Module 2: Language of Mathematics

Theme 1: Sets

A **set** is a collection of objects. We describe a set by listing all of its elements (if this set is finite and not too big) or by specifying a property that uniquely identifies it.

Example 1: The set A of all decimal digits is

$$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

But to define a set of all even positive integers we write:

$$I = \{k : \ k = 2n, \text{ where } n \text{ is a natural number}\}.$$

The last definition can be also written in another form, namely:

$$I = \{k \mid k \text{ is an even natural number}\}.$$

In the rest of this course, we shall either write $\{x : \text{ property describing } x\}$ or $\{x \mid \text{property describing } x\}$, where : or | should be read as "such as". Both are used in discrete math, however, we prefer the former. This notation is called the **set builder**.

Let A be a set such that elements $a, b, \ldots$ belong to it. We shall write

$$a \in A$$

if a is an element of A. If x does *not* belong to A we denote it as $x \notin A$.

Uppercase letters are usually used to denote sets. Some letters are reserved for often used sets such as the set of natural numbers $\mathbf{N} = \{0, 1, 2, \ldots\}$ (i.e., set of all counting numbers), the set of integers $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ (i.e., positive and negative natural numbers together with zero), and the set of rational numbers which are ratios of integers, that is, $\mathbf{Q} = \{r : \ r = m/n, \ m, n \in \mathbf{Z}\}$. A set with no elements is called the **empty** (or **null**) **set** and is denoted as $\emptyset$.

The set A is said to be a **subset** of B if and only if every element of A is also an element of B. We shall write $A \subseteq B$ to indicate that A is a subset of B.

Example 2: The set $A = \{1, 3\}$ is a subset of $B = \{0, 1, 3, 5, 7\}$. Actually, in this case A is a **proper** subset of A, and we write it as $A \subset B$. By proper we mean that there exits at least one element of B that is *not* an element of A (in our example such elements are 0, or 5 or 7).

Two sets A and B are **equal** if and only if they have the same elements. We will subsequently make this statement more precise. For example, the sets $A = \{1, 3, 5\}$ and $B = \{5, 3, 1\}$ are equal since order does not matter for sets. When the sets are finite and small, one can verify this by listing all elements of the sets and comparing them. However, when sets are defined by the set builder it is sometimes harder to decide whether two sets are equal or not. For example, is the set $R = \{x : \ e^{2\pi ix} = 1\}$ (i.e., solutions of this weird looking equation $e^{2\pi ix} = 1$, where $i = \sqrt{-1}$) equal to **Z**? Therefore, we introduce another equivalent definition: $A = B$ if whenever $a \in A$, then $a \in B$ **and** whenever $b \in B$, then $b \in B$. The last statement can be written as follows:

$$A = B \quad \text{if and only if} \quad A \subseteq B \ \textbf{ and } \ B \subseteq A. \tag{1}$$

(To see this, one can think of two real numbers a and b that are equal; to prove this fact it suffices to show that $a \le b$ and $b \le a$.) This equivalence is very useful when proving some theorems regarding sets.

If A is finite, then the number of elements of A is called its **cardinality** and denoted as $|A|$, that is,

$$|A| \ = \ \text{number of elements in A.}$$

A set is said to be infinite if it has an infinite number of elements. For example, the cardinality of $A = \{a, b, c\}$ is 3, while **N** is an infinite set.

The set of *all* subsets of a given set A is called the **power set** and denoted $\mathcal{P}(A)$.

Example 3: If $A = \{a, b, c\}$, then there are 8 subsets of A, namely:

$$\emptyset, \ \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}.$$

Thus the cardinality of $\mathcal{P}(A)$ is $8 = 2^3$.

Now, we shall prove our first theorem about sets.

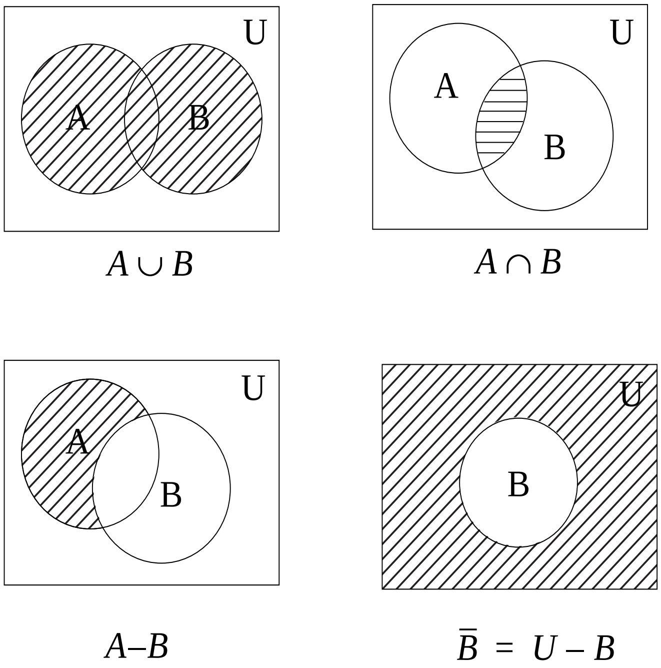
Theorem 1. *If* $|A| = n$, *then* $|\mathcal{P}(A)| = 2^n$.

Proof:[1] The set A has n elements and we can name them any way we want. For example, $A = \{1, 2, \ldots, n\}$. Any subset of A, say $B \subset A$, contains some elements form A. We can list these elements or better we can associate with every element $i \in A$ an indicator $x_i(B)$ which is set to be 1 if $i \in B$ and zero otherwise. More formally, for every subset B of A we construct an indicator $(x_1, \ldots, x_n)$ with understanding that $x_i = 1$ if and only if the ith element of A belongs to B; otherwise we set $x_i = 0$. For example, for $A = \{1, 2, 3\}$, the identifier of $\{2, 3\}$ is $(0, 1, 1)$ since 1 is *not* an element of B (i.e., $x_1 = 0$) while $2, 3 \in B$, that is, $x_2 = 1$ and $x_3 = 1$. Observe that every set of $\mathcal{P}(A)$ has a *unique* indicator $(x_1, \ldots, x_n)$. Thus counting the number of indicators will give us the desired cardinality of $\mathcal{P}(A)$. Since x_i can take only two values, and there are n possibilities the total number of indicators is $2 \cdot 2 \cdots 2 = 2^n$, which is the cardinality of $\mathcal{P}(A)$. This completes the proof.

The **Cartesian product** of two sets A and B, denoted by $A \times B$, is the set of *ordered* pairs (a, b) where $a \in A$ and $b \in B$, that is,

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

[1] This proof can be omitted in the first reading.



$A \cup B$ $A \cap B$

$A – B$ $\overline{B} = U - B$

Figure 1: Venn diagrams for the union, intersection, difference, and complementary set.

Example 4: If $A = \{1, 2\}$ and $B = \{a, b\}$, then

$$A \times B = \{(1, a), (1, b), (2, a), (2, b)\}.$$

In general, we can consider Cartesian products of three, four, or n sets. If $A_1, \dots, A_n$, then an element of $A_1 \times A_2 \times \cdots \times A_n$ is called an n-tuple.

We now introduce **set operations**. Let A and B be two sets. We define the **union** $A \cup B$, the **intersection** $A \cap B$, and the **difference** $A - B$, respectively, as follows:

$$\begin{aligned} A \cup B &= \{x : x \in A \textbf{ or } x \in B\}, \\ A \cap B &= \{x : x \in A \textbf{ and } x \in B\}, \\ A - B &= \{x : x \in A \textbf{ and } x \notin B\}. \end{aligned}$$

Example 5: Let $A = \{1, 2\}$ and $B = \{2, 5\}$, then

$$\begin{aligned} A \cup B &= \{1, 2, 5\}, \\ A \cap B &= \{2\}, \\ A - B &= \{1\}. \end{aligned}$$

We say that A and B are **disjoint** if $A \cap B = \emptyset$, that is, there is no element that belongs to both sets.

Sometimes we deal with sets that are subsets of a (master) set U. We will call such a set the **universal set** or the **universe**. One defines the complement of the set A, denoted as $\bar{A}$, as $\bar{A} = U - A$.

We can represent visually the union, intersection, difference, and complementary set using **Venn diagrams** as shown in Figure 1, which is self-explanatory.

When A and B are disjoint, the cardinality of $A \cup B$ is the sum of cardinalities of A and B, that is, $|A \cup B| = |A| + |B|$ (provided $A \cap B = \emptyset$). This identity is not true when A and B are not disjoint, since the intersection part would be counted twice!. To avoid this, we must subtract $|A \cap B|$ yielding

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

The above property is called the **principle of inclusion-exclusion**. An astute reader may want to generalize this to three and more sets. For example, consider the sets from Example 5. Note that $|A \cup B| = 3$, while $|A| = 2$, $|B| = 2$ and $|A \cap B| = 1$, thus $|A \cup B| = |A| + |B| - |A \cap B|$.

We have already observed some relationships between set operations. For example, if $A = \{1, 3, 5\}$, then $A \cup A = A$, but $A \cap \emptyset = \emptyset$. There are more to discover. We list these identities in Table 1.

Table 1: Set Identities

Identity	*Name*
$A \cup \emptyset = A$ $A \cap U = A$	Identity Laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cap A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation laws
$A \cup B = B \cap A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive laws
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan's laws

We will prove several of these identities, using different methods. We are not yet ready to use sophisticated proof techniques, but we will be able to use either Venn diagrams or the the principle expressed in (1) (i.e., to prove that two sets are equal it suffices to show that one set is a subset of the other *and* vice versa). The reader may want to use Venn's diagram to verify all the identities of Table 1.

Example 6: Let us prove one of the identities, say De Morgan's law, showing that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$ and $\overline{A \cap B} \supseteq \overline{A} \cup \overline{B}$. First suppose $x \in \overline{A \cap B}$ which implies that $x \notin A \cap B$. Hence, $x \notin A$ **or** $x \notin B$ (observe this by drawing the Venn diagram or referring to the logical de Morgan laws discussed in Module 1). Thus, $x \in \overline{A}$ or $x \in \overline{B}$ which implies $x \in \overline{A} \cup \overline{B}$. This shows that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

Suppose now that $x \in \overline{A} \cup \overline{B}$, that is, $x \in \overline{A}$ or $x \in \overline{B}$. This further implies that $x \notin A$ or $x \notin B$. Hence $x \notin A \cap B$, and therefore $x \in \overline{A \cap B}$. This proves $\overline{A \cap B} \supseteq \overline{A} \cup \overline{B}$, and completes the proof of the De Morgan law.

Exercise 2A: Using the same arguments as above prove the complementation law.

Theme 2: Relations

In Theme 1 we defined the Cartesian product of two sets A and B, denoted as $A \times B$, as the set of **ordered pairs** (a, b) such that $a \in A$ and $b \in B$. We can use this to define a (binary) relation R. We say that R is a **binary relation** from A to B if it is a subset of the Cartesian product $A \times B$. If $(a, b) \in R$, then we write aRb and say that a is related to b.

Example 7: Let $A = \{2, 3, 4\}$ and $B = \{3, 4, 5, 6, 7\}$. Define the relation R as

$$R = \{(a, b) \in A \times B : \ a \text{ divides } b\},$$

where by "divides" we mean with zero remainder. Then

$$R = \{(2, 4), (2, 6), (3, 3), (3, 6), (4, 4)\}.$$

We now define two important sets for a relation, namely, its domain and its range. The **domain** of R is defined as

$$\{x : \ x \in A \text{ and } (x, y) \in R \text{ for some } y \in B\},$$

while the **range** of R is the set

$$\{y : \ y \in B \text{ and } (x, y) \in R \text{ for some } x \in A\}.$$

In words, the domain of R is composed of all $x \in A$ for which there is y such that xRy. The set of all $y \in B$ such that there exists xRy is the range of B.

Example 8: In Example 7 the domain of R is the set $\{2, 3, 4\}$ while the range is $\{3, 4, 6\}$. Observe that domain of A is a subset of A while the range is a subset of B.

There are several important properties that are used to classify relations on sets. Let R be a relation on the set X. We say that:

- R is **reflexive** if xRx for every $x \in X$;
- R is **symmetric** if xRy implies yRx for all $x, y \in X$;
- R is **antisymmetric** if xRy and yRx implies that $x = y$;
- R is **transitive** if xRy and yRz implies xRz for all $x, y, z \in X$.

Example 9: Consider $A = \{1, 2, 3, 4\}$ and let $R = \{(1, 3), (4, 2), (2, 4), (2, 3), (3, 1)\}$. Observe that the relation R is:

- *not* reflexive since $(1, 1) \notin R$;
- *not* symmetric since for example $(2, 3) \in R$ but $(3, 2) \notin R$;

- *not* antisymmetric since $(1,3) \in R$ and $(3,1) \in R$ but $1 \neq 3$;
- *not* transitive since $(2,3) \in R$ and $(3,1) \in R$, but $(2,1) \notin R$.

On the other hand, consider this relation $S = \{(1,1),(2,2),(3,3),(4,4),(2,3),(3,1)(2,1)\}$. The relation S is reflexive, transitive, but not symmetric, however, its antisymmetric, as easy to check.

Exercise 2B: Let $X = \{1,2,3,4\}$. Is the following relation

$$R = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$$

reflexive, symmetric, antisymmetric, or transitive?

Relations are used in mathematics and in computer science to generalize and make more rigorous certain commonly acceptable notion. For example, "$=$" is a relation that defines equality between elements.

Example 10: Let $A = \mathbf{Q}$ be the set of rational numbers, that is, ratios of integers. Then $a = b$ means that $a \in \mathbf{Q}$ has the same value as $b \in \mathbf{Q}$. For example, $\frac{1}{2} = \frac{4}{8}$. The relation $=$ partitions the set of all rational numbers $\mathbf{Q}$ into subsets such every subset contains all numbers that are equal. Observe that $=$ is reflexive, symmetric and transitive. Indeed, $x = x$, $x = y$ is the same as $y = x$, and finally if $x = y$ and $y = z$, then $x = z$. Such relations are called equivalence relations and they play important role in mathematics and computer science.

A relation R that is *reflexive, symmetric*, and *transitive* is called an **equivalence relation** on the set X. As we have seen above, the relation $=$ divides (actually, *partitions*) the set of all rational numbers into *disjoint* sets that cover the the whole set of rational numbers. Let us generalize this. For an equivalence relation R we define the **equivalence set** for any $a \in X$ denoted by $[a]$ as follows

$$[a] := \{x \in X : \; xRa\}.$$

In words, $[a]$ is the set of *all* elements $x \in X$ such that x and a are related by R. This is a special set, as we formally explain below. Informally, the two *different* equivalence sets $[a]$ and $[b]$ are disjoint and the whole set X is partitioned into disjoint equivalence sets (i.e., X is the sum of disjoint equivalence sets).

More formally, observe that if aRb, then $[a] = [b]$. Indeed, let $x \in [a]$. We shall prove that $x \in [b]$, hence $[a] \subseteq [b]$. Thus xRa and from aRb and transitivity we conclude that xRb, hence $x \in [b]$, as needed. In a similar manner we can prove that $[b] \subseteq [a]$ which proves that $[a] = [b]$. Clearly if $[a] = [b]$, then aRb (by definition of $[a]$). The latter can be expressed in a different, but logically equivalent, manner: If $(a,b) \notin R$, then $[a] \neq [b]$ (this is an example of *counterpositive* argument discussed in Module 1: *Basic Logic*). We should conclude that the set X can be partitioned into disjoint subsets $[a]$ such that every element of X belongs to exactly one equivalence class $[a]$. In other words, the set

$$\mathcal{S} = \{[a] : \; a \in X\}$$

is a partition of X.

There is one important example of equivalence classes, called **congruence class**, that we must discuss.

Example 11: Fix a number n that is a *positive integer* (i.e., a natural number). Let **Z** be the set of all integers. We define a relation R_n on **Z** by xR_ny if $x - y$ is divisible by n, that is, there is an integer $k \in$ **Z** such that $x - y = kn$. We will write $x \equiv y \bmod n$ for R_n, or more often $x \bmod n = y$. Such a relation is also called **congruence modulo n**. For example, $17 \equiv 2 \bmod 5$ since $17 - 2 = 3 \cdot 5$, but $17 \not\equiv 3 \bmod 5$ since $17 - 3 = 14$ is not divisible by 5.

It is not difficult to prove that $\equiv$ is reflexive, symmetric and transitive. Indeed, $x \equiv x$ since $x - x = 0 \cdot n$. If $x \equiv y \bmod n$, then $y \equiv x \bmod n$ since $x - y = kn$ implies $y - x = (-k)n$. Finally, let $x \equiv y \bmod n$ and $y \equiv z \bmod n$. That is, $x - y = k_1 n$ and $y - z = k_2 n$. Then $x - z = (k_1 + k_2)n$, hence $x \equiv z \bmod n$.

Since $\equiv$ is an equivalence relation, we can define equivalence classes which are called *congruence classes*. From the definition we know that

$$[a] = \{a + k \cdot n : \text{ for some } k \in \mathbf{Z}\}.$$

Example 12: Congruence classes modulo 5 are

$$\begin{aligned} [0] &= \{5k : k \in \mathbf{Z}\}, \\ [1] &= \{5k + 1 : k \in \mathbf{Z}\}, \\ [2] &= \{5k + 2 : k \in \mathbf{Z}\}, \\ [3] &= \{5k + 3 : k \in \mathbf{Z}\}, \\ [4] &= \{5k + 4 : k \in \mathbf{Z}\}. \end{aligned}$$

In words, an integer belongs to one of the above classes because when dividing by 5 the remainder is either 0 or 1 or 2 or 3 or 4, but nothing more than this.

We have seen before that the relation $=$ was generalized to the equivalence relations. Let us do the same with well known $\leq$ relation. Notice that it defines an order among of real number. Let now xRy if $x \leq y$ and $x, y \in$ **R**. Clearly, this relation is reflexive and transitive because $x \leq x$ and if $x \leq y$ and $y \leq z$, then $x \leq z$. It is definitely *not* symmetric since $x \leq y$ doe snot imply $y \leq x$ unless $x = y$. Actually, it is easy to see that it is antisymmetric since if $x \leq y$ and $y \leq x$, then $x = y$. We call such relations **partial orders**. More precisely, *a relation R on a set X is partial order if R is reflexive, antisymmetric, and transitive*.

Example 13: Let xRy if x divides y (evenly) for $x, y \in$ **Z**. This relation is reflexive and transitive as we saw in Example 11. It is not symmetric (indeed, 5 divides 10 but not the other way around). Is it antisymmetric? Let x divides y and y divides x, that is, there are integers n and m such that $y = m \cdot x$

and $x = n \cdot y$. That is, $y = m \cdot n \cdot y$, hence $m \cdot n = 1$. Since $m, n \in$ **Z** we must have $m = n = 1$. Thus R is antisymmetric.

A reflexive, antisymmetric, and transitive relation R is called **partial** order (not just an order or total order) since for $x, y \in X$ it may happen that neither xRy nor yRx. In Example 13 we see that $(2, 3) \notin R$ and $(3, 2) \notin R$. If for all $x, y \in X$ we have either xRy or yRx, then R defines a total order. For example, the usual ordering of real numbers defines a total ordering, but pairs of real numbers in a plane define only a partial order.

Theme 3: Functions

Functions are one of the most important concepts in mathematics. They are also special kinds of relations. Recall that a relation R from X to Y is a subset of the Cartesian product $X \times Y$. Recall also that the domain of R is the set of $x \in X$ such that there exists y related to x through R, that is, xRy. For relations it is not important that for *every* x there is y related to x by R. Moreover, it is legitimate to have two y's, say y_1 and y_2 such that xRy_1 and xRy_2 for some x. These two properties are eliminated in the definition of a *function*. More formally, we define *a* **function** *denoted as f from X to Y as a relation from X to Y having two additional properties:*

1. The domain of f is X;

2. If xfy_1 and xfy_2, then $y_1 = y_2$.

The last item means that if there is an x such that it is related to y_1 and y_2, then y_1 *must* be equal to y_2. In other words, there is no x that has two different values of y related to it.

We shall use lowercase letters f, g, h, etc. to denote functions. Furthermore, when xfy we shall write it as $y = f(x)$. Finally, we will also use another standard notation for functions, namely:

$$f : X \to Y.$$

Functions are also called *mappings* or *transformations*.

The second property of the function definition is very important, so we characterize it in another way. Consider a relation R on X and Y. Define

$$R(x) = \{y \in Y : (x, y) \in R\}.$$

Observe that $R(x)$ is a set. It may be empty, may contain one element or many elements. When R is a function, then $R(x)$ is not empty for *every* $x \in X$ and in fact it contains *exactly* one element that is called an **image** of x. More generally, the image of X denoted as $f(X)$ for a function $f : X \to Y$ is defined as

$$f(X) = \{y \in Y : y = f(x) \text{ for some } x \in X\}.$$

In other words, $f(X)$ is a subset of Y for which there is $x \in X$ such that $f(x) \in Y$. For example in Figure 2 the image of $X = \{1, 2, 3\}$ is $\{a, b\}$.

Example 14: (a) Consider the relation $f = \{(1, a), (2, b), (3, b)\}$ from $X = \{1, 2, 3\}$ to $Y = \{a, b, c, d\}$. It is a function since every x has exactly one image in Y. In fact, $f(1) = a$, $f(2) = f(3) = b$ and $f(X) = \{a, b\} \subset Y$. Figure 2 shows a graphical representation of this function.
(b) The relation $R = \{(1, a), (2, a), (3, c)\}$ is not a function since $x = 1$ and $x = 2$ have the same image a.

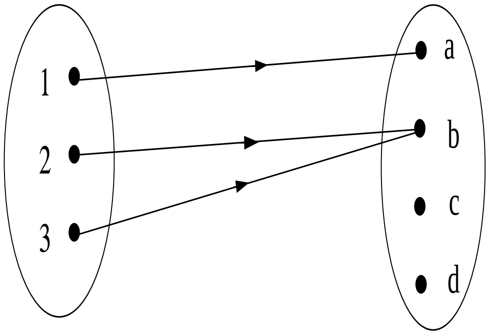
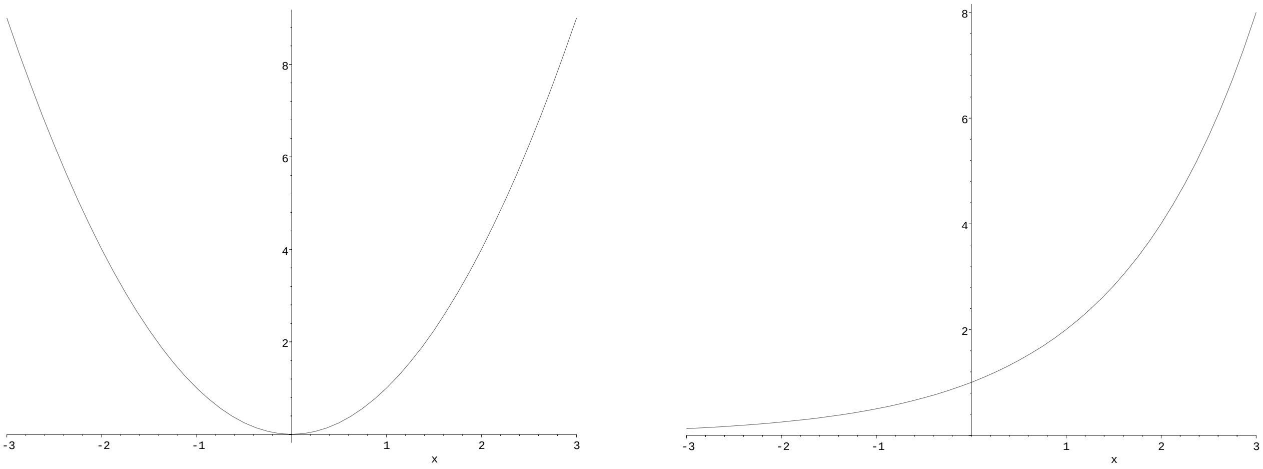


Figure 2: The function f defined in Example 14.



(a)

(b)

Figure 3: Plots of two functions: (a) $f(x) = x^2$; (b) $f(x) = 2^x$.

Functions are often represented by mathematical formulas. For example, we can write $f(x) = x^2$ for every real x, or more formally

$$x \in \mathbf{R} \rightarrow f(x) = x^2,$$

or

$$f = \{(x, x^2) : x \in \mathbf{R}\}.$$

To visualize such functions we often graph them in the (x, y) coordinates where $y = f(x)$.

Example 15: In Figure 3 we draw the functions $y = f_1(x) = x^2$ and $f_2(x) = 2^x$. Both functions are defined on the set of reals $\mathbf{R}$ which is the domain for both functions. Since $x^2 \geq 0$ and $2^x > 0$ hence the range of f_1 is the set of nonnegative reals while for f_2 it is the set of positive reals. That is, $f_1(\mathbf{R}) = \mathbf{R}^+ \cup \{0\}$ and $f_2(\mathbf{R}) = \mathbf{R}^+$.

Exercise 2C: What is the image of $f(\mathbf{R})$ for $f(x) = x^4$? What about the image of $\mathbf{R}$ over the function $f(x) = x^3$?

There are some functions occurring so often in computer science that we must briefly discuss them here. The first function, the **modulus operator**, we already studied in Example 11. We say that $x \bmod y$ is equal to the remainder when x is divided by y (we, of course, implicitly assume that $x, y \in \mathbf{Z}$, i.e., x and y are integers). We recall that $x \bmod y = n$ is equivalent to $x \equiv n \bmod y$ used before. For example, $10 \bmod 3 = 1$ and $13 \bmod 5 = 3$.

We shall write this function as

$$h(x) = y \bmod n, \qquad n \in \mathbf{N}$$

with the understanding that y is the remainder of the division x/n. The domain of such a function is the set of integers, while the image (or range) is the set of natural numbers. In fact, we can restrict the range of h to the set $\{0, 1, \ldots, n-1\}$ because the remainder of any division by n must be an integer between 0 and $n-1$.

The other important and often used functions are the **floor** and **ceiling** of a real number. Let $x \in \mathbf{R}$, then

$$\begin{aligned} \lfloor x \rfloor &= \text{the greatest } \textbf{integer} \text{ less than or equal to } x, \\ \lceil x \rceil &= \text{the least } \textbf{integer} \text{ greater than or equal to } x. \end{aligned}$$

For example,

$$\begin{aligned} \lfloor 8.99 \rfloor &= 8, & \lceil 8.99 \rceil = 9 \\ \lfloor -7.5 \rfloor &= -8 & \lceil -7.7 \rceil = -7 \\ \lfloor 10 \rfloor &= 10 & \lceil 10 \rceil = 10. \end{aligned}$$

Finally, we introduce some classes of functions as we did with relations. Consider the function $f(x) = x^2$ shown in Figure 3(a). We have $f(-2) = f(2) = 4$, that is, there are two values of x that are mapped into the same value of y (or with the same image). This is an example of a function that is *not* one-to-one or injective. We say that *a function f from X to Y is* **one-to-one** *or* **injective** *if there are $x_1, x_2 \in X$ such that if $f(x_1) = f(x_2)$, then $x_1 = x_2$*. In other words, for one-to-one function f for each $y \in Y$ there is at most one $x \in X$ with $f(x) = y$. The function in Figure 3(b) is one-to-one, as easy to see.

Example 16: Consider

$$f = \{(1, b), (2, a), (3, c)\}$$

from $X = \{1, 2, 3\}$ to $Y = \{a, b, c, d\}$. This function is injective.

How to know weather a function is one-to-ne or not? We provide some conditions below. We first introduce *increasing* and *decreasing* functions. *A function $f : X \to Y$ is* **increasing** *(***non-decreasing***) if $f(x) < f(y)$ ($f(x) \leq f(y)$) whenever $x < y$ for all $x, y \in X$*. For example, the function $f(x) = 2^x$ is increasing in the domain $\mathbf{R}$ (cf. Figure 3(b)). Similarly, *a function $f: X \to Y$ is* **decreasing** *(***non-increasing***) if $f(x) > f(y)$ ($f(x) \geq f(y)$) whenever $x < y$ for all $x, y \in X$*. For an increasing (decreasing) function the bigger the value of x is, the bigger (smaller) the value of y will be.

The function $f(x) = x^2$ plotted in Figure 3(a) is neither increasing or decreasing in the domain $\mathbf{R}$. However, it is a decreasing function for all negative reals and increasing in the set of all positive reals.

In Example 16 we have $f(X) = \{a, b, c\} \subset Y$. A function f from X to Y such that $f(X) = Y$ is said to be **onto** Y or **surjective** function.

Example 17: Let $f: \mathbf{R} \to \mathbf{R}^+ \cup \{0\}$ be such that $f(x) = x^2$, where $\mathbf{R}^+$ is the set of positive real numbers. Clearly, $f(\mathbf{R}) = \mathbf{R}^+ \cup \{0\}$, thus it is *onto* $\mathbf{R}^+ \cup \{0\}$. But if we define $f: \mathbf{R} \to \mathbf{R}$ with $f(x) = x^2$, then such a function is not surjective.

A function $f: X \to Y$ that is both injective and surjective is called a **bijection**. The function in Example 16 is a bijection while the function in Example 17 is not. For a bijection we can define an *inverse function* $f^{-1}: Y \to X$ as

$$f^{-1} = \{(y, x): (x, y) \in f\},$$

that is, x and y switch their roles. Observe that we **do not** need to have bijection in order to define the inverse since: (i) the domain of the inverse function is Y and by the definition of a function, for every y there must be x such that $x = f^{-1}(y)$; (ii) There must be *only* one x such that $x = f^{-1}(y)$ and this is guaranteed by the requirement that f is one-to-one function.

Example 18. Let $f: \mathbf{R} \to \mathbf{R}$ be such that $f(x) = x^2$. This is not a one-to-one function. Let us restrict the domain X to the set of *nonnegative* reals $X = \mathbf{R}^+ \cup \{0\}$ and we do the same with the range, that is, $Y = \mathbf{R}^+ \cup \{0\}$. Now $f(x) = x^2$ has an inverse function defined on $\mathbf{R}^+ \cup \{0\}$ which is $f^{-1}(y) = \sqrt{y}$.

Finally, we define the composition of two functions. Let

$$g: X \to Y \quad \text{and} \quad f: Y \to Z.$$

Then for every $x \in X$ we find $g(x) = y$, but for such y we compute $f(y) = f(g(x))$. The resulting function is called the **composition** of f and g and is denoted as $f \circ g$.

Example 19: Let

$$\begin{aligned} g &= \{(1, a)(2, a), (3, c)\} \\ f &= \{(a, z), (b, x), (c, y)\}. \end{aligned}$$

Then

$$f \circ g = \{(1, z), (2, z), (3, y)\}.$$

Example 20: Let $g(x) = \sin(x)$ and $f(x) = 2^x$. The composition $f \circ g = f(g(x)) = 2^{\sin(x)}$.

Theme 4: Sequences, Sums, and Products

Sequences are special functions whose domain is the set of natural numbers $\mathbf{N} = \{1, 2, \ldots\}$ or $\mathbf{N}_0 = \{0, 1, 2, \ldots\}$, that is, $f : \mathbf{N} \to \mathbf{R}$ is a **sequence**. We shall write $a_n := f(n)$ to denote an element of a sequence, where the letter a in a_n can be replaced by any other letter, say u_n or x_n. Since a sequence a_n is a set we often write it as $\{a_n\}_{n\in\mathbf{N}}$ or simply $\{a_n\}$.

Example 21: Let $a_n = 1/n^2$ for $n \in \mathbf{N}$. That is, the sequence

$$a_1, a_2, a_3, \ldots$$

starts with

$$1, \frac{1}{4}, \frac{1}{9}, \ldots$$

If $b_n = 1 + (-1)^n$, then the sequence begins with

$$0, 2, 0, 2, \ldots$$

Finally, $x_n = 2^{-n}$ looks like

$$\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots$$

We can create another sequence from a given sequence $\{a_n\}$ by selecting only some terms. For example, we can take very second term of the sequence $\{1/n\}$, that is, $1, 1/3, 1/5, \ldots$. This amounts to restricting the domain to a subset of natural numbers. If we denote this subset as $S \subset \mathbf{N}$, then we can denote such a sequence (subsequence) as $\{a_n\}_{n\in S}$. Another way of denoting a subsequence is $\{a_{n_k}\}_{k\in\mathbf{N}}$ where $\{n_k\}$ is a subsequence of natural numbers, that is, $n_k : \mathbf{N} \to S \subset \mathbf{N}$. It is usually required that $n_k < n_{k+1}$, that is, $\{n_k\}$ is an increasing sequence.

There is one important subsequence that we often use. Namely, define $S = \{m, m+1, m+2, \ldots\}$. Sometimes, we shall denote such a sequence as $\{a_n\}_{n=m}^{\infty}$.

Example 22: Let $a_n = 2^n$. The first terms are $2, 4, 8, 16, 32, \ldots$. Take every second term to produce a sequence that starts $2, 8, 32, \ldots$. We can write it as $b_n = 2^{2n}$ or as a_{2n}.

Sequences are important since they are very often used in computer science. They are frequently used in sums and products that we discuss next. Consider a (sub)sequence

$$a_m, a_{m+1}, \cdots, a_n,$$

and add all the elements to yield

$$a_m + a_{m+1} + a_{m+2} + \cdots + a_n.$$

To avoids the dots $\cdots$ we have a short hand notation for such sums, namely

$$\sum_{j=m}^{n} a_j = \sum_{k=m}^{n} a_k = \sum_{i=m}^{n} a_i.$$

In the above, we use different **indices of summation** j, k or i since they do not matter. What matters is the lower bound m and the upper bound n of the index of summation, and the sequence a_n itself.

In a similar manner we can define the *product notation*. For the above case instead of writing

$$a_m a_{m+1} \cdots a_n$$

we simply write

$$\prod_{j=m}^{n} a_j = \prod_{k=m}^{n} a_k = \prod_{i=m}^{n} a_i.$$

Example 23: Here are some examples:

$$\begin{aligned} \sum_{i=1}^{4} \frac{1}{i} &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12}, \\ \sum_{k=2}^{5} 2^k &= 2^2 + 2^3 + 2^4 + 2^5 = 60, \\ \sum_{j=1}^{4} \frac{j}{j+1} &= \frac{1}{2} + \frac{2}{3} + \frac{3}{4} + \frac{4}{5} == \frac{163}{60}. \end{aligned}$$

Exercise 2D: Find
1. $\sum_{i=1}^{3} i^2$.
2. $\prod_{k=0}^{2} 2^k$.

We have to learn how to manipulate sums and products. Observe that

$$\sum_{j=1}^{n} a_j = \sum_{k=3}^{n+2} a_{k-2} = a_1 + a_2 + \cdots + a_n.$$

In the above we change the index of summation from j to $k = j + 2$. We obtained *exactly* the same sum $a_1 + a_2 + \cdots + a_n$. In general, when we change index $j \in \{1, 2, \ldots, n\}$ to, say $k = j + m$ for some $m \in \mathbf{Z}$, we must change the lower summation index from $j = 1$ to $k = m$, the upper summation index from $j = n$ to $j = n + m$, and a_j must be replaced by a_{k-m}.

Example 24: This is the most sophisticated example in this module, however, it is important that the reader understands it. We consider a special sequence called the **geometric progression**. It is defined as follows: Fix $r > 0$ and define $a_n = r^n$ for $n = \{0, 1, 2, \ldots\}$. This sequence begins with

$$1, r, r^2, r^3, \ldots$$

Let us now consider the sum of the first $n + 1$ terms of such a sequence, that is,

$$S_n = \sum_{i=0}^{n} r^i. \tag{2}$$

Can we find a simple formula for such a sum? Consider the following chain of implications

$$\begin{aligned} S_{n+1} = S_n + r^{n+1} = \sum_{i=0}^{n+1} r^i &= 1 + \sum_{i=1}^{n+1} r^i \\ &= 1 + \sum_{j=0}^{n} r^{j+1} \\ &= 1 + r \sum_{j=0}^{n} r^j \\ &= 1 + rS_n, \end{aligned}$$

where the second line follows from the change of the index summation $i = j + 1$, in the third line we factor r in front of the sum, while in the last line we replaced $\sum_{j=0}^{n} r^j$ by S_n as defined in (2). Thus we prove that

$$S_n + r^{n+1} = 1 + rS_n,$$

from which we find S_n:

$$S_n = \frac{1 - r^{n+1}}{1 - r}$$

as long as $r \neq 1$. Therefore, the complicated sum as in (2) has a very simple closed-form solution given above. An unconvinced reader may want to verify on some numerical examples that these two formulas give the same numerical value.