Linear Transformations

Evan Halloran

2025

The theory of linear transformations is the only "solved" field of mathematics—that is to say, every question formulated within the confines of linear algebra has already been solved. Because of this, it is often said that if one can reduce a problem in a different field (e.g. algebra, analysis, partial differential equations) to that of linear algebra, then a solution will emerge with ease. Linearization as a technique is ubiquitous throughout mathematics, and facility with linear algebra will pay dividends. These notes will cover both the basic computations of linear algebra as well as the theory of linear transformations as a whole.

1 Preliminaries

1.1 Sets

Definition (Georg Cantor, 1895)**.** A **set** is any collection M of definite, distinguishable objects m of our perception or thought conceived of as a whole. The objects m of M are called the **elements** of M.

> "Nowadays it is known to be possible, logically speaking, to derive practically the whole known mathematics from a single source, namely the Theory of Sets."
> — Nicolas Bourbaki, 1950

Notation. $M = \{m \mid \text{defining property for } m \text{ to belong to } M\}$. If m is an element of M, we write $m \in M$ and say m belongs to M. Otherwise, we write $m \notin M$.

Examples.

$$\begin{aligned}
\mathbb{N} = \{1,\, 2,\, 3,\, 4,\, ...\} &= \text{ positive integers} \\
-1 \notin \mathbb{N}_0 = \{0,\, 1,\, 2,\, 3,\, ...\} &= \text{ non-negative integers} \\
-1 \in \mathbb{Z} = \{0,\, 1,\, -1,\, 2,\, -2,\, 3,\, -3,\, ...\} &= \text{ integers} \\
\sqrt{2} \notin \mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a\,, b \in \mathbb{Z},\, b \neq 0 \right\} &= \text{ rational numbers} \\
\sqrt{2} \in \mathbb{R} = &\text{ real numbers} \\
i \in \mathbb{C} = &\text{ complex numbers}
\end{aligned}$$

If a set M has only finitely many elements then it's called finite, and $|M|$ = number of elements in M = cardinality (size) of M. For example, $|\{1, 2, 3\}| = 3$.

Caution. A set is not the same as a list or sequence. For instance, $\{1, 2\} = \{2, 1\} = \{1, 2, 1\}$, but $(1, 2) \neq (2, 1)$. The later are examples of ordered pairs.

Example. The **empty set** $\emptyset$ is the only set which has **no** element, i.e. $|\emptyset| = 0$.

Notation (operations on sets)**.** Let M and N be sets.
$M \subset N$: M is a subset of N, i.e. every $m \in M$ also belongs to N. $\mathbb{N} \in \mathbb{N}_0 \in \mathbb{Z} \in \mathbb{Q} \in \mathbb{R} \in \mathbb{C}$
$M \cap N$: intersection of M and N, i.e. count of all $m \in M$ which also belong to N.
$M \backslash N$: complement of N in M, consists of all $m \in M$ which do not belong to N.

(a) $M \cap N$ (b) $M \setminus N$

Figure 1: Venn diagrams illustrating set intersection and set difference.

Definition. The **cartesian product** of two sets M and N is the set
$M \times N = \{(a, b) \mid a \in M,\, b \in N\}$ consisting of all ordered pairs with first coordinate in M and second coordinate in N. If $a \neq b$, then $(a, b) \neq (b, a)$, even if $N = M$.

Example. The cartesian product $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(a, b) \mid a \in \mathbb{R},\, b \in \mathbb{R}\}$ is the set of vectors in the plane.

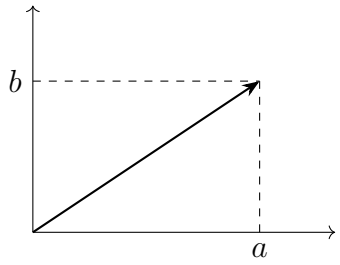

Figure 2: The vector (a, b) in $\mathbb{R}^2$.

Example. If $M = \{1, 2\}$ and $N = \{1, 2, 3\}$, then $|M \times N| = |M| \cdot |N| = 6$. In particular, $(1, 1) \in M \times N$.

Definition. The **power set** $\mathcal{P}(M)$ of a set M consists of all subsets of M, including $\emptyset$ ($\emptyset \subset M$) and M itself.

Example. If $M = \{1, 2\}$, then $\mathcal{P}(M) = \{\emptyset, \{1, 2\}, \{1\}, \{2\}\}$ and $|\mathcal{P}(M)| = 4$.

Fact. If $|M| < \infty$, then $|\mathcal{P}(M)| = 2^{|M|}$.

1.2 Functions

Definition. Let X and Y be sets. A **map** (function) from X to Y (written $f : X \to Y$, or $X \xrightarrow{f} Y$) is a rule which assigns to every $x \in X$ a unique element $f(x) \in Y$. The set X is called the **domain** of f, and Y is called the **target** of f.

Examples. Some mappings are presented below.

1. $X = \mathbb{R} = Y$, $f(x) = x^2$.
2. $X = \mathbb{R}$, $Y = \mathbb{Z}$, $f(x) = \lfloor x \rfloor$ = floor function of x = largest integer $\leq x$.
3. $X = \mathbb{R}^2$, $Y = \mathbb{R}$, $f(x, y) = 3x - 2y$.

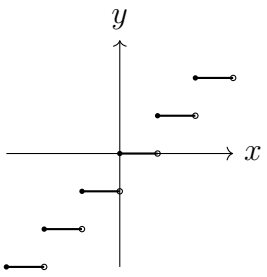

Figure 3: Graph of the floor function $y = \lfloor x \rfloor$.

Definition. Let $f : X \to Y$ be a map. The map f is called

1. **injective** (or one-to-one) if for every $x_1, x_2 \in X$ the following is true: $f(x_1) = f(x_2) \implies x_1 = x_2$;
2. **surjective** (or onto) if for every $y \in Y$, there is some $x \in X$ such that $f(x) = y$;
3. **bijective** if it is injective and surjective.

Fact. If $f : X \to Y$ and $|X|, |Y| < \infty$, then f injective $\implies |X| \leq |Y|$.

(a) Injective but not surjective

(b) Surjective but not injective

Figure 4: Illustrations of injective and surjective functions.

Examples.

1. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = e^x$ is injective but not surjective.
2. $f : \mathbb{R} \to \mathbb{R}_{>0} := \{x \in \mathbb{R} \mid x > 0\}$, $f(x) = e^x$ is bijective. In this case, the inverse of f is $f^{-1} : \mathbb{R}_{>0} \to \mathbb{R}$, $f^{-1} = \ln(x)$.
3. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ is neither injective nor surjective. However, $f : [0, \infty) \to \mathbb{R}$, $f(x) = x^2$ is injective.

(a) $y = e^x$

(b) $y = x^2$

Figure 5: (a) Exponential function maps onto $\mathbb{R}_{>0}$; (b) Quadratic function maps x and $-x$ to the same point.

Some notation from logic.

1. $\forall$ = "for all"
2. $\exists$ = "there exist(s)"
3. $\implies$ = "implication"
4. $A \iff B$ = "A and B are equivalent"

The first two of these symbols are called quantifiers.

Example. $f : X \to Y$ is surjective if $\forall y \in Y \ \exists x \in X : f(x) = y$.

Definition. Given $X \xrightarrow{f} Y$, we call $f(x)$ the **image of** $x \in X$. If $S \subset X$ is a subset of X, then $f(S) = \{f(x) \mid x \in S\} \subset Y$ is called the **image of** S. The **image of the function** f is $\mathrm{im}(f) := f(X)$.

Note: f is surjective $\iff \mathrm{im}(f) = Y$.

Definition. Given $T \subset Y$, we call $f^{-1}(T) = \{x \in X \mid f(x) \in T\}$ the **preimage of** T under f. An element $x \in X$ with $f(x) = y$ is called **a preimage of** y.

Note:

1. $f : X \to Y$ is **surjective** if $\forall y \in Y : |f^{-1}(\{y\})| \geq 1$;
2. $f : X \to Y$ is **injective** if $\forall y \in Y : |f^{-1}(\{y\})| \leq 1$;
3. $f : X \to Y$ is **bijective** if $\forall y \in Y : |f^{-1}(\{y\})| = 1$.

Caution. Do not confuse $\{y\} \subset Y$ with $y \in Y$. There is a difference between $f^{-1}(\{y\})$ and $f^{-1}(y)$ (the later is only defined when f is bijective).

If $f : X \to Y$ is bijective, then the **inverse map** $f^{-1} : Y \to X$ is defined by $f^{-1}(y) = x$ if $f(x) = y$.

Note:

1. $\forall x \in X, \ f^{-1}(f(x)) = x$;
2. $\forall y \in Y, \ f(f^{-1}(y)) = y$.

Two maps $f : X \to Y$ and $g : X' \to Y'$ are the same if $X' = X$ and $Y' = Y$ and $\forall x \in X, \ f(x) = g(x)$.

1.3 Fields

Definition. A **field** F is a set equipped with two maps

$$\text{“addition”} \ + : \ F \times F \to F, \ (a, b) \mapsto a + b$$
$$\text{“multiplication”} \ \cdot \ : \ F \times F \to F, \ (a, b) \mapsto a \cdot b \ \ (= ab)$$

satisfying the following conditions (called the field axioms) for all a, b, $c \in F$:

F1. $a + b = b + a$ and $a \cdot b = b \cdot a$ (**commutativity** of $+$ and $\cdot$)

F2. $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (**associativity** of $+$ and $\cdot$)

F3. $\exists\, 0_F \in F, \ \exists\, 1_F \in F : \ a + 0_F = a$ and $a \cdot 1_F = a$. Moreover, we require that $0_F \neq 1_F$.

F4. $\forall\, a \in F, \ \exists\, b \in F : \ a + b = 0_F$. The element $b = -a$ is called the **additive inverse** of a.
$\forall\, a \in F \setminus \{0\}, \ \exists\, c \in F : \ a \cdot c = 1_F$. The element $c = a^{-1} = \frac{1}{a}$ is called the **multiplicative inverse** of a.

F5. $a \cdot (b + c) = ab + ac$ (**distributive law**)

Examples.

1. $F = \mathbb{R}$ with the usual addition and multiplication is a field
2. $F = \mathbb{Q}$ with the usual addition and multiplication is a field
3. $F = (\mathbb{Z}, +, \cdot)$ is <u>not</u> a field
4. $\mathbb{F}_2 = \{0, 1\}$ is a field under the following addition and multiplication:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Field axiom **F3** alone generates most of the tables. Notice that it cannot be the case that $1 + 1 = 1$, for then $1 = 0$ which is not permitted in any field.

Cancellation Laws. If a, b, c are elements of a field F, then $a + b = a + c \implies b = c$. If $a \neq 0$, then $a \cdot b = a \cdot c \implies b = c$.

1.4 Complex Numbers

Definition. Set $i = \sqrt{-1}$ and consider it for the moment just as a symbol. A **complex number** is a linear combination of the form $x + iy$ with $x, y \in \mathbb{R}$.

$$\begin{aligned} \text{addition:} \quad & (x+iy) + (x'+iy') = (x+x') + i(y+y') \\ \text{multiplication:} \quad & (x+iy) \cdot (x'+iy') = (xx'-yy') + i(xy'+yx') \end{aligned}$$

We call $x = \mathrm{Re}(x+iy)$ the real part and $y = \mathrm{Im}(x+iy)$ the imaginary part.
Note. $i \cdot i = (0 + i \cdot 1)(0 + i \cdot 1) = (0 \cdot 0 - 1 \cdot 1) + i(0 \cdot 1 + 1 \cdot 0) = -1$.
We consider $x + i \cdot 0$ to be equal to x. The set of all the numbers $x + iy$ we denote by $\mathbb{C}$, called the **the field of complex numbers**. Commutativity and associativity follow from the definitions of complex addition and multiplication.

$$\begin{aligned} \text{zero element:} \quad & 0 = 0 + i \cdot 0 \\ \text{identity for multiplication:} \quad & 1 = 1 + 0 \cdot i \cdot \\ \text{inverse for addition:} \quad & -(x+iy) = -x + i(-y) \\ \text{inverse for multiplication:} \quad & (x+iy)^{-1} = \frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2} \\ & \qquad = \frac{x}{x^2+y^2} + i\frac{-y}{x^2+y^2} \end{aligned}$$

If $z = x + iy$, then $|z| = \sqrt{x^2+y^2}$ is called the (complex) absolute value, or **modulus**, of z, and $\bar{z} = x - iy = x + i(-y)$ is called the (complex) **conjugate** of z.