematics that also states "G.M. $\le$ A.M.", but it is the inequality of arithmetic and geometric means, also known as the AM-GM inequality.]

Proof. Let $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_r\}$ be a basis for the λ-eigenspace E_λ, where r is the G.M. of λ.

We then find vectors $\boldsymbol{w}_1, \dots, \boldsymbol{w}_{n-r}$ such that $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_r, \boldsymbol{w}_1, \dots, \boldsymbol{w}_{n-r}\}$ is a basis for $\mathbb{R}^n$, denoted by β.

Let β_{st} be the standard basis for $\mathbb{R}^n$ and $Q = [\text{id}_{\mathbb{R}^n}]_\beta^{\beta_{\text{st}}} = \begin{bmatrix} \boldsymbol{v}_1 & \cdots & \boldsymbol{v}_r & \boldsymbol{w}_1 & \cdots & \boldsymbol{w}_{n-r} \end{bmatrix}$ be the change of coordinates matrix from β to β_{st}. By Theorem 4.5.b, we have $[L_A]_\beta = Q^{-1}[L_A]_{\beta_{\text{st}}} Q = Q^{-1}AQ$ where $L_A(\boldsymbol{v}) = A\boldsymbol{v}$ for any $\boldsymbol{v} \in \mathbb{R}^n$. Hence, A and $[L_A]_\beta = Q^{-1}AQ$ are similar, thus having the same characteristic polynomial.

So, to analyze the A.M. of λ, we may inspect the characteristic polynomial of $Q^{-1}AQ$. For any $i = 1, \dots, r$, the ith column of $Q^{-1}AQ$ is $Q^{-1}AQ\boldsymbol{e}_i = [L_A(\boldsymbol{v}_i)]_\beta = [A\boldsymbol{v}_i]_\beta = [\lambda \boldsymbol{v}_i]_\beta = \lambda \boldsymbol{e}_i$, so we can express $Q^{-1}AQ$ as the following block form:

$$Q^{-1}AQ = \begin{bmatrix} \lambda I_r & * \\ O_{(n-r)\times r} & A' \end{bmatrix}$$

for some $(n-r) \times (n-r)$-matrix A'.

Finally, we will compute the A.M. of λ. By cofactor expansion, the characteristic polynomial of $Q^{-1}AQ$ (also of A) is

$$\det(A - tI_n) = \det\big(Q^{-1}AQ - tI_n\big) = (\lambda - t)^r \det(A' - tI_{n-1}) = (-1)^r (t-\lambda)^r \det(A' - tI_{n-1}),$$

thus $(t-\lambda)^r$ divides $\det(A - tI_n)$. It follows that the A.M. of λ is at least r, which is the G.M. of λ. $\square$

5.4.10 Finally, we are going to introduce a general and useful criterion for diagonalizability, involving A.M. and G.M.

Theorem 5.4.b. Let A be an $n \times n$ matrix. Then A is diagonalizable iff the A.M. of λ equals the G.M. of λ for every eigenvalue λ of A.

Proof. "$\Rightarrow$": Assume A is diagonalizable. Then by Theorem 5.1.c, there is a basis β for $\mathbb{R}^n$ whose elements are eigenvectors of A. Let $\lambda_1, \dots, \lambda_k$ be the eigenvalues of A. Denote the A.M. and G.M. of an eigenvalue λ by $m_a(\lambda)$ and $m_g(\lambda)$ respectively. For each $i = 1, \dots, k$, let $\beta_i = \beta \cap E_{\lambda_i}$. Note that for each $i = 1, \dots, k$, $|\beta_i| \le \dim(E_{\lambda_i}) = m_g(\lambda_i)$, as β_i is a linearly independent subset of E_{λ_i}. Applying also Theorem 5.4.a, we get

$$n = \sum_{i=1}^{k} |\beta_i| \le \sum_{i=1}^{k} m_g(\lambda_i) \le \sum_{i=1}^{k} m_a(\lambda_i) = n,$$

where the first equality holds since there are n eigenvectors in β, and the last equality holds by [5.4.4]. This forces $\sum_{i=1}^{k} m_g(\lambda_i) = \sum_{i=1}^{k} m_a(\lambda_i)$, thus

$$\sum_{i=1}^{k} [m_a(\lambda_i) - m_g(\lambda_i)] = 0.$$

By Theorem 5.4.a again, we have $m_a(\lambda_i) - m_g(\lambda_i) \ge 0$ for each $i = 1, \dots, k$. Hence, we must have $m_a(\lambda_i) = m_g(\lambda_i)$ for each $i = 1, \dots, k$.

"$\Leftarrow$": Assume that the A.M. of λ equals the G.M. of λ for every eigenvalue λ of A. By [5.4.4] the sum of all the algebraic multiplicities is n. Hence, by assumption, the sum of all the geometric multiplicities is also n.

Next, for each eigenvalue λ of A, we find a basis β_λ for the λ-eigenspace E_λ. The union $\beta \triangleq \bigcup_\lambda \beta_\lambda \subseteq \mathbb{R}^n$ of all those bases has n vectors as the sum of all the G.M. is n. To show that the union β is a basis for $\mathbb{R}^n$, it then suffices to prove that it is linearly independent, by Theorem 3.6.b.

First write $\beta = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ and let $\lambda_1, \dots, \lambda_k$ be the eigenvalues of A. Consider

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

For the n terms on the LHS, for each $i = 1, \dots, k$, we collect all the terms belonging to the eigenspace E_{λ_i}, and add them up to get a vector $\boldsymbol{w}_i \in E_{\lambda_i}$. After that, we can rewrite the equation as

$$\boldsymbol{w}_1 + \cdots + \boldsymbol{w}_k = \mathbf{0}.$$

This forces $\boldsymbol{w}_i = \mathbf{0}$ for every $i = 1, \dots, k$ since if not, it would imply that those nonzero $\boldsymbol{w}_i$'s are linearly dependent, contradicting the linear independence of those nonzero $\boldsymbol{w}_i$'s, as suggested in Theorem 5.3.a.

It then follows that $a_1 = \cdots = a_n = 0$ since $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ are all nonzero (as they all originate from basis of eigenspace). This shows the linear independence, hence β is a basis for $\mathbb{R}^n$.

Now note that the vectors in β are all eigenvectors of A by construction. It then follows by Theorem 5.1.c that A is diagonalizable. $\square$

5.4.11 Practically, when we use Theorem 5.4.b to determine diagonalizability, it suffices to only compare the A.M. and G.M. for eigenvalues with A.M. greater than 1. This is because when the A.M. of an eigenvalue is 1, then the G.M. of that eigenvalue has to be 1 as well since it is less than or equal to the A.M., by Theorem 5.4.a, and is also at least 1.

5.4.12 Using both Theorem 5.4.a and Theorem 5.4.b, we can deduce another criterion for diagonalizability.

Corollary 5.4.c. Let A be an $n \times n$ matrix. Then, A is diagonalizable iff the sum of G.M. of all the eigenvalues is n.

Proof. "$\Rightarrow$": Assume that A is diagonalizable. Then by Theorem 5.4.b, the A.M. of λ equals the G.M. of λ for each eigenvalue λ of A. It then follows that the sum of the G.M. of all the eigenvalues is n, by [5.4.4].

"$\Leftarrow$": Assume that the sum of G.M. of all the eigenvalues is n. Let $\lambda_1, \dots, \lambda_k$ be the eigenvalues of A, and denote the A.M. and G.M. of an eigenvalue λ by $m_a(\lambda)$ and $m_g(\lambda)$ respectively. By Theorem 5.4.a, $m_g(\lambda_i) \le m_a(\lambda_i)$ for every $i = 1, \dots, n$. By [5.4.4] and assumption, we have $\sum_{i=1}^n m_g(\lambda_i) = \sum_{i=1}^n m_a(\lambda_i) = n$. This then forces $m_g(\lambda_i) = m_a(\lambda_i)$ for every $i = 1, \dots, n$, hence A is diagonalizable by Theorem 5.4.b. $\square$

5.5 Applications of Diagonalization

5.5.1 Although diagonalization appears to be a rather theoretical thing to do, it can be applied to some practical computations. Here we will discuss two applications: (i) taking high powers of a matrix, and (ii) computing matrix exponentials.

5.5.2 First, consider taking high powers of a matrix. Let A be an $n \times n$ matrix and suppose we would like to compute A^k where k is large. Although one can compute it by definition of matrix multiplication, it is not an efficient approach. When A is diagonalizable, we have a better approach.

5.5.3 Suppose that A is diagonalizable. Then we can write $A = QDQ^{-1}$ for some diagonal matrix D. The matrices D and Q can be found by some standard diagonalization approach as discussed previously. Here, one important observation is that

$$A^k = \underbrace{(QDQ^{-1})(QDQ^{-1})\cdots(QDQ^{-1})}_{k \text{ times}} = QD^kQ^{-1},$$

where D^k can be computed easily as it is just another diagonal matrix where each diagonal entry is raised to the power k. So, via this formula, we can compute A^k efficiently.

5.5.4 Another application is about matrix exponentials. Let A be an $n \times n$ matrix. The **exponential of A** is defined to be

$$e^A = I_n + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \cdots$$

If A is a 1×1 matrix, i.e., a scalar, then e^A reduces to the usual exponential function.

[Note: It can be shown that such infinite series always converges, but we shall omit the details here.]

5.5.5 Examples:

- Let $A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$. Then,

$$\begin{aligned} e^A &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} + \frac{1}{2!}\begin{bmatrix} 2^2 & 0 \\ 0 & 3^2 \end{bmatrix} + \frac{1}{3!}\begin{bmatrix} 2^3 & 0 \\ 0 & 3^3 \end{bmatrix} + \cdots \\ &= \begin{bmatrix} 1 + 2^1 + \frac{2^2}{2!} + \frac{2^3}{3!} + \cdots & 0 \\ 0 & 1 + 3^1 + \frac{3^2}{2!} + \frac{3^3}{3!} + \cdots \end{bmatrix} \\ &= \begin{bmatrix} e^2 & 0 \\ 0 & e^3 \end{bmatrix}. \end{aligned}$$

- More generally, let $A = \text{diag}(a_1, \ldots, a_n)$. Then, $e^A = \text{diag}(e^{a_1}, \ldots, e^{a_n})$.

5.5.6 When A is not a diagonal matrix, we do not have a straightforward formula to compute e^A as in [5.5.5]. If A is diagonalizable, then diagonalization is very helpful for computing e^A.

5.5.7 Suppose that A is diagonalizable. Then, we have $A = QDQ^{-1}$ for some diagonal matrix D. Hence, we have

$$\begin{aligned} e^A &= I_n + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \cdots \\ &= QI_nQ^{-1} + QDQ^{-1} + \frac{1}{2!}QD^2Q^{-1} + \frac{1}{3!}QD^3Q^{-1} + \cdots \\ &= Q\left(I_n + D + \frac{1}{2!}D^2 + \frac{1}{3!}D^3 + \cdots\right)Q^{-1} \\ &= Qe^DQ^{-1}. \end{aligned}$$

[Note: It turns out that the distributive law for matrices still works for (convergent) infinite series.]

6 Inner Product Spaces

6.1 Inner Product Spaces

6.1.1 Given two vectors $\boldsymbol{u} = \begin{bmatrix} u_1 & \cdots & u_n \end{bmatrix}^T$ and $\boldsymbol{v} = \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix}^T$ in $\mathbb{R}^n$, their *dot product* is the sum of the products of the corresponding pairs of entries:

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

6.1.2 Here, we would like to generalize this notion to a general vector space V (not necessarily $\mathbb{R}^n$). A difficulty is that vectors in V may not have "entries" like the ones in $\mathbb{R}^n$, so the above "sum of products" definition of dot product may not work anymore. We need an alternative approach.

6.1.3 Instead of explicitly defining how to compute the "generalized dot product" in a vector space, we shall use an axiomatic approach, i.e., specify some properties that need to be satisfied to qualify as a "generalized dot product" (we call it *inner product*). To achieve the "generalization", those properties should be satisfied by the usual dot product in $\mathbb{R}^n$.

6.1.4 Let V be a vector space. An **inner product on V** is a function $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ satisfying the following properties:

(1) (preserving addition in the first argument) For any $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$, $\langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w} \rangle = \langle \boldsymbol{u}, \boldsymbol{w} \rangle + \langle \boldsymbol{v}, \boldsymbol{w} \rangle$.

(2) (preserving scalar multiplication in the first argument) For any $\boldsymbol{u}, \boldsymbol{v} \in V$ and $c \in \mathbb{R}$, $\langle c\boldsymbol{u}, \boldsymbol{v} \rangle = c \langle \boldsymbol{u}, \boldsymbol{v} \rangle$.

(3) (symmetry) For any $\boldsymbol{u}, \boldsymbol{v} \in V$, $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \langle \boldsymbol{v}, \boldsymbol{u} \rangle$.

(4) (positive definiteness) For any $\boldsymbol{v} \in V$, $\langle \boldsymbol{v}, \boldsymbol{v} \rangle > 0$ if $\boldsymbol{v} \neq \boldsymbol{0}$.

A vector space V equipped with an inner product $\langle \cdot, \cdot \rangle$ on V is said to be an **inner product space**, denoted by $(V, \langle \cdot, \cdot \rangle)$. For convenience, often we just denote such inner product space by V (and we shall use the notation $\langle \cdot, \cdot \rangle$ to stand for the equipped inner product by default).

6.1.5 Based on these defining properties for inner product, we can readily deduce some more extra properties:

Proposition 6.1.a. Let V be an inner product space, and $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ be any vectors in V. Then,

(a) $\langle \boldsymbol{w}, \boldsymbol{u} + \boldsymbol{v} \rangle = \langle \boldsymbol{w}, \boldsymbol{u} \rangle + \langle \boldsymbol{w}, \boldsymbol{v} \rangle$.

(b) For any $c \in \mathbb{R}$, $\langle \boldsymbol{u}, c\boldsymbol{v} \rangle = c \langle \boldsymbol{u}, \boldsymbol{v} \rangle$.

(c) $\langle \boldsymbol{v}, \boldsymbol{0} \rangle = \langle \boldsymbol{0}, \boldsymbol{v} \rangle = 0$.

(d) $\langle \boldsymbol{v}, \boldsymbol{v} \rangle = 0$ iff $\boldsymbol{v} = \boldsymbol{0}$.

Proof.

(a) Note that

$$\langle \boldsymbol{w}, \boldsymbol{u} + \boldsymbol{v} \rangle \overset{(3)}{=} \langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w} \rangle \overset{(1)}{=} \langle \boldsymbol{u}, \boldsymbol{w} \rangle + \langle \boldsymbol{v}, \boldsymbol{w} \rangle \overset{(3)}{=} \langle \boldsymbol{w}, \boldsymbol{u} \rangle + \langle \boldsymbol{w}, \boldsymbol{v} \rangle .$$

(b) Note that

$$\langle \boldsymbol{u}, c\boldsymbol{v} \rangle \overset{(3)}{=} \langle c\boldsymbol{v}, \boldsymbol{u} \rangle \overset{(2)}{=} c \langle \boldsymbol{v}, \boldsymbol{u} \rangle \overset{(3)}{=} c \langle \boldsymbol{u}, \boldsymbol{v} \rangle .$$

(c) Since $0\boldsymbol{v} = \boldsymbol{0}$, we have

$$\langle \boldsymbol{0}, \boldsymbol{v} \rangle = \langle 0\boldsymbol{v}, \boldsymbol{v} \rangle \overset{(3)}{=} 0 \langle \boldsymbol{v}, \boldsymbol{v} \rangle = 0,$$

proving the second equality. The first equality follows from (3).

(d) "$\Rightarrow$": We prove by contrapositive. Suppose $\boldsymbol{v} \neq \boldsymbol{0}$. Then, by (4), we have $\langle \boldsymbol{v}, \boldsymbol{v} \rangle > 0$.
"$\Leftarrow$": Suppose $\boldsymbol{v} = \boldsymbol{0}$. Then by (c), $\langle \boldsymbol{v}, \boldsymbol{v} \rangle = 0$.

$\square$

6.1.6 Examples of inner product spaces:

- The vector space $\mathbb{R}^n$ with $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = u_1 v_1 + \cdots + u_n v_n$ for any $\boldsymbol{u} = \begin{bmatrix} u_1 & \cdots & u_n \end{bmatrix}^T$ and $\boldsymbol{v} = \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix}^T$ in $\mathbb{R}^n$ (the usual dot product). This inner product is said to be the **standard inner product** on $\mathbb{R}^n$.

  Proof. Fix any $\boldsymbol{u} = \begin{bmatrix} u_1 & \cdots & u_n \end{bmatrix}^T$, $\boldsymbol{v} = \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix}^T$, and $\boldsymbol{w} = \begin{bmatrix} w_1 & \cdots & w_n \end{bmatrix}^T$ in $\mathbb{R}^n$, and any $c \in \mathbb{R}$. Now check:

  (1):

$$\begin{aligned} \langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w} \rangle &= (u_1 + v_1) w_1 + \cdots + (u_n + v_n) w_n \\ &= (u_1 w_1 + \cdots + u_n w_n) + (v_1 w_1 + \cdots + v_n w_n) \\ &= \langle \boldsymbol{u}, \boldsymbol{w} \rangle + \langle \boldsymbol{v}, \boldsymbol{w} \rangle . \end{aligned}$$

  (2):

$$\begin{aligned} \langle c\boldsymbol{u}, \boldsymbol{v} \rangle &= (cu_1) v_1 + \cdots + (cu_n) v_n \\ &= c(u_1 v_1 + \cdots + u_n v_n) \\ &= c \langle \boldsymbol{u}, \boldsymbol{v} \rangle . \end{aligned}$$

  (3):

$$\begin{aligned} \langle \boldsymbol{u}, \boldsymbol{v} \rangle &= (cu_1) v_1 + \cdots + (cu_n) v_n \\ &= u_1 v_1 + \cdots + u_n v_n \\ &= v_1 u_1 + \cdots + v_n u_n \\ &= \langle \boldsymbol{v}, \boldsymbol{u} \rangle . \end{aligned}$$

  (4): When $\boldsymbol{v} \neq \boldsymbol{0}$,

$$\langle \boldsymbol{v}, \boldsymbol{v} \rangle = v_1^2 + \cdots + v_n^2 > 0$$

  (since at least one of the n terms is positive, and all the n terms are nonnegative). □

- Let $(V, \langle \cdot, \cdot \rangle)$ be an inner product space, and r be any *positive* number. Define $\langle \cdot, \cdot \rangle' : V \times V \to \mathbb{R}$ by $\langle \boldsymbol{u}, \boldsymbol{v} \rangle' = r \langle \boldsymbol{u}, \boldsymbol{v} \rangle$ for any $\boldsymbol{u}, \boldsymbol{v} \in V$. Then $\langle \cdot, \cdot \rangle'$ is also an inner product on V.

  Proof. Fix any $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$, and any $c \in \mathbb{R}$. Now check:

  (1):

$$\langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w} \rangle' = r \langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w} \rangle = r(\langle \boldsymbol{u}, \boldsymbol{w} \rangle + \langle \boldsymbol{v}, \boldsymbol{w} \rangle) = \langle \boldsymbol{u}, \boldsymbol{w} \rangle' + \langle \boldsymbol{v}, \boldsymbol{w} \rangle' .$$

  (2):

$$\langle c\boldsymbol{u}, \boldsymbol{v} \rangle' = r \langle c\boldsymbol{u}, \boldsymbol{v} \rangle = cr \langle \boldsymbol{u}, \boldsymbol{v} \rangle = c \langle \boldsymbol{u}, \boldsymbol{v} \rangle' .$$

  (3):

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle' = r \langle \boldsymbol{u}, \boldsymbol{v} \rangle = r \langle \boldsymbol{v}, \boldsymbol{u} \rangle = \langle \boldsymbol{v}, \boldsymbol{u} \rangle' .$$

  (4): When $\boldsymbol{v} \neq \boldsymbol{0}$,

$$\langle \boldsymbol{v}, \boldsymbol{v} \rangle' = r \underbrace{\langle \boldsymbol{v}, \boldsymbol{v} \rangle}_{>0} > 0.$$

  □

  [Note: The positivity of r is only needed for proving (4).]

- Let $T : V \to W$ be an *injective* linear transformation, and let $\langle \cdot, \cdot \rangle_W$ be an inner product on W. For any $\boldsymbol{x}, \boldsymbol{y} \in V$, define $\langle \boldsymbol{x}, \boldsymbol{y} \rangle_V = \langle T(\boldsymbol{x}), T(\boldsymbol{y}) \rangle_W$. Then, $\langle \cdot, \cdot \rangle_V$ is an inner product on V.

  Proof. Fix any $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in V$, and any $c \in \mathbb{R}$. Now check:

  (1):

$$\begin{aligned}
\langle \boldsymbol{x} + \boldsymbol{y}, \boldsymbol{z} \rangle_V &= \langle T(\boldsymbol{x} + \boldsymbol{y}), T(\boldsymbol{z}) \rangle_W \\
&= \langle T(\boldsymbol{x}) + T(\boldsymbol{y}), T(\boldsymbol{z}) \rangle_W \\
&= \langle T(\boldsymbol{x}), T(\boldsymbol{y}) \rangle_W + \langle T(\boldsymbol{x}), T(\boldsymbol{z}) \rangle_W \\
&= \langle \boldsymbol{x}, \boldsymbol{y} \rangle_V + \langle \boldsymbol{x}, \boldsymbol{z} \rangle_V .
\end{aligned}$$

  (2):

$$\begin{aligned}
\langle c\boldsymbol{x}, \boldsymbol{y} \rangle_V &= \langle T(c\boldsymbol{x}), T(\boldsymbol{y}) \rangle_W \\
&= \langle cT(\boldsymbol{x}), T(\boldsymbol{y}) \rangle_W \\
&= c \langle T(\boldsymbol{x}), T(\boldsymbol{y}) \rangle_W \\
&= c \langle \boldsymbol{x}, \boldsymbol{y} \rangle_V .
\end{aligned}$$

  (3):

$$\begin{aligned}
\langle \boldsymbol{x}, \boldsymbol{y} \rangle_V &= \langle T(\boldsymbol{x}), T(\boldsymbol{y}) \rangle_W \\
&= \langle T(\boldsymbol{y}), T(\boldsymbol{x}) \rangle_W \\
&= \langle \boldsymbol{y}, \boldsymbol{x} \rangle_V .
\end{aligned}$$

  (4): When $\boldsymbol{v} \neq \boldsymbol{0}$, since T is injective, we must have $T(\boldsymbol{v}) \neq \boldsymbol{0} = T(\boldsymbol{0})$. Hence,

$$\langle \boldsymbol{v}, \boldsymbol{v} \rangle_V = \langle T(\boldsymbol{v}), T(\boldsymbol{v}) \rangle_W > 0.$$

  □

  [Note: The injectivity of T is only needed for proving (4).]

6.1.7 Standard inner products naturally induce the appearance of matrix transposes. Let A be an $m \times n$ matrix, and $\boldsymbol{u} \in \mathbb{R}^n, \boldsymbol{v} \in \mathbb{R}^m$ be any column vectors. Then, $\langle A\boldsymbol{u}, \boldsymbol{v} \rangle = \langle \boldsymbol{u}, A^T\boldsymbol{v} \rangle$, where $\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbb{R}^m$.

Proof. For the standard inner product $\langle \cdot, \cdot \rangle$, we have $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \boldsymbol{u}^T\boldsymbol{v}$ for any $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^m$. Hence,

$$\langle A\boldsymbol{u}, \boldsymbol{v} \rangle = (A\boldsymbol{u})^T\boldsymbol{v} = \boldsymbol{u}^T A^T \boldsymbol{v} = \boldsymbol{u}^T(A^T\boldsymbol{v}) = \langle \boldsymbol{u}, A^T\boldsymbol{v} \rangle .$$

□

6.1.8 After exploring the theoretical properties of inner products, we turn our attention to their geometric interpretation. In fact, apart from being a "generalized dot product", inner product also serves as a generalization to the geometric concept of *length*.

6.1.9 Let $(V, \langle \cdot, \cdot \rangle)$ be an inner product space. For any $\boldsymbol{v} \in V$, the **length** or **norm** of $\boldsymbol{v}$ is $\|\boldsymbol{v}\| = \sqrt{\langle \boldsymbol{v}, \boldsymbol{v} \rangle}$.

6.1.10 Example: Consider $\mathbb{R}^n$ equipped with the standard inner product. Then, the norm of any vector $\boldsymbol{v} = \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix}^T \in \mathbb{R}^n$ is $\|\boldsymbol{v}\| = \sqrt{v_1^2 + \cdots + v_n^2}$ (familiar?).

6.1.11 Next, we consider some properties of norm. The first one suggests that norm-preserving linear transformation must be injective.

Proposition 6.1.b. Let V be an inner product space and $T : V \to V$ be a linear transformation. Suppose that $\|T(\boldsymbol{v})\| = \|\boldsymbol{v}\|$ for any $\boldsymbol{v} \in V$ (i.e., T *preserves the norm*). Then, T is injective.

Proof. By Proposition 4.3.a, it suffices to prove that $\text{null}(T) \subseteq \{\mathbf{0}\}$. Suppose $T(\boldsymbol{v}) = \mathbf{0}$. Then, $\|\boldsymbol{v}\| = \|T(\boldsymbol{v})\| = \|\mathbf{0}\| = 0$, which implies that $\langle \boldsymbol{v}, \boldsymbol{v} \rangle = 0$, thus $\boldsymbol{v} = \mathbf{0}$ by Proposition 6.1.a. ☐

6.1.12 The result below gives us more properties about norm.

Proposition 6.1.c. Let V be an inner product space. Fix any $\boldsymbol{u}, \boldsymbol{v} \in V$ and $c \in \mathbb{R}$. Then,

(a) (norm after scaling) $\|c\boldsymbol{v}\| = |c|\|\boldsymbol{v}\|$.

(b) (only zero vector has zero norm) $\|\boldsymbol{v}\| = 0$ iff $\boldsymbol{v} = \mathbf{0}$.

(c) (Cauchy-Schwartz inequality) $\langle \boldsymbol{u}, \boldsymbol{v} \rangle \leq \|\boldsymbol{u}\|\|\boldsymbol{v}\|$.

(d) (triangle inequality) $\|\boldsymbol{u} + \boldsymbol{v}\| \leq \|\boldsymbol{u}\| + \|\boldsymbol{v}\|$.

Proof.

(a) Note that

$$\|c\boldsymbol{v}\| = \sqrt{\langle c\boldsymbol{v}, c\boldsymbol{v} \rangle} = \sqrt{c^2 \langle \boldsymbol{v}, \boldsymbol{v} \rangle} = |c|\sqrt{\langle \boldsymbol{v}, \boldsymbol{v} \rangle} = |c|\|\boldsymbol{v}\|.$$

(b) Note that

$$\|\boldsymbol{v}\| = 0 \iff \langle \boldsymbol{v}, \boldsymbol{v} \rangle = 0 \overset{\text{Proposition 6.1.a}}{\iff} \boldsymbol{v} = \mathbf{0}.$$

(c) For any $c \in \mathbb{R}$, we have

$$\begin{aligned} 0 &\leq \langle \boldsymbol{u} - c\boldsymbol{v}, \boldsymbol{u} - c\boldsymbol{v} \rangle \\ &= \langle \boldsymbol{u}, \boldsymbol{u} - c\boldsymbol{v} \rangle - c \langle \boldsymbol{v}, \boldsymbol{u} - c\boldsymbol{v} \rangle \\ &= \langle \boldsymbol{u}, \boldsymbol{u} \rangle - c \langle \boldsymbol{u}, \boldsymbol{v} \rangle - c \langle \boldsymbol{v}, \boldsymbol{u} \rangle + c^2 \langle \boldsymbol{v}, \boldsymbol{v} \rangle \\ &= \langle \boldsymbol{u}, \boldsymbol{u} \rangle - 2c \langle \boldsymbol{u}, \boldsymbol{v} \rangle + c^2 \langle \boldsymbol{v}, \boldsymbol{v} \rangle . \end{aligned}$$

Then, we take $c = \langle \boldsymbol{u}, \boldsymbol{v} \rangle / \|\boldsymbol{v}\|^2$ (tricky!), so that the inequality can be simplified to

$$\begin{aligned} 0 &\leq \|\boldsymbol{u}\|^2 - 2\frac{\langle \boldsymbol{u}, \boldsymbol{v} \rangle}{\|\boldsymbol{v}\|^2} \langle \boldsymbol{u}, \boldsymbol{v} \rangle + \left(\frac{\langle \boldsymbol{u}, \boldsymbol{v} \rangle}{\|\boldsymbol{v}\|^2} \right)^2 \|\boldsymbol{v}\|^2 \\ &= \|\boldsymbol{u}\|^2 - \frac{\langle \boldsymbol{u}, \boldsymbol{v} \rangle}{\|\boldsymbol{v}\|^2}, \end{aligned}$$

which implies that $\langle \boldsymbol{u}, \boldsymbol{v} \rangle^2 \leq \|\boldsymbol{u}\|^2\|\boldsymbol{v}\|^2$, hence $\langle \boldsymbol{u}, \boldsymbol{v} \rangle \leq \|\boldsymbol{u}\|\|\boldsymbol{v}\|$.

(d) We have

$$\begin{aligned} \|\boldsymbol{u} + \boldsymbol{v}\|^2 &= \langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{u} + \boldsymbol{v} \rangle \\ &= \langle \boldsymbol{u}, \boldsymbol{u} \rangle + \langle \boldsymbol{u}, \boldsymbol{v} \rangle + \langle \boldsymbol{v}, \boldsymbol{u} \rangle + \langle \boldsymbol{v}, \boldsymbol{v} \rangle \\ &= \langle \boldsymbol{u}, \boldsymbol{u} \rangle + 2 \langle \boldsymbol{u}, \boldsymbol{v} \rangle + \langle \boldsymbol{v}, \boldsymbol{v} \rangle \\ &\leq \|\boldsymbol{u}\|^2 + 2\|\boldsymbol{u}\|\|\boldsymbol{v}\| + \|\boldsymbol{v}\|^2 && \text{(c)} \\ &= (\|\boldsymbol{u}\| + \|\boldsymbol{v}\|)^2. \end{aligned}$$

☐

6.2 Orthonormal Bases

6.2.1 Consider the inner product space $\mathbb{R}^n$ equipped with the standard inner product, and consider the standard basis $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ for $\mathbb{R}^n$.

As we have seen previously, it is nice to work with this basis. In fact, this basis possesses some special properties that makes it an *orthonormal basis*. In Section 6.2, we shall investigate properties enjoyed by orthonormal bases, and also discuss how to construct orthonormal bases, in a general inner product space.

6.2.2 Let V be an inner product space. For any $\boldsymbol{u}, \boldsymbol{v} \in V$, the vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ are said to be **orthogonal** if $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 0$. [Note: In the case where $V = \mathbb{R}^2$ or $\mathbb{R}^3$ equipped with the standard inner product, the geometrical meaning of being orthogonal is just being perpendicular (excluding the zero vector in our consideration). So orthogonality may be seen as a generalization to perpendicularity.]

Also, we say that a subset S of V is **orthogonal** if $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$ for any *distinct* $\boldsymbol{x}, \boldsymbol{y} \in S$, i.e., any two *distinct* vectors in S are orthogonal.

Remarks:

- We exclude the case where $\boldsymbol{x} = \boldsymbol{y}$ since in such case we have $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$ iff $\boldsymbol{x} = \boldsymbol{0}$, by Proposition 6.1.a. So if we did not include "distinct" in the definition, the only orthogonal subset of V would be $\{\boldsymbol{0}\}$!
- By definition, any singleton subset S of V is orthogonal since there are not two distinct vectors in S, so the condition is trivially true.

6.2.3 Next, we will define orthonormality. Firstly, a vector $\boldsymbol{v} \in V$ is an **unit vector** if $\|\boldsymbol{v}\| = 1$. Then, a subset S of V is called **orthonormal** if (i) it is orthogonal and (ii) every vector in S is an unit vector.

Examples and non-examples: (We consider the inner product space $\mathbb{R}^2$ equipped with standard inner product in the following.)

- The standard basis $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ is an orthonormal basis.
- The standard basis $\{2\boldsymbol{e}_1, 2\boldsymbol{e}_2\}$ is orthogonal, but *not* orthonormal.
- The basis $\left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$ is orthogonal, but *not* orthonormal.
- The basis $\left\{ \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}, \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix} \right\}$ is an orthonormal basis.

6.2.4 Given an orthogonal subset S of V containing nonzero vectors, one can always obtain an orthonormal subset from it by scaling the vectors inside S such that they become unit vectors, i.e., **normalizing** the vectors. More specifically, the subset $S' = \left\{ \dfrac{\boldsymbol{v}}{\|\boldsymbol{v}\|} : \boldsymbol{v} \in S \right\}$ is orthonormal.

Proof. Fix any distinct $\boldsymbol{u}', \boldsymbol{v}' \in S'$. Then we have $\boldsymbol{u}' = \boldsymbol{u}/\|\boldsymbol{u}\|$ and $\boldsymbol{v}' = \boldsymbol{v}/\|\boldsymbol{v}\|$ where $\boldsymbol{u}, \boldsymbol{v} \in S$ are distinct. Hence, due to the orthogonality of S, we have

$$\langle \boldsymbol{u}', \boldsymbol{v}' \rangle = \frac{1}{\|\boldsymbol{u}\|\|\boldsymbol{v}\|} \langle \boldsymbol{u}, \boldsymbol{v} \rangle = \frac{0}{\|\boldsymbol{u}\|\|\boldsymbol{v}\|} = 0.$$

This proves S' is orthogonal.

Next, consider any $\boldsymbol{v}' \in S$. By Proposition 6.1.c, its norm is

$$\|\boldsymbol{v}'\| = \left| \frac{1}{\|\boldsymbol{v}\|} \right| \|\boldsymbol{v}\| = \frac{1}{\|\boldsymbol{v}\|} \|\boldsymbol{v}\| = 1,$$

hence S' is orthonormal. $\square$

6.2.5 Now we discuss some properties of orthogonal sets. The first one is about linear independence.

Theorem 6.2.a. Let V be an inner product space, and S be an orthogonal set of nonzero vectors in V. Then S is linearly independent.

[Intuition 💡: Some intuition can be gained by considering the case where $V = \mathbb{R}^2$ or $\mathbb{R}^3$. In such case, orthogonality is about perpendicularity and linear independence is like being "not parallel". So, intuitively, being perpendicular should imply being not parallel (but not converse).]

Proof. Fix any $n \in \mathbb{N}$ and any distinct $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in S$. Suppose

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

where $a_1, \dots, a_n$ are scalars.

Now, fix any $i = 1, \dots, n$ and consider

$$\langle a_1 \boldsymbol{v}_1 + \cdots + a_n \boldsymbol{v}_n, \boldsymbol{v}_i \rangle = a_i \langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle .$$

(All other terms vanish due to orthogonality of S.)

On the other hand, we have

$$\langle a_1 \boldsymbol{v}_1 + \cdots + a_n \boldsymbol{v}_n, \boldsymbol{v}_i \rangle = \langle \mathbf{0}, \boldsymbol{v}_i \rangle = \mathbf{0}$$

by Proposition 6.1.a.

This means that $a_i \langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle = \mathbf{0}$. But as $\boldsymbol{v}_i$ is nonzero (since S only contains nonzero vectors), we must have $\langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle > 0$. It follows that $a_i = 0$.

Applying this argument for every $i = 1, \dots, n$, we have $a_1 = \cdots = a_n = 0$. □

The converse of Theorem 6.2.a is not true. For example, consider the inner product space $\mathbb{R}^2$ equipped with standard inner product, and take $\boldsymbol{u} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $\boldsymbol{v} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Then $S = \{\boldsymbol{u}, \boldsymbol{v}\}$ is linearly independent but S is not orthogonal, since $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 1 \neq 0$.

6.2.6 Let V be a vector space and $S = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ be a subset of V. Given a vector $\boldsymbol{v} \in \operatorname{span}(S)$, expressing $\boldsymbol{v}$ as a linear combination of the vectors in S generally requires us to solve a system of linear equation or use some other approach, which can be cumbersome.

However, when we equip V with an inner product, and if S is orthogonal, then we would have a more convenient approach.

Theorem 6.2.b. Let V be an inner product space, and $S = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ be an orthogonal subset of V containing nonzero vectors. Then, for any $\boldsymbol{u} \in \operatorname{span}(S)$, we have

$$\boldsymbol{u} = \frac{\langle \boldsymbol{u}, \boldsymbol{v}_1 \rangle}{\|\boldsymbol{v}_1\|^2} \boldsymbol{v}_1 + \cdots + \frac{\langle \boldsymbol{u}, \boldsymbol{v}_n \rangle}{\|\boldsymbol{v}_n\|^2} \boldsymbol{v}_n.$$

[Note: Given $\boldsymbol{u} \in \operatorname{span}(S)$, $\dfrac{\langle \boldsymbol{u}, \boldsymbol{v}_i \rangle}{\|\boldsymbol{v}_i\|^2}$ can be found directly by straightforward computation, for any $i = 1, \dots, n$. So we can express $\boldsymbol{u}$ as a linear combination of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ conveniently using this result.]

Proof. Fix any $\boldsymbol{u} \in \operatorname{span}(S)$, and we can write

$$\boldsymbol{u} = a_1 \boldsymbol{v}_1 + \cdots + a_n \boldsymbol{v}_n$$

for some $a_1, \dots, a_n \in \mathbb{R}$.

Now, fix any $i = 1, \dots, n$, and consider

$$\langle \boldsymbol{u}, \boldsymbol{v}_i \rangle = \langle a_1 \boldsymbol{v}_1 + \cdots + a_n \boldsymbol{v}_n, \boldsymbol{v}_i \rangle = a_i \langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle .$$

(All other terms vanish due to orthogonality of S.) It follows that

$$a_i = \frac{\langle \boldsymbol{u}, \boldsymbol{v}_i \rangle}{\langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle} = \frac{\langle \boldsymbol{u}, \boldsymbol{v}_i \rangle}{\|\boldsymbol{v}_i\|^2}.$$

The result then follows by applying this argument for every $i = 1, \dots, n$. □

6.2.7 After discussing some properties of orthogonal sets, we will introduce a way to systematically construct orthonormal bases, known as *Gram-Schmidt process*. Let us start with the following result, which gives us a systematic way to construct *orthogonal* bases.

Theorem 6.2.c. Let V be an inner product space and $S = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ be a basis for V. Let $\boldsymbol{v}_1 = \boldsymbol{u}_1$, and for any $j = 2, \ldots, n$, let

$$\boldsymbol{v}_i = \boldsymbol{u}_i - \sum_{j=1}^{i-1} \frac{\langle \boldsymbol{u}_i, \boldsymbol{v}_j \rangle}{\|\boldsymbol{v}_j\|^2} \boldsymbol{v}_j.$$

More explicitly, we let:

$$\begin{aligned}
\boldsymbol{v}_1 &= \boldsymbol{u}_1, \\
\boldsymbol{v}_2 &= \boldsymbol{u}_2 - \frac{\langle \boldsymbol{u}_2, \boldsymbol{v}_1 \rangle}{\|\boldsymbol{v}_1\|^2} \boldsymbol{v}_1, \\
\boldsymbol{v}_3 &= \boldsymbol{u}_3 - \frac{\langle \boldsymbol{u}_3, \boldsymbol{v}_1 \rangle}{\|\boldsymbol{v}_1\|^2} \boldsymbol{v}_1 - \frac{\langle \boldsymbol{u}_3, \boldsymbol{v}_2 \rangle}{\|\boldsymbol{v}_2\|^2} \boldsymbol{v}_2, \\
&\vdots \\
\boldsymbol{v}_n &= \boldsymbol{u}_n - \frac{\langle \boldsymbol{u}_n, \boldsymbol{v}_1 \rangle}{\|\boldsymbol{v}_1\|^2} \boldsymbol{v}_1 - \frac{\langle \boldsymbol{u}_n, \boldsymbol{v}_2 \rangle}{\|\boldsymbol{v}_2\|^2} \boldsymbol{v}_2 - \cdots - \frac{\langle \boldsymbol{u}_n, \boldsymbol{v}_{n-1} \rangle}{\|\boldsymbol{v}_{n-1}\|^2} \boldsymbol{v}_{n-1}.
\end{aligned}$$

Then, $S' = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is an orthogonal basis for V.

Proof. It suffices to show that S' is an orthogonal spanning set of V, since orthogonality implies linear independence by Theorem 6.2.a, and S' contains nonzero vectors as for any $i = 1, \ldots, n$, $\boldsymbol{u}_i \neq \sum_{j=1}^{i-1} \frac{\langle \boldsymbol{u}_i, \boldsymbol{v}_j \rangle}{\|\boldsymbol{v}_j\|^2} \boldsymbol{v}_j$ (since the latter is a linear combination of $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}$, and if the equality held, it would contradict the linear independence of S).

Spanning set: For each $i = 1, \ldots, n$, we can write

$$\boldsymbol{u}_i = \boldsymbol{v}_i + \sum_{j=1}^{i-1} \frac{\langle \boldsymbol{u}_i, \boldsymbol{v}_j \rangle}{\|\boldsymbol{v}_j\|^2} \boldsymbol{v}_j, \tag{5}$$

which shows that $\boldsymbol{u}_i$ is a linear combination of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$, thus $\boldsymbol{u}_i \in \operatorname{span}(S')$. Since this holds for any $i = 1, \ldots, n$, it follows that $V = \operatorname{span}(\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}) \subseteq \operatorname{span}(S')$. On the other hand, we readily have $\operatorname{span}(S') \subseteq V$ since $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in V$.

Orthogonal: We use an induction argument. First, note that

$$\langle \boldsymbol{v}_2, \boldsymbol{v}_1 \rangle = \left\langle \boldsymbol{u}_2 - \frac{\langle \boldsymbol{u}_2, \boldsymbol{v}_1 \rangle}{\|\boldsymbol{v}_1\|^2} \boldsymbol{v}_1, \boldsymbol{v}_1 \right\rangle = \langle \boldsymbol{u}_2, \boldsymbol{v}_1 \rangle - \frac{\langle \boldsymbol{u}_2, \boldsymbol{v}_1 \rangle}{\|\boldsymbol{v}_1\|^2} \langle \boldsymbol{v}_1, \boldsymbol{v}_1 \rangle = 0.$$

This shows $\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ is orthogonal.

Now suppose for induction that $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ is orthogonal for a $k \in \{2, \ldots, n-1\}$. Then, fix any $\ell \in \{1, \ldots, k\}$, and consider

$$\begin{aligned}
\langle \boldsymbol{v}_{k+1}, \boldsymbol{v}_\ell \rangle &= \left\langle \boldsymbol{u}_{k+1} - \sum_{j=1}^{k} \frac{\langle \boldsymbol{u}_{k+1}, \boldsymbol{v}_j \rangle}{\|\boldsymbol{v}_j\|^2} \boldsymbol{v}_j, \boldsymbol{v}_\ell \right\rangle \\
&= \langle \boldsymbol{u}_{k+1}, \boldsymbol{v}_\ell \rangle - \left\langle \sum_{j=1}^{k} \frac{\langle \boldsymbol{u}_{k+1}, \boldsymbol{v}_j \rangle}{\|\boldsymbol{v}_j\|^2} \boldsymbol{v}_j, \boldsymbol{v}_\ell \right\rangle \\
&= 0 - \frac{\langle \boldsymbol{u}_{k+1}, \boldsymbol{v}_\ell \rangle}{\|\boldsymbol{v}_\ell\|^2} \langle \boldsymbol{v}_\ell, \boldsymbol{v}_\ell \rangle && \text{(by induction hypothesis)} \\
&= -\langle \boldsymbol{u}_{k+1}, \boldsymbol{v}_\ell \rangle \\
&= 0 && (\boldsymbol{v}_\ell \text{ is a linear combination of } \boldsymbol{u}_1, \ldots, \boldsymbol{u}_\ell).
\end{aligned}$$

It follows that $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k+1}\}$ is orthogonal. Hence $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is orthogonal. ∎

6.2.8 After obtaining an orthogonal basis for V, we can normalize the vectors inside to obtain an orthonormal basis for V:

Corollary 6.2.d. Let V be an inner product space. Then there exists an orthonormal basis for V.

Proof. Firstly, there always exists a basis S for V (e.g., constructed by the extension approach). Then, by Theorem 6.2.c, we can obtain an orthogonal basis S' for V. Then we normalize the vectors in S' to get $\left\{\frac{\boldsymbol{v}}{\|\boldsymbol{v}\|} : \boldsymbol{v} \in S\right\}$, which is an orthonormal basis for V.

[Note: Such orthonormal basis is called a **Gram-Schmidt orthonormal basis**, and the process of obtaining this orthonormal basis as suggested above is said to be the **Gram-Schmidt process**.] ☐

6.2.9 Example: Let $S = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ where $\boldsymbol{u}_1 = \begin{bmatrix}1 & 0 & -1\end{bmatrix}^T$ and $\boldsymbol{u}_2 = \begin{bmatrix}2 & 1 & -1\end{bmatrix}^T$, and consider the inner product space $V = \operatorname{span}(S)$ equipped with the standard inner product. Note that S is linearly independent, so S is a basis for V. However, it is not orthogonal as $\left\langle \begin{bmatrix}1 & 0 & -1\end{bmatrix}^T, \begin{bmatrix}2 & 1 & -1\end{bmatrix}^T \right\rangle = 3 \neq 0$.

To obtain an orthonormal basis for V, we can carry out the Gram-Schmidt process:

- $\boldsymbol{v}_1 = \boldsymbol{u}_1 = \begin{bmatrix}1\\0\\-1\end{bmatrix}$.
- $\boldsymbol{v}_2 = \boldsymbol{u}_2 - \frac{\langle \boldsymbol{u_2}, \boldsymbol{v}_1\rangle}{\|\boldsymbol{v}_1\|^2}\boldsymbol{v}_1 = \begin{bmatrix}2\\1\\-1\end{bmatrix} - \frac{3}{2}\begin{bmatrix}1\\0\\-1\end{bmatrix} = \begin{bmatrix}1/2\\1\\1/2\end{bmatrix}$.

Hence an orthonormal basis for V is $\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$. We then normalize the vectors to get an orthonormal basis for V:

$$\left\{\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\-1\end{bmatrix}, \frac{1}{\sqrt{6}/2}\begin{bmatrix}1/2\\1\\1/2\end{bmatrix}\right\}.$$

6.3 Orthogonal Complements

6.3.1 Next, we will discuss the concept of orthogonal complements, which is closely related to the idea of *orthogonal projections*.

6.3.2 Let S be a nonempty subset of an inner product space V. Then, the **orthogonal complement** of S is

$$S^\perp = \{\boldsymbol{v} \in V : \langle \boldsymbol{v}, \boldsymbol{s}\rangle = 0 \text{ for any } \boldsymbol{s} \in S\},$$

i.e., the subset of V containing vectors orthogonal to *all* vectors in S.

Examples:

- $\{\mathbf{0}\}^\perp = V$ by Proposition 6.1.a.
- $V^\perp = \{\mathbf{0}\}$ since $\langle \boldsymbol{v}, \boldsymbol{v}\rangle \neq 0$ for any $\boldsymbol{v} \neq \mathbf{0}$, and $\langle \mathbf{0}, \boldsymbol{v}\rangle = 0$ for any $\boldsymbol{v} \in V$ by Proposition 6.1.a.
- Let $V = \mathbb{R}^3$ equipped with standard inner product, and let $S = \{\boldsymbol{e}_2\} \subseteq \mathbb{R}^3$. Then $S^\perp = \left\{\begin{bmatrix}x & 0 & z\end{bmatrix}^T : x, z \in \mathbb{R}\right\}$.

  Proof. "$\supseteq$": Observe that $\left\langle \begin{bmatrix}x & 0 & z\end{bmatrix}^T, \boldsymbol{e}_2 \right\rangle = x(0) + 0(1) + z(0) = 0$ for any $x, z \in \mathbb{R}$.

  "$\subseteq$": For any $\boldsymbol{v} = \begin{bmatrix}v_1 & v_2 & v_3\end{bmatrix}^T \in S^\perp$, we have $\langle \boldsymbol{v}, \boldsymbol{e}_2\rangle = 0$, which implies that $v_2 = 0$, thus $\boldsymbol{v} \in \left\{\begin{bmatrix}x & 0 & z\end{bmatrix}^T : x, z \in \mathbb{R}\right\}$. ☐

6.3.3 The following provides some properties about orthogonal complements.

Proposition 6.3.a. Let V be an inner product space and S be a nonempty subset of V. Then,

(a) $S^{\perp} = \operatorname{span}(S)^{\perp}$.

(b) $S^{\perp}$ is a vector subspace of V.

(c) $S \cap S^{\perp} = \{\mathbf{0}\}$, under the further assumption that S is a vector subspace of V.

(d) $\dim(V) = \dim(S) + \dim(S^{\perp})$ and $(S^{\perp})^{\perp} = S$.

Proof.

(a) Recall that
$$\operatorname{span}(S) = \left\{\sum_{i=1}^{k} a_i \boldsymbol{s}_i : a_1, \dots, a_k \in \mathbb{R}, \boldsymbol{s}_1, \dots, \boldsymbol{s}_k \in S, k \in \mathbb{N}\right\}.$$
"$\subseteq$": For any $\boldsymbol{v} \in S^{\perp}$, we have $\langle \boldsymbol{v}, \boldsymbol{s}\rangle = 0$ for any $\boldsymbol{s} \in S$. Then, for any $k \in \mathbb{N}$, $\boldsymbol{s}_1, \dots, \boldsymbol{s}_k \in S$, and $a_1, \dots, a_k \in \mathbb{R}$, we have
$$\left\langle \boldsymbol{v}, \sum_{i=1}^{k} a_i \boldsymbol{s}_i \right\rangle = \sum_{i=1}^{k} a_i \langle \boldsymbol{v}, \boldsymbol{s}_i\rangle = 0,$$
thus $\boldsymbol{v} \in \operatorname{span}(S)^{\perp}$.
"$\supseteq$": For any $\boldsymbol{v} \in \operatorname{span}(S)^{\perp}$, we have $\langle \boldsymbol{v}, \boldsymbol{u}\rangle = 0$ for any $\boldsymbol{u} \in \operatorname{span}(S)$. Note that $S \subseteq \operatorname{span}(S)$, so particularly we have $\langle \boldsymbol{v}, \boldsymbol{s}\rangle = 0$ for any $\boldsymbol{s} \in \operatorname{span}(S)$, thus $\boldsymbol{v} \in S^{\perp}$.

(b) Fix any $\boldsymbol{u}, \boldsymbol{v} \in S^{\perp}$ and $c \in \mathbb{R}$.
<u>Addition</u>: For any $\boldsymbol{s} \in S$,
$$\langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{s}\rangle = \langle \boldsymbol{u}, \boldsymbol{s}\rangle + \langle \boldsymbol{v}, \boldsymbol{s}\rangle = 0 + 0 = 0,$$
thus $\boldsymbol{u} + \boldsymbol{v} \in S^{\perp}$.
<u>Scalar multiplication</u>: For any $\boldsymbol{s} \in S$,
$$\langle c\boldsymbol{v}, \boldsymbol{s}\rangle = c\langle \boldsymbol{v}, \boldsymbol{s}\rangle = c(0) = 0,$$
thus $c\boldsymbol{v} \in S^{\perp}$.

(c) "$\subseteq$": For any $\boldsymbol{v} \in S \cap S^{\perp}$, we have
$$\left\langle \underbrace{\boldsymbol{v}}_{\in S^{\perp}}, \underbrace{\boldsymbol{v}}_{\in S} \right\rangle = 0,$$
which implies that $\boldsymbol{v} = \mathbf{0}$.
"$\supseteq$": Note that $\mathbf{0} \in S^{\perp}$ always since we must have $\langle \mathbf{0}, \boldsymbol{s}\rangle = 0$ for any $\boldsymbol{s} \in S$, by Proposition 6.1.a. Furthermore, we have $\mathbf{0} \in S$ since S is a vector subspace, by Proposition 3.1.b.

(d) If $S = \{\mathbf{0}\}$ or $S = V$, then the result follows by the examples in [6.3.2]. So, henceforth we assume that S is strictly between $\{\mathbf{0}\}$ and V (i.e., a strict superset of $\{\mathbf{0}\}$ and a strict subset of V). Let $n = \dim(V)$ and $m = \dim(S)$. Then, we have $0 < m < n$ by Lemma 4.3.d and the fact that the only vector space with zero dimension is $\{\mathbf{0}\}$.
Now, by Corollary 6.2.d, there exists an orthonormal basis $\beta = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_m\}$ for S. Note that β is linearly independent in V. Performing extension approach followed by the Gram-Schmidt process, we can extend β to an orthonormal basis $\beta' = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_m, \boldsymbol{v}_{m+1}, \dots, \boldsymbol{v}_n\}$ for V.
Fix any $\boldsymbol{v} \in S^{\perp} \subseteq V$. Since β' is a basis for V, we can write
$$\boldsymbol{v} = a_1\boldsymbol{v}_1 + \cdots + a_m\boldsymbol{v}_m + a_{m+1}\boldsymbol{v}_{m+1} + \cdots + a_n\boldsymbol{v}_n$$
for some unique $a_1, \dots, a_n \in \mathbb{R}$, by Theorem 3.4.a. For every $i = 1, \dots, m$, note that $\boldsymbol{v}_i \in S$ and $\boldsymbol{v}_i \neq \mathbf{0}$. Also, since $\boldsymbol{v} \in S^{\perp}$, we have $\langle \boldsymbol{v}, \boldsymbol{v}_i\rangle = 0$. Thus, we can write
$$0 = \langle \boldsymbol{v}, \boldsymbol{v}_i\rangle = a_i \underbrace{\langle \boldsymbol{v}_i, \boldsymbol{v}_i\rangle}_{>0},$$

which implies $a_i = 0$. (All other terms vanish due to the orthogonality of β'.) This means that, for any $\boldsymbol{v} \in S^{\perp}$, we can actually write

$$\boldsymbol{v} = a_{m+1}\boldsymbol{v}_{m+1} + \cdots + a_n\boldsymbol{v}_n$$

for some unique $a_{m+1}, \ldots, a_n \in \mathbb{R}$. Hence, by Theorem 3.4.a again, $\beta^* = \{\boldsymbol{v}_{m+1}, \ldots, \boldsymbol{v}_n\}$ is an orthonormal basis for $S^{\perp}$. This shows $\dim(V) = \dim(S) + \dim(S^{\perp})$ in particular.

Knowing that $\boldsymbol{v}_{m+1}, \ldots, \boldsymbol{v}_n \in S^{\perp}$, we can use a similar argument as above to deduce that for any $\boldsymbol{u} \in (S^{\perp})^{\perp}$, we can write

$$\boldsymbol{u} = b_1\boldsymbol{v}_1 + \cdots + b_m\boldsymbol{v}_m$$

for some unique $b_1, \ldots, b_m \in \mathbb{R}$. This means $\beta = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ is an orthonormal basis for $(S^{\perp})^{\perp}$. Particularly, it implies that

$$(S^{\perp})^{\perp} = \operatorname{span}(\beta) = S.$$

□

6.3.4 Using the concept of orthogonal complement, we have the following important result about orthogonal projection.

Theorem 6.3.b (Orthogonal decomposition theorem)**.** Let V be an inner product space and W be a vector subspace of V. Then for any $\boldsymbol{v} \in V$, there exist *unique* $\boldsymbol{x} \in W$ and $\boldsymbol{y} \in W^{\perp}$ such that $\boldsymbol{v} = \boldsymbol{x} + \boldsymbol{y}$.

The vector $\boldsymbol{x}$ is called the **orthogonal projection of $\boldsymbol{v}$ onto W**, and can be obtained by the formula

$$\boldsymbol{x} = \frac{\langle \boldsymbol{v}, \boldsymbol{v}_1 \rangle}{\|\boldsymbol{v}_1\|^2}\boldsymbol{v}_1 + \cdots + \frac{\langle \boldsymbol{v}, \boldsymbol{v}_k \rangle}{\|\boldsymbol{v}_k\|^2}\boldsymbol{v}_k.$$

where $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ is an orthogonal basis for W.

[Note: The formula for $\boldsymbol{x}$ is "inspired" by Theorem 6.2.b.]

Proof. <u>Existence</u>: Let $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ be an orthogonal basis for W. First let

$$\boldsymbol{x} = \frac{\langle \boldsymbol{v}, \boldsymbol{v}_1 \rangle}{\|\boldsymbol{v}_1\|^2}\boldsymbol{v}_1 + \cdots + \frac{\langle \boldsymbol{v}, \boldsymbol{v}_k \rangle}{\|\boldsymbol{v}_k\|^2}\boldsymbol{v}_k.$$

which belongs to W since $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in W$.

Then, we let $\boldsymbol{y} = \boldsymbol{v} - \boldsymbol{x}$. For any $i = 1, \ldots, k$, we have □

$$\begin{aligned}
\langle \boldsymbol{y}, \boldsymbol{v}_i \rangle &= \langle \boldsymbol{v} - \boldsymbol{x}, \boldsymbol{v}_i \rangle \\
&= \langle \boldsymbol{v}, \boldsymbol{v}_i \rangle - \langle \boldsymbol{x}, \boldsymbol{v}_i \rangle \\
&= \langle \boldsymbol{v}, \boldsymbol{v}_i \rangle - \left\langle \frac{\langle \boldsymbol{v}, \boldsymbol{v}_1 \rangle}{\|\boldsymbol{v}_1\|^2}\boldsymbol{v}_1 + \cdots + \frac{\langle \boldsymbol{v}, \boldsymbol{v}_k \rangle}{\|\boldsymbol{v}_k\|^2}\boldsymbol{v}_k, \boldsymbol{v}_i \right\rangle \\
&= \langle \boldsymbol{v}, \boldsymbol{v}_i \rangle - \frac{\langle \boldsymbol{v}, \boldsymbol{v}_i \rangle}{\|\boldsymbol{v}_i\|^2} \langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle && \text{(all other terms vanish due to orthogonality)} \\
&= 0.
\end{aligned}$$

<u>Uniqueness</u>: Suppose we have $\boldsymbol{v} = \boldsymbol{x} + \boldsymbol{y} = \boldsymbol{x}' + \boldsymbol{y}'$ where $\boldsymbol{x}, \boldsymbol{x}' \in W$ and $\boldsymbol{y}, \boldsymbol{y}' \in W^{\perp}$. Then,

$$\boldsymbol{x} - \boldsymbol{x}' = \boldsymbol{y}' - \boldsymbol{y}.$$

Since $\boldsymbol{x} - \boldsymbol{x}' \in W$ and $\boldsymbol{y}' - \boldsymbol{y} \in W^{\perp}$, we have $\boldsymbol{x} - \boldsymbol{x}' = \boldsymbol{y}' - \boldsymbol{y} \in W \cap W^{\perp} = \{\boldsymbol{0}\}$, by Proposition 6.3.a.

Thus, we have $\boldsymbol{x} - \boldsymbol{x}' = \boldsymbol{y}' - \boldsymbol{y} = \boldsymbol{0}$, so $\boldsymbol{x} = \boldsymbol{x}'$ and $\boldsymbol{y} = \boldsymbol{y}'$.

6.3.5 Examples: (Here the inner product spaces are equipped with standard inner product.)

- Let $W = \operatorname{span}(\{\boldsymbol{e}_1, \boldsymbol{e}_3\}) \subseteq \mathbb{R}^3$. Then, it can be checked that $W^\perp = \operatorname{span}(\boldsymbol{e}_2)$. For $\boldsymbol{v} = \begin{bmatrix} 2 & 3 & 4 \end{bmatrix}^T$, we can write

$$\boldsymbol{v} = \underbrace{\begin{bmatrix} 2 \\ 0 \\ 4 \end{bmatrix}}_{\in W} + \underbrace{\begin{bmatrix} 0 \\ 3 \\ 0 \end{bmatrix}}_{\in W^\perp},$$

where $\begin{bmatrix} 2 & 0 & 4 \end{bmatrix}^T$ is the orthogonal projection of $\boldsymbol{v}$ onto W.
This expression can be obtained by "inspection", or alternatively, by using the formula

$$\boldsymbol{x} = \langle \boldsymbol{v}, \boldsymbol{e}_1 \rangle \boldsymbol{e}_1 + \langle \boldsymbol{v}, \boldsymbol{e}_3 \rangle \boldsymbol{e}_3 = \begin{bmatrix} 2 \\ 0 \\ 4 \end{bmatrix} \quad \text{and} \quad \boldsymbol{y} = \boldsymbol{v} - \boldsymbol{x} = \begin{bmatrix} 0 \\ 3 \\ 0 \end{bmatrix}$$

since $\{\boldsymbol{e}_1, \boldsymbol{e}_3\}$ is an orthonormal basis for W.

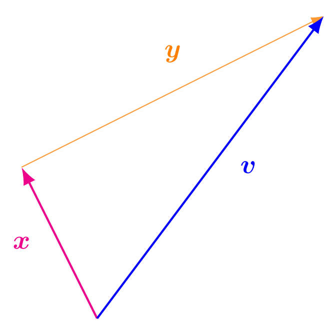
- Let $W = \operatorname{span}\left(\left\{\begin{bmatrix} 1 & -2 \end{bmatrix}^T\right\}\right)$. Then, it can be checked that $W^\perp = \operatorname{span}\left(\left\{\begin{bmatrix} 2 & 1 \end{bmatrix}^T\right\}\right)$. For $\boldsymbol{v} = \begin{bmatrix} 3 & 4 \end{bmatrix}^T$, since $\{\boldsymbol{v}_1\}$ is an orthogonal basis for W, we can use the formula

$$\boldsymbol{x} = \frac{\langle \boldsymbol{v}, \boldsymbol{v}_1 \rangle}{\|\boldsymbol{v}_1\|^2} \boldsymbol{v}_1 = \frac{3-8}{5} \begin{bmatrix} 1 \\ -2 \end{bmatrix} = \begin{bmatrix} -1 \\ 2 \end{bmatrix} \quad \text{and} \quad \boldsymbol{y} = \boldsymbol{v} - \boldsymbol{x} = \begin{bmatrix} 4 \\ 2 \end{bmatrix}$$

to get the decomposition

$$\boldsymbol{v} = \underbrace{\begin{bmatrix} -1 \\ 2 \end{bmatrix}}_{\in W} + \underbrace{\begin{bmatrix} 4 \\ 2 \end{bmatrix}}_{\in W^\perp}$$

where $\begin{bmatrix} -1 & 2 \end{bmatrix}^T$ is the orthogonal projection of $\boldsymbol{v}$ onto W.



References

Friedberg, S., Insel, A., & Spence, L. (2019). *Linear algebra* (5th ed.). Pearson Education.

Spence, L., Insel, A., & Friedberg, S. (2014). *Elementary linear algebra: A matrix approach* (2nd ed.). Pearson Education.

Concepts and Terminologies

Results

Section 1

- [1.2.2]: commutativity and associativity of matrix addition
- [1.2.6]: distributivity of addition and scalar multiplication of matrices
- [1.2.7]: "associativity" of scalar multiplication of matrices
- [1.2.10]: properties of matrix transpose
- [1.4.5]: multiplying identity matrix and a vector gives the vector again
- [1.4.6]: distributivity and "associativity" of matrix-vector product
- [1.6.2]: associativity of matrix multiplication
- [1.6.3]: distributivity of matrix multiplication
- [1.6.4]: non-commutativity of matrix multiplication
- [1.6.5]: anti-commutativity for transpose of AB
- Theorem 1.7.a: cofactor expansion theorem
- [1.7.9]: determinant of a block triangular matrix
- Proposition 1.8.a: alternating property of determinant
- Corollary 1.8.b: zero determinant for a matrix with two identical rows

- Proposition 1.8.c: multilinearity of determinant
- Proposition 1.8.d: taking transpose does not affect determinant
- Proposition 1.8.e: column version of alternating and multilinear properties of determinant
- Proposition 1.8.f: determinant of a scalar multiple of a matrix
- Proposition 1.8.g: multiplicativity of determinant
- [1.8.9]: "rule" for simplifying computations of determinant
- Proposition 1.9.a: uniqueness of matrix inverse
- Proposition 1.9.b: formula for determinant of matrix inverse
- Theorem 1.9.c: relationship between adjugate matrix and determinant
- Corollary 1.9.d: formula for matrix inverse
- Theorem 1.9.e: a matrix is invertible iff its determinant is nonzero
- Proposition 1.9.f: properties of matrix inverse

Section 2

- [2.1.4]: method of solving a system of linear equations by matrix inverse
- Proposition 2.1.a: uniqueness of solution of a system when the coefficient matrix is invertible
- Theorem 2.1.b: Cramer's rule
- Theorem 2.3.a: relationship between elementary matrix and ERO
- Proposition 2.3.b: invertibility of elementary matrices
- Theorem 2.4.a: criteria for invertibility of a matrix in RREF
- [2.5.3]: row equivalence is an equivalence relation
- Theorem 2.5.a: two systems with row equivalent augmented matrices have the same solution set
- Corollary 2.5.b: column correspondence property
- Theorem 2.5.c: uniqueness of RREF of a matrix
- Proposition 2.5.d: a matrix is invertible iff its RREF is invertible
- [2.5.11]: algorithm for solving a system of linear equations (assuming consistency)
- Theorem 2.6.a: a system $A\boldsymbol{x} = \boldsymbol{b}$ is inconsistent iff $[A|\boldsymbol{b}]$ has a leading one in the last column
- Corollary 2.6.b: a system $A\boldsymbol{x} = \boldsymbol{b}$ has a unique solution iff the RREF of $[A|\boldsymbol{b}]$ has a leading one in each column except the last one
- Proposition 2.6.c: homogeneous system with more variables than equations has infinitely many solution
- Proposition 2.6.d: expression of solution set for a consistent system with more variables than equations
- Proposition 2.6.e: whenever a system has more than one solution, it has infinitely many solutions
- Proposition 2.6.f: criteria for matrix invertibility relating to homogeneous system with same number of variables and equations

- Proposition 2.6.g: invertibility of square coefficient matrix when a system has a unique solution
- Proposition 2.6.h: square matrix A is invertible iff the system $\boldsymbol{Ax} = \boldsymbol{b}$ has a unique solution
- Proposition 2.7.a: a matrix is invertible iff its RREF is identity matrix
- Corollary 2.7.b: every invertible matrix is a product of elementary matrices
- Theorem 2.7.c: method for finding matrix inverses using EROs

Section 3

- Proposition 3.1.a: properties of a vector space
- Proposition 3.1.b: vector subspace always contains zero vector
- Proposition 3.1.c: vector subspace is a vector space
- Proposition 3.2.a: span is a vector subspace
- [3.2.7]: expression for column space
- [3.3.4]: equivalent definition of linear dependence for two nonzero vectors
- [3.3.5]: relationship between linear (in)dependence of subsets
- [3.4.2]a: spanning set cannot be strictly smaller than basis
- [3.4.2]b: spanning set strictly greater than basis is not linearly independent
- Theorem 3.4.a: criterion for being a basis (unique linear combination)
- Proposition 3.5.a: cardinality of linear independent set is less than or equal to the dimension
- Corollary 3.5.b: same cardinality for two bases
- [3.5.6]a: dimension of span
- [3.5.6]b: dimension of vector subspace
- Theorem 3.6.a: adding a vector not in span preserves linear independence
- Theorem 3.6.b: linear independent set having cardinality equal to dimension must be basis
- Theorem 3.6.c: possibility of removing a vector from a linearly dependent set while preserving the span
- Lemma 3.6.d: existence of basis for $\operatorname{span}(S)$ in finite set S
- Theorem 3.6.e: spanning set having cardinality equal to dimension must be basis
- Theorem 3.7.a: criteria for matrix invertibility
- Theorem 3.7.b: preservation of linear independence after multiplication of invertible matrix
- Theorem 3.7.c: preservation of dimension of column space after multiplication of invertible matrix
- Proposition 3.7.d: reduction of dimension of column space after multiplication of matrix
- Theorem 3.7.e: columns corresponding to the leading ones in the RREF form a basis for column space
- Corollary 3.7.f: dimension of column space is the number of leading ones in the RREF
- Theorem 3.8.a: preservation of row space after multiplication of invertible matrix

- Proposition 3.8.b: reduction of dimension of row space after multiplication of matrix
- Theorem 3.8.c: nonzero rows of the RREF form a basis for row space
- Corollary 3.8.d: dimension of row space is the number of leading ones in the RREF
- Theorem 3.9.a: equality of dimensions of column and row spaces
- Corollary 3.9.b: taking matrix transpose does not change rank
- Theorem 3.10.a: null space is a vector subspace
- Theorem 3.10.b: dimension and basis of null space

Section 4

- Proposition 4.1.a: preservation of zero and linear combinations after linear transformation
- Theorem 4.1.b: construction of linear transformation from basis
- [4.2.4]: null space and range of a linear transformation associated to a matrix
- Proposition 4.2.a: null space and range of a linear transformation are vector subspaces
- Proposition 4.2.b: range is the spanning set of linearly transformed vectors in basis
- Theorem 4.2.c: dimension formula
- [4.2.10]: rank-nullity theorem
- Proposition 4.3.a: relationship between injectivity and null space
- Theorem 4.3.b: criteria for injectivity of a linear transformation
- Proposition 4.3.c: sufficient condition for non-injectivity of a linear transformation
- Lemma 4.3.d: subspace W of V equals V if W has the same dimension as V
- Theorem 4.3.e: criterion for bijectivity of a linear transformation about null space and dimensions
- Corollary 4.3.f: criteria for bijectivity of a linear transformation
- Theorem 4.4.a: relationship between matrix representation and matrix-vector product
- Theorem 4.4.b: addition of linear transformations corresponds to addition of matrix representations
- Theorem 4.4.c: composition of linear transformations corresponds to multiplication of matrix representations
- Theorem 4.4.d: invertibility of a linear transformation corresponds to invertibility of its matrix representation
- [4.4.15]: finding matrix inverse from the inverse of linear transformation
- Theorem 4.4.e: equality of ranks/nullities of linear transformation and its matrix representation
- Theorem 4.5.a: properties of change of coordinates matrix
- Theorem 4.5.b: method for changing matrix representation of linear transformation
- [4.5.5]: matrix similarity is an equivalence relation
- [4.5.6]a: similar matrices have the same rank
- [4.5.6]b: similar matrices have the same determinant

Section 5

- [5.1.3]: a matrix is diagonalizable iff its inverse is diagonalizable
- Proposition 5.1.a: eigenvalues and eigenvectors of diagonal matrices
- [5.1.7]: properties about eigenvalues of eigenvectors for invertible matrices
- Theorem 5.1.b: diagonalization through eigenvalues and eigenvectors
- Theorem 5.1.c: criterion for diagonalizability based on eigenvectors
- [5.1.11]: criterion for diagonalizability for matrix with one eigenvalue
- Theorem 5.2.a: eigenvalues are roots of characteristic polynomials
- Proposition 5.2.b: upper bound of number of distinct eigenvalues
- Theorem 5.3.a: eigenvectors with different eigenvalues are linear independent
- Corollary 5.3.b: sufficient condition for being diagonalizable based on number of distinct eigenvalues
- [5.4.3]: expression of characteristic polynomial with algebraic multiplicities
- [5.4.4]: sum of all algebraic multiplicities for an $n \times n$ matrix is n
- [5.4.5]: bounds for algebraic multiplicity
- [5.4.7]: lower bound for geometric multiplicity
- Theorem 5.4.a: G.M. $\leq$ A.M.
- Theorem 5.4.b: diagonalizability criterion based on A.M. and G.M.
- Corollary 5.4.c: diagonalizability criterion based on sum of all geometric multiplicities
- [5.5.3]: computing high powers of matrices through diagonalization
- [5.5.7]: computing matrix exponentials through diagonalization

Section 6

- Proposition 6.1.a: properties of inner product
- [6.1.7]: relationship between standard inner product and matrix transpose
- Proposition 6.1.b: injectivity of norm-preserving linear transformation
- Proposition 6.1.c: properties of norm
- Theorem 6.2.a: linear independence of orthogonal set containing nonzero vectors
- Theorem 6.2.b: expression of linear combination of vectors in orthogonal set
- Theorem 6.2.c: method for constructing orthogonal basis from an arbitrary basis
- Corollary 6.2.d: existence of orthonormal basis for a finite-dimensional inner product space
- Proposition 6.3.a: properties of orthogonal complements
- Theorem 6.3.b: orthogonal decomposition theorem