Sets and functions

Before beginning with the linear algebra content proper we revise some important general concepts and notations. Sets and functions are fundamental to linear algebra (and to modern mathematics in general).

1.1 Sets

A **set** is a collection of objects called **elements** (or **members**) of that set.[a] The notation $x \in A$ means that x is an element of the set A. The notation $x \notin A$ is used to mean that x is not a member of A.

Let A and B be sets. We say that A is **a subset of** (or **is contained in** B), written $A \subseteq B$, if every element of A is also an element of B (i.e., $x \in A$ implies $x \in B$). Two sets are **equal** if they have the same members. Thus $A = B$ exactly when both $A \subseteq B$ and $B \subseteq A$. If $A \subseteq B$ and $A \neq B$ then we say that A is a **proper subset** of B and sometimes write $A \subsetneq B$.

Sets are often defined either by listing their elements, as in $A = \{0, 2, 3\}$, or by giving a rule or condition which determines membership in the set, as in $A = \{x \in \mathbb{R} \mid x^3 - 5x^2 + 6x = 0\}$.

Here are some familiar (mostly mathematical) sets:

- ▷ **natural numbers**: $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$
- ▷ **integers**: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- ▷ **rational numbers**: $\mathbb{Q} = \{\, \frac{x}{y} \mid x, y \in \mathbb{Z}, y \neq 0\}$
- ▷ real numbers:[b] $\mathbb{R}$
- ▷ $(1, 3] = \{x \in \mathbb{R} \mid 1 < x \leqslant 3\}$
- ▷ Greek alphabet (lower case): $\{\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, \theta, \iota, \kappa, \lambda, \mu, \nu, \xi, o, \pi, \sigma, \tau, \upsilon, \varphi, \chi, \psi, \omega\}$

In these examples we have the following containment relations: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ and $(1, 3] \subset \mathbb{R}$. Note that $(1, 3] \not\subseteq \mathbb{Q}$ because the interval $(1, 3]$ contains real numbers that are not rational. For example, $\sqrt{2} \in (1, 3]$ but $\sqrt{2} \notin \mathbb{Q}$.

Example 1.1. Let $A = \{5m + 1 \mid m \in \mathbb{Z}\}$ and $B = \{5m - 4 \mid m \in \mathbb{Z}\}$. It is clear that $A \subseteq \mathbb{Z}$ and $B \subseteq \mathbb{Z}$. We show that $A = B$. Suppose that $a \in A$. Then $a = 5m + 1$ for some $m \in \mathbb{Z}$. But then $a = 5(m + 1) - 4$, which, since $m + 1 \in \mathbb{Z}$, implies that $a \in B$. Therefore $A \subseteq B$. For the reverse inclusion, let $b \in B$. Then $b = 5m - 4$ for some $m \in \mathbb{Z}$. But then $b = 5(m - 1) + 1$, which, since $m - 1 \in \mathbb{Z}$, implies that $b \in A$. Therefore $B \subseteq A$. Having shown that $A \subseteq B$ and $B \subseteq A$ we conclude that $A = B$.

As indicated above, the notation $\{\ldots\}$ is used for set formation. Sets are themselves mathematical objects and so can be members of other sets. For instance, the set $\{3, 5\}$ consists of two elements,

[a] In fact, more care is needed in the definition of a set. In general one must place some restriction on set formation. For example, trying to form $\{x \mid x \text{ is a set}\}$ or $\{x \mid x \notin x\}$ can lead to logical paradoxes (Russell's paradox). This can be dealt with or excluded in a more formal or axiomatic treatment of set theory. We will be careful to avoid situations where this difficulty arises.

[b] It's a bit more difficult to define the real numbers precisely, but one can think of them either as the points on the real line or as (infinite) decimal expansions. In this subject we will be using some standard properties of $\mathbb{R}$, but we will not give a construction.

namely the numbers 3 and 5. The set $\{\{3,5\},\{3,7\},\{7\},3\}$ consists of 4 elements, namely the sets $\{3,5\}$,$\{3,7\}$, $\{7\}$ and the integer 3. Note that $7 \notin \{\{3,5\},\{3,7\},\{7\},3\}$. Observe that $\{7\}$ is the set whose only element is the number 7. Note that $7 \in \{7\}$ but $7 \not\subseteq \{7\}$.

The **empty set**, denoted by $\emptyset$, is the set that has no elements, that is, $x \in \emptyset$ is never true.

Lemma 1.2

The empty set is a subset of every set.

Proof. Let A be a set. We need to show that the following statement is true:

$$\text{if } a \in \emptyset, \text{ then } a \in A \tag{$*$}$$

Let's suppose that $(*)$ were not true. Then there would be an element a such that $a \in \emptyset$ is true and $a \in A$ is false. However, since $a \in \emptyset$ is never true, no such a exists and we conclude that $(*)$ must in fact be true. □

Note that $\emptyset \in \{\emptyset\}$ and $\emptyset \subseteq \{\emptyset\}$ but $\emptyset \notin \emptyset$.

1.1.1 Operations on sets

The **intersection** of two sets A and B is the set

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

The **union** of A and B is the set

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

Example 1.3.

1) $\{2m+5 \mid m \in \mathbb{Z}\} \cup \{2m \mid m \in \mathbb{Z}\} = \mathbb{Z}$

2) $\{2m+5 \mid m \in \mathbb{Z}\} \cap \{2m \mid m \in \mathbb{Z}\} = \emptyset$

3) $\{n \in \mathbb{N} \mid n \text{ is prime}\} \cap \{2n \mid n \in \mathbb{N}\} = \{2\}$

The **set difference** of two sets A and B is the set

$$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$$

If $B \subseteq A$, then $A \setminus B$ is called the **complement** of B in A. If the larger set A is clear from the context, we sometimes write B^c for the complement of B in A.

Example 1.4.

1) $\mathbb{Z} \setminus \mathbb{N} = \{\ldots, -2, -1, 0\}$

2) $\mathbb{N} \setminus \mathbb{Z} = \emptyset$

3) $[0,2] \setminus \mathbb{N} = [0,1) \cup (1,2)$

4) $\mathbb{N} \setminus [0,2] = \{3,4,\ldots\}$

Proposition 1.5: De Morgan's Laws

Let $A, B \subseteq X$ be two sets. Then

1. $A \subseteq B$ if and only if $B^c \subseteq A^c$
2. $(A \cap B)^c = A^c \cup B^c$
3. $(A \cup B)^c = A^c \cap B^c$

Given a set A, the **power set** of A is the set containing all subsets of A. It is denoted $\mathcal{P}(A)$.

Example 1.6. For $A = \{\alpha, \beta, \gamma\}$ we have $\mathcal{P}(A) = \{\emptyset, \{\alpha\}, \{\beta\}, \{\gamma\}, \{\alpha, \beta\}, \{\alpha, \gamma\}, \{\beta, \gamma\}, \{\alpha, \beta, \gamma\}\}$.

Let A and B be two sets. We define a set, called the **Cartesian product** of A and B, by

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

Each element (a, b) of the set $A \times B$ is called an **ordered pair**.

Remark.
1. $(a, b) = (a', b')$ precisely when $a = a'$ and $b = b'$.
2. If $A \neq B$, then $A \times B \neq B \times A$.
3. If $A = B$, we often write A^2 in place of $A \times A$.

1.2 Functions

The concept of a function is fundamental in mathematics. Functions on the real numbers are often described using some sort of a formula (e.g., $f(x) = \sin(x)$), but we want to define the notion of function in a way that makes sense more generally. The idea is to make a definition out of what is sometimes called the graph of a function.

Definition 1.7

Let A and B be sets. A **function from A to B** is a subset f of $A \times B$ such that for each $a \in A$ there is exactly one element of f whose first entry is a. We write $f(a) = b$ to mean $(a, b) \in f$. We write $f : A \to B$ to mean that f is a function from A to B. The set A is called the **domain** of the function and B is called the **codomain** of the function.

Remark.
1. Functions are often (but not always!) given by a formula such as $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. When written in this way, the subset of $A \times B$ is understood to be $\{(a, f(a)) \mid a \in A\}$.
2. The domain and codomain are part of the defining data of a function. The following two functions are *not* the same:

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2$$
$$g : [0, \infty) \to \mathbb{R}, \quad g(x) = x^2$$

Definition 1.8

Let $f : A \to B$ be a function.

1. We say that f is **injective** if $f(a_1) = f(a_2)$ implies $a_1 = a_2$.
2. We say that f is **surjective** if for all $b \in B$ there exists $a \in A$ with $f(a) = b$.
3. We say that f is **bijective** if it is both injective and surjective.

Example 1.9.

1) The function $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ is neither injective nor surjective.

2) The function $g : [0, \infty) \to \mathbb{R}, g(x) = x^2$ is injective but not surjective.

3) The function $h : \mathbb{R} \to [0, \infty), h(x) = x^2$ is surjective but not injective.

4) The function $k : [0, \infty) \to [0, \infty), k(x) = x^2$ is bijective.

Example 1.10.

1) $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, f(m, n) = 2^m 3^n$ is injective (but not surjective).

2) $g : \mathbb{N} \to \mathbb{Z}, g(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{1-n}{2} & \text{if } n \text{ is odd} \end{cases}$ is bijective.

Let $f : A \to B$ and $g : B \to C$ be two functions. The **composition** of f and g is the function $g \circ f : A \to C$ given by $g \circ f(a) = g(f(a))$. Given a set A, the **identity function** on A is the function $\mathrm{Id}_A : A \to A$, $\mathrm{Id}_A(a) = a$. If $f : A \to B$ is a bijection, then there is a well-defined **inverse function** $f^{-1} : B \to A$ having the property that $f \circ f^{-1} = \mathrm{Id}_B$ and $f^{-1} \circ f = \mathrm{Id}_A$. Indeed, if we think of functions as sets of ordered pairs and f is a bijection, then the ordered pairs of f^{-1} are just the pairs of f in reverse order.

Example 1.11. Consider the function $f : \mathbb{N} \to \mathbb{Z}_{\geqslant 2}, f(n) = n+1$. The corresponding subset of $\mathbb{N} \times \mathbb{Z}_{\geqslant 2}$ is

$$\{(1, 2), (2, 3), (3, 4), \dots\}$$

The function f is a bijection. Its inverse is $f^{-1} : \mathbb{Z}_{\geqslant 2} \to \mathbb{N}, f^{-1}(n) = n-1$ which as a subset of $\mathbb{Z}_{\geqslant 2} \times \mathbb{N}$ is

$$\{(2, 1), (3, 2), (4, 3), \dots\}$$

In mathematics one often needs functions of several variables, for example the operation of addition of real numbers is a function of two variables which assigns to each pair of real numbers (x, y) their sum $x + y$. Thus addition is a function from $\mathbb{R}^2$ to $\mathbb{R}$. More generally, a **function of n variables** from A to B (or an n-ary function f from A to B) is just a function of the form $f : A^n \to B$.

1.3 Exercises

1. List five elements belonging to each of the following sets:

   (a) $\{n \in \mathbb{N} \mid n \text{ is divisible by } 5\}$
   (b) $\mathcal{P}(\{1, 2, 3, 4, 5\})$
   (c) $\{n \in \mathbb{N} \mid n + 1 \text{ is a prime }\}$
   (d) $\{2^n \mid n \in \mathbb{N}\}$
   (e) $\{r \in \mathbb{Q} \mid 0 < r < 1\}$

2. Determine which of the following sets are nonempty and list their elements:

   (a) $\{n \in \mathbb{N} \mid n^2 = 3\}$
   (b) $\{n \in \mathbb{Z} \mid 3 < |n| < 7\}$
   (c) $\{x \in \mathbb{R} \mid x < 1 \text{ and } x \geqslant 2\}$
   (d) $\{3n + 1 \mid n \in \mathbb{N} \text{ and } n \leqslant 6\}$
   (e) $\{n \in \mathbb{N} \mid n \text{ is a prime and } n \leqslant 15\}$

3. Consider the sets

   $A = \{n \in \mathbb{N} \mid n \text{ is odd }\}$
   $B = \{n \in \mathbb{N} \mid n \text{ is a prime }\}$
   $C = \{4n + 3 \mid n \in \mathbb{N}\}$
   $D = \{x \in \mathbb{R} \mid x^2 - 8x + 15 = 0\}$

   Which are subsets of which? Consider all sixteen possibilities.

4. Consider the sets

$A = \{n \in \mathbb{N} \mid n \leq 11\}$ $E = \{n \in \mathbb{N} \mid n \text{ is even}\}$
$B = \{n \in \mathbb{N} \mid n \text{ is even and } n \leq 20\}$

Determine each of the following sets:

(a) $A \cup B$ (c) $A \setminus B$ (e) $E \cap B$ (g) $E \setminus B$
(b) $A \cap B$ (d) $B \setminus A$ (f) $B \setminus E$ (h) $\mathbb{N} \setminus E$

5. Prove (directly from the definitions of the operations) that $(A \cup B) \cap A^c \subseteq B$.

6. Prove or disprove each of the following: (A proof needs to be a general argument. A single counterexample is enough to disprove an assertion.)

   (a) $A \cap B = A \cap C$ implies $B = C$
   (b) $A \cup B = A \cup C$ implies $B = C$
   (c) ($A \cap B = A \cap C$ and $A \cup B = A \cup C$) implies $B = C$

7. Let $S = \{0, 1, 2, 3, 4\}$ and $T = \{0, 2, 4\}$.

   (a) How many elements are there in $S \times T$? How many in $T \times S$?
   (b) List the elements in $\{(m, n) \in S \times T \mid m < n\}$.
   (c) List the elements in $\{(m, n) \in T \times S \mid m < n\}$.
   (d) List the elements in $\{(m, n) \in S \times T \mid m + n \geq 3\}$.
   (e) List the elements in $\{(m, n) \in T \times S \mid mn \geq 4\}$.
   (f) List the elements in $\{(m, n) \in S \times S \mid m + n = 10\}$.

8. Let $S = \{1, 2, 3, 4, 5\}$ and $T = \{a, b, c, d\}$. For each question below: if the answer is "yes" give an example; if the answer is "no" explain briefly.

   (a) Are there any injective functions from S to T?
   (b) Are there any injective functions from T to S?
   (c) Are there any surjective functions from S to T?
   (d) Are there any surjective functions from T to S?
   (e) Are there any bijective functions from S and T?

9. Let $S = \{1, 2, 3, 4, 5\}$ and consider the following functions from S to S: $1_S(n) = n$, $f(n) = 6 - n$, $g(n) = max\{3, n\}$ and $h(n) = max\{1, n - 1\}$.

   (a) Write each of these functions as a set of ordered pairs.
   (b) Which of these functions are injective and which are surjective?

10. Consider the two functions from $\mathbb{N}^2$ to $\mathbb{N}$ defined by $f(m, n) = 2^m 3^n$ and $g(m, n) = 2^m 4^n$. Show that f is injective but that g is not injective. Is f surjective? Explain. (You may use that every $n \in \mathbb{N}$ with $n \geqslant 2$ has a unique prime factorisation.)

11. Show that if $f : A \to B$ and $g : B \to C$ are injective functions, then $g \circ f$ is injective.

12. Show that composition of functions is associative, that is, $h \circ (g \circ f) = (h \circ g) \circ f$.

13. Here are two 'shift functions' mapping $\mathbb{N}$ to $\mathbb{N}$:

$$R : \mathbb{N} \to \mathbb{N}, \quad R(n) = n + 1$$
$$L : \mathbb{N} \to \mathbb{N}, \quad L(n) = \max\{1, n - 1\}$$

   (a) Show that R is injective but not surjective.
   (b) Show that L is surjective but not injective.
   (c) Show that $L \circ R = \mathrm{Id}_{\mathbb{N}}$ but that $R \circ L \neq \mathrm{Id}_{\mathbb{N}}$.

Further reading for lecture 1

The extra material at the end of a lecture can include extra theory or references. It is NOT required! It is just for those who would like to know more.

▷ Some references for introductory set theory:

The Art of Proof by Beck and Geoghegan, chapter 5.
Naive Set Theory by Halmos.
Zermelo-Fraenkel set theory on Wikipedia.
Russell's paradox on Wikipedia.

▷ The axiomatic definition of the real numbers $\mathbb{R}$ and their construction from $\mathbb{Q}$ will be covered in the subject *MAST20033 Real Analysis: Advanced* (amongst others). An important difference between $\mathbb{Q}$ and $\mathbb{R}$ is that every bounded subset of $\mathbb{R}$ has a least upper bound. A standard construction of $\mathbb{R}$ from $\mathbb{Q}$ is via "Dedekind cuts" which, roughly speaking, carefully adds least upper bounds to $\mathbb{Q}$.

The Art of Proof by Beck and Geoghegan, chapter 8.
Principles of Mathematical Analysis by Rudin, chapter 1.

▷ Bijections are used in the definition of the **cardinality** (or size) of a set. Two sets are said to have the same cardinality if there exists a bijection from one to the other. The sets $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ all have the same cardinality, but $\mathbb{R}$ does not. In particular, there is a bijection from $\mathbb{N}$ to $\mathbb{Q}$. That there is no bijection from $\mathbb{N}$ to $\mathbb{R}$ can be shown with an elegant argument known as 'Cantor diagonalisation'.

The Art of Proof by Beck and Geoghegan, chapter 13.

▷ **Terminology:** theorem, proposition, lemma, corollary,... what's the difference?
These are all statements of results that are proven to be true. The difference is a little subjective, and the choice usually reflects the author's view of how important or interesting the result is. Theorems are results that are considered important. Propositions are less important but still interesting. Lemmas are usually shorter results that are used in proving other statements. A corollary is a statement that follows easily from a previously proven theorem or proposition.