Lecture Notes on Discrete Mathematics

July 30, 2019

Contents

Chapter 1

Basic Set Theory

The following notations will be followed throughout the book. 1.

The empty set, denoted ∅, is the set that has no element. 2.

N := {1, 2, . . .}, the set of Natural numbers;

3. W := {0, 1, 2, . . .}, the set of whole numbers

4. Z := {0, 1, −1, 2, −2, . . .}, the set of Integers;

5. Q := {$^{p}{}_{q}$: p, q ∈ Z, q 6= 0}, the set of Rational
numbers; 6. R := the set of Real numbers; and

7. C := the set of Complex
numbers.

This chapter will be devoted to understanding set theory, relations, functions. We start with the basic set theory.

1.1 Sets

Mathematicians over the last two centuries have been used to the idea of considering a collection of objects/numbers as a single entity. These entities are what are typically called sets. The technique of using the concept of a set to answer questions is hardly new. It has been in use since ancient times. However, the rigorous treatment of sets happened only in the 19-th century due to the German math ematician Georg Cantor. He was solely responsible in ensuring that sets had a home in mathematics. Cantor developed the concept of the set during his study of the trigonometric series, which is now known as the limit point or the derived set operator. He developed two types of transfinite numbers, namely, transfinite ordinals and transfinite cardinals. His new and path-breaking ideas were not well received by his contemporaries. Further, from his definition of a set, a number of contradictions and paradoxes arose. One of the most famous paradoxes is the Russell's Paradox, due to Bertrand Russell in 1918. This paradox amongst others, opened the stage for the development of axiomatic set theory. The interested reader may refer to Katz [8].

In this book, we will consider the intuitive or naive view point of sets. The notion of a set is taken as a primitive and so we will not try to define it explicitly. We only give an informal description of sets and then proceed to establish their properties.

A "well-defined collection" of distinct objects can be considered to be a set. Thus, the principal property of a set is that of "membership" or "belonging". Well-defined, in this context, would enable us to determine whether a particular object is a member of a set or not.

Members of the collection comprising the set are also referred to as elements of the set.

Elements of a set can be just about anything from real physical objects to abstract mathematical objects. An important feature of a set is that its elements are "distinct" or "uniquely identifiable."

A set is typically expressed by curly braces, *{ }* enclosing its elements. If A is a set and a is an element of it, we write $a \in A$. The fact that a is not an element of A is written as $a\ 6\in A$. For instance, if A is the set $\{1, 4, 9, 2\}$, then $1 \in A$, $4 \in A$, $2 \in A$ and $9 \in A$. But $7\ 6\in A$, $\pi\ 6\in A$, the English word 'four' is not in A, etc.

Example 1.1.1. 1. Let $X = \{$apple,tomato, orange$\}$. Here, orange $\in X$, but potato $6\in X$. 2. X

$= \{a_1, a_2, \ldots, a_{10}\}$. Then, $a_{100}\ 6\in X$.

3. Observe that the sets $\{1, 2, 3\}$, $\{3, 1, 2\}$ and $\{$digits in the number 12321$\}$ are the same as the order in which the elements appear doesn't matter.

We now address the idea of distinctness of elements of a set, which comes with its own

subtleties. Example 1.1.2. 1. Consider the list of digits 1, 2, 1, 4, 2. Is it a set?

2. Let $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Then X is the set of first 10 natural numbers. Or equivalently, X is the set of integers between 0 and 11.

Definition 1.1.3. The set S that contains no element is called the empty set or the null set and is denoted by *{ }* or $\varnothing$. A set that has only one element is called a singleton set.

One has three main ways for specifying a set. They are:

1. Listing all its elements (list notation), *e.g.*, $X = \{2, 4, 6, 8, 10\}$. Then X is the set of even integers between 0 and 12.

2. Stating a property with notation (predicate notation), *e.g.*,

   (a) $X = \{x : x$ is a prime number$\}$. This is read as "X is the set of all x such that x is a prime number". Here, x is a variable and stands for any object that meets the criteria after the colon.

   (b) The set $X = \{2, 4, 6, 8, 10\}$ in the predicate notation can be written as

      i. $X = \{x : 0 < x \leq 10,\ x$ is an even integer $\}$, or

      ii. $X = \{x : 1 < x < 11,\ x$ is an even integer $\}$, or

      iii. $x = \{x : 2 \leq x \leq 10,\ x$ is an even integer $\}$ etc.

   Note that the above expressions are certain rules that help in defining the elements of the set X. In general, one writes $X = \{x : p(x)\}$ or $X = \{x \mid p(x)\}$ to denote the set of all elements x (variable) such that property $p(x)$ holds. In the above, note that "colon" is sometimes replaced by "|".

3. Defining a set of rules which generate its members (recursive notation), *e.g.*,

$$\text{let } X = \{x : x \text{ is an even integer greater than } 3\}.$$

   Then, X can also be specified by

   (a) $4 \in X$,

   (b) whenever $x \in X$, then $x + 2 \in X$, and

   (c) every element of X satisfies the above two rules.

In the recursive definition of a set, the first rule is the basis of recursion, the second rule gives a method to generate new element(s) from the elements already determined and the third rule binds or restricts the defined set to the elements generated by the first two rules. The third rule should always be there. But, in practice it is left implicit. At this stage, one should make it explicit.

Definition 1.1.4. Let X and Y be two sets.

1. Suppose X is the set such that whenever $x \in X$, then $x \in Y$ as well. Here, X is said to be a subset of the set Y , and is denoted by $X \subseteq Y$. When there exists $x \in X$ such that x 6$\in$ Y , then we say that X is not a subset of Y ; and we write X 6$\subseteq$ Y .

2. If $X \subseteq Y$ and $Y \subseteq X$, then X and Y are said to be equal, and is denoted by $X = Y$. 3.

If $X \subseteq Y$ and X 6= Y , then X is called a proper subset of Y .

Thus, X is a proper subset of Y if and only if $X \subseteq Y$ and X 6= Y .

Example 1.1.5. 1. For any set X, we see that $X \subseteq X$. Thus, $\varnothing \subseteq \varnothing$. Also, $\varnothing \subseteq X$. Hence, the empty set is a subset of every set. It thus follows that there is only one empty set.

2. We know that N ⊆ W ⊆ Z ⊆ Q ⊆ R ⊆ C.

3. Note that $\varnothing$ 6$\in$ $\varnothing$.

4. Let $X = \{a, b, c\}$. Then $a \in X$ but $\{a\} \subseteq X$. Also, $\{\{a\}\}$ 6$\subseteq$ X.

5. Notice that $\{\{a\}\}$ 6$\subseteq$ $\{a\}$ and $\{a\}$ 6$\subseteq$ $\{\{a\}\}$; though $\{a\} \in \{a, \{a\}\}$ and also $\{a\} \subseteq \{a, \{a\}\}$. We

now mention some set operations that enable us in generating new sets from existing ones.

be two sets.

1.2 Operations on sets

Definition 1.2.1. *Let X and Y*

1. *The* union *of X and Y , denoted by $X \cup Y$, is the set that consists of all elements of X and also all elements of Y . More specifically, $X \cup Y = \{x|x \in X \text{ or } x \in Y\}$.*

2. *The* intersection *of X and Y , denoted by $X \cap Y$, is the set of all common elements of X and Y . More specifically, $X \cap Y = \{x|x \in X \text{ and } x \in Y\}$.*

3. *The sets X and Y are said to be* disjoint *if $X \cap Y = \varnothing$.*

Example 1.2.2. 1. Let $A = \{1, 2, 4, 18\}$ and $B = \{x : x$ is an integer, $0 < x \leq 5\}$. Then, $A \cup B$

$$= \{1, 2, 3, 4, 5, 18\} \text{ and } A \cap B = \{1, 2, 4\}.$$

2. Let $S = \{x \in \mathrm{R} : 0 \leq x \leq 1\}$ and $T = \{x \in \mathrm{R} : .5 \leq x < 7\}$. Then,

$$S \cup T = \{x \in \mathrm{R} : 0 \leq x < 7\} \text{ and } S \cap T = \{x \in \mathrm{R} : .5 \leq x \leq 1\}.$$

3. Let $X = \{\{b, c\}, \{\{b\}, \{c\}\}, b\}$ and $Y = \{a, b, c\}$. Then

$$X \cap Y = \{b\} \text{ and } X \cup Y = \{a, b, c, \{b, c\}, \{\{b\}, \{c\}\}\}.$$

We now state a few properties related to the union and intersection of sets.

Lemma 1.2.3. *Let R, S and T be sets. Then,*

1. *(a) $S \cup T = T \cup S$ and $S \cap T = T \cap S$ (union and intersection are commutative operations).*

(b) $R \cup (S \cup T) = (R \cup S) \cup T$ *and* $R \cap (S \cap T) = (R \cap S) \cap T$ *(union and intersection are associative operations).*

(c) $S \subseteq S \cup T, T \subseteq S \cup T.$

(d) $S \cap T \subseteq S, S \cap T \subseteq T.$

(e) $S \cup \varnothing = S, S \cap \varnothing = \varnothing.$

(f) $S \cup S = S \cap S = S.$

2. Distributive laws (combines union and intersection):

(a) $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$ *(union distributes over intersection).*

(b) $R \cap (S \cup T) = (R \cap S) \cup (R \cup T)$ *(intersection distributes over union).*

Proof. 2*a*. Let $x \in R \cup (S \cap T)$. Then, $x \in R$ or $x \in S \cap T$. If $x \in R$ then, $x \in R \cup S$ and $x \in R \cup T$. Thus, $x \in (R \cup S) \cap (R \cup T)$. If $x 6\in R$, then $x \in S \cap T$. So, $x \in S$ and $x \in T$. Here, $x \in R \cup S$ and $x \in R \cup T$. Thus, $x \in (R \cup S) \cap (R \cup T)$. In other words, $R \cup (S \cap T) \subseteq (R \cup S) \cap (R \cup T)$.

Now, let $y \in (R \cup S) \cap (R \cup T)$. Then, $y \in R \cup S$ and $y \in R \cup T$. Now, if $y \in R \cup S$ then either $y \in R$ or $y \in S$ or both.

If $y \in R$, then $y \in R \cup (S \cap T)$. If $y 6\in R$ then the conditions $y \in R \cup S$ and $y \in R \cup T$ imply that $y \in S$ and $y \in T$. Thus, $y \in S \cap T$ and hence $y \in R \cup (S \cap T)$. This shows that $(R \cup S) \cap (R \cup T) \subseteq R \cup (S \cap T)$, and thereby proving the first distributive law. The remaining proofs are left as exercises.

Exercise 1.2.4. *1. Complete the proof of Lemma 1.2.3.*

2. Prove the following:

(a) $S \cup (S \cap T) = S \cap (S \cup T) = S.$

(b) $S \subseteq T$ *if and only if* $S \cup T = T.$

(c) *If* $R \subseteq T$ *and* $S \subseteq T$ *then* $R \cup S \subseteq T.$

(d) *If* $R \subseteq S$ *and* $R \subseteq T$ *then* $R \subseteq S \cap T.$

(e) *If* $S \subseteq T$ *then* $R \cup S \subseteq R \cup T$ *and* $R \cap S \subseteq R \cap T.$

(f) *If* $S \cup T 6= \varnothing$ *then either* $S 6= \varnothing$ *or* $T 6= \varnothing.$

(g) *If* $S \cap T 6= \varnothing$ *then both* $S 6= \varnothing$ *and* $T 6= \varnothing.$

(h) $S = T$ *if and only if* $S \cup T = S \cap T.$

Definition 1.2.5. Let X and Y be two sets.

1. The set difference of X and Y, denoted by $X \setminus Y$, is defined by $X \setminus Y = \{x \in X : x 6\in Y\}$. 2. The set $(X \setminus Y) \cup (Y \setminus X)$, denoted by $X \Delta Y$, is called the symmetric difference of X and Y. Example 1.2.6. 1. Let $A = \{1, 2, 4, 18\}$ and $B = \{x \in Z : 0 < x \le 5\}$. Then,

$$A \setminus B = \{18\}, B \setminus A = \{3, 5\} \text{ and } A \Delta B = \{3, 5, 18\}.$$

2. Let $S = \{x \in R : 0 \le x \le 1\}$ and $T = \{x \in R : 0.5 \le x < 7\}$. Then,

$$S \setminus T = \{x \in R : 0 \le x < 0.5\} \text{ and } T \setminus S = \{x \in R : 1 < x < 7\}.$$

3. Let $X = \{\{b, c\}, \{\{b\}, \{c\}\}, b\}$ and $Y = \{a, b, c\}$. Then

$$X \setminus Y = \{\{b, c\}, \{\{b\}, \{c\}\}\},\ Y \setminus X = \{a, c\} \text{ and } X \Delta Y = \{a, c, \{b, c\}, \{\{b\}, \{c\}\}\}.$$

In naive set theory, all sets are essentially defined to be subsets of some reference set, referred to as the universal set, and is denoted by U. We now define the complement of a set.

Definition 1.2.7. Let U be the universal set and $X \subseteq U$. Then, the complement of X, denoted by X^c, is defined by $X^c = \{x \in U : x\ 6\!\in X\}$.

We state more properties of sets.

Lemma 1.2.8. *Let U be the universal set and $S, T \subseteq U$. Then,*

1. $U^c = \varnothing$ and $\varnothing^c = U$.

2. $S \cup S^c = U$ and $S \cap S^c = \varnothing$.

3. $S \cup U = U$ and $S \cap U = S$.

4. $(S^c)^c = S$.

5. $S \subseteq S^c$ if and only if $S = \varnothing$.

6. $S \subseteq T$ if and only if $T^c \subseteq S^c$.

7. $S = T^c$ if and only if $S \cap T = \varnothing$ and $S \cup T = U$.

8. $S \setminus T = S \cap T^c$ and $T \setminus S = T \cap S^c$.

9. $S \Delta T = (S \cup T) \setminus (S \cap T)$.

10. De-Morgan's Laws:

(a) $(S \cup T)^c = S^c \cap T^c$. (b)
$(S \cap T)^c = S^c \cup T^c$.

The De-Morgan's laws help us to convert arbitrary set expressions into those that involve only complements and unions or only complements and intersections.

Exercise 1.2.9. *Let S and T be subsets of a universal set U.*

1. Then prove Lemma 1.2.8.

2. Suppose that $S \Delta T = T$. Is $S = \varnothing$?

Definition 1.2.10. Let X be a set. Then, the set that contains all subsets of X is called the power set of X and is denoted by $P(X)$ or 2^X.

Example 1.2.11. 1. Let $X = \varnothing$. Then $P(\varnothing) = P(X) = \{\varnothing, X\} = \{\varnothing\}$.

2. Let $X = \{\varnothing\}$. Then $P(\{\varnothing\}) = P(X) = \{\varnothing, X\} = \{\varnothing, \{\varnothing\}\}$.

3. Let $X = \{a, b, c\}$. Then $P(X) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. 4. Let $X = \{\{b,$

$c\}, \{\{b\}, \{c\}\}\}$. Then $P(X) = \{\varnothing, \{\{b, c\}\}, \{\{\{b\}, \{c\}\}\}, \{\{b, c\}, \{\{b\}, \{c\}\}\}\ \}$.

1.3 Relations

In this section, we introduce the set theoretic concepts of relations and functions. We will use these concepts to relate different sets. This method also helps in constructing new sets from existing ones.

Definition 1.3.1. Let X and Y be two sets. Then their Cartesian product, denoted by $X \times Y$, is defined as $X \times Y = \{(a, b) : a \in X, b \in Y\}$. The elements of $X \times Y$ are also called ordered pairs with the elements of X as the first entry and elements of Y as the second entry. Thus,

$$(a_1, b_1) = (a_2, b_2) \text{ if and only if } a_1 = a_2 \text{ and } b_1 = b_2.$$

Example 1.3.2. 1. Let $X = \{a, b, c\}$ and $Y = \{1, 2, 3, 4\}$. Then

$$X \times X = \{(a, a),(a, b),(a, c),(b, a),(b, b),(b, c),(c, a),(c, b),(c, c)\}.$$

$$X \times Y = \{(a, 1),(a, 2),(a, 3),(a, 4),(b, 1),(b, 2),(b, 3),(b, 4),(c, 1),(c, 2),(c, 3),(c, 4)\}.$$

2. The Euclidean plane, denoted by $R^2 = R \times R = \{(x, y) : x, y \in R\}$.

3. By convention, $\emptyset \times Y = X \times \emptyset = \emptyset$. In fact, $X \times Y = \emptyset$ if and only if $X = \emptyset$ or $Y = \emptyset$.

Remark 1.3.3. Let X and Y be two nonempty sets. Then, $X \times Y$ can also be defined as follows: Let $x \in X$ and $y \in Y$ and think of (x, y) as the set $\{\{x\}, \{x, y\}\}$, *i.e.*, we have a new set in which an element (a set formed using the first element of the ordered pair) is a subset of the other element (a set formed with both the elements of the ordered pair). Then, with the above understanding, the ordered pair (y, x) will correspond to the set $\{\{y\}, \{x, y\}\}$. As the two sets $\{\{x\}, \{x, y\}\}$ and $\{\{y\}, \{x, y\}\}$ are not the same, the ordered pair (x, y) 6= (y, x).

Exercise 1.3.4. *Let X, Y, Z and W be nonempty sets. Then, prove the following statements:*

1. *The product construction can be used on sets several times, e.g.,*

$$X \times Y \times Z = \{(x, y, z) : x \in X, y \in Y, z \in Z\} = (X \times Y) \times Z = X \times (Y \times Z).$$

2. $X \times (Y \cup Z) = (X \times Y) \cup (X \times Z)$.
3. $X \times (Y \cap Z) = (X \times Y) \cap (X \times Z)$.
4. $(X \times Y) \cap (Z \times W) = (X \cap Z) \times (Y \cap W)$.
5. $(X \times Y) \cup (Z \times W) \subseteq (X \cup Z) \times (Y \cup W)$. *Give an example to show that the converse need not be true.*
6. *Is it possible to write the set $T = \{(x, x, y) : x, y \in N\}$ as Cartesian product of* 3 *sets? What about the the set $T = \{(x, x^2, y) : x, y \in N\}$?*

A relation can be informally thought of as a property which either holds or does not hold between two objects. For example, x is taller than y can be a relation. However, if x is taller than y, then y cannot be taller than x.

Definition 1.3.5. Let X and Y be two nonempty sets. A relation R from X to Y is a subset of $X \times Y$, *i.e.*, it is a collection of certain ordered pairs. We write xRy to mean $(x, y) \in R \subseteq X \times Y$. Thus, for any two sets X and Y, the sets $\emptyset$ and $X \times Y$ are always relations from X to Y. A relation from X to X

is called a relation on *X*.

Example 1.3.6. 1. Let *X* be any nonempty set and consider the set *P*(*X*). Define a relation *R* on *P*(*X*) by $R = \{(S, T) \in P(X) \times P(X) : S \subseteq T\}$.

2. Let $A = \{a, b, c, d\}$. Some relations *R* on *A* are:

(a) $R = A \times A$.

(b) $R = \{(a, a),(b, b),(c, c),(d, d),(a, b),(a, c),(b, c)\}$.

(c) $R = \{(a, a),(b, b),(c, c)\}$.

(d) $R = \{(a, a),(a, b),(b, a),(b, b),(c, d)\}$.

(e) $R = \{(a, a),(a, b),(b, a),(a, c),(c, a),(c, c),(b, b)\}$.

(f) $R = \{(a, b),(b, c),(a, c),(d, d)\}$.

(g) $R = \{(a, a),(b, b),(c, c),(d, d),(a, b),(b, c)\}$.

(h) $R = \{(a, a),(b, b),(c, c),(d, d),(a, b),(b, a),(b, c),(c, b)\}$.

(i) $R = \{(a, a),(b, b),(c, c),(a, b),(b, c)\}$.

Sometimes, we draw pictures to have a better understanding of different relations. For example, to draw pictures for relations on a set *X*, we first put a node for each element $x \in X$ and label it *x*. Then, for each $(x, y) \in R$, we draw a directed line from *x* to *y*. If $(x, x) \in R$ then a loop is drawn at *x*. The pictures for some of the relations is given in Figure 1.1.

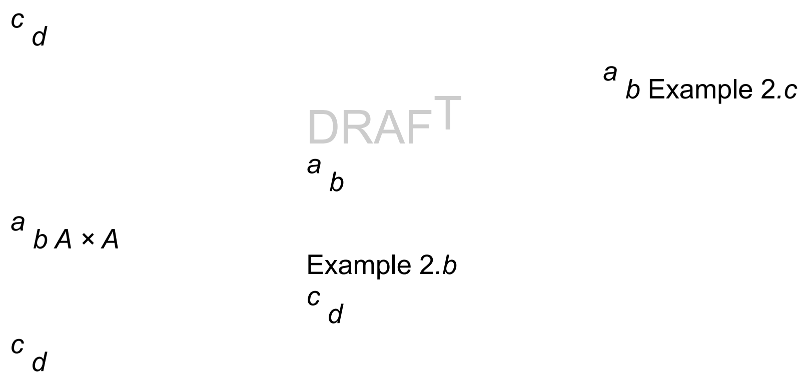

Figure 1.1: Pictorial representation of some relations from Example 2

3. Let $A = \{1, 2, 3\}$, $B = \{a, b, c\}$ and let $R = \{(1, a),(1, b),(2, c)\}$. Figure 1.2 represents the relation *R*.[1]

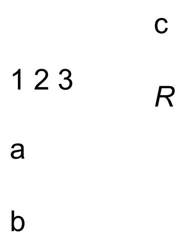

Figure 1.2: Pictorial representation of the relation in Example 3

4. Let $R = \{(x, y) : x, y \in$ Z and $y = x + 5m$ for some $m \in$ Z$\}$ is a relation on Z. If we try to draw a picture for this relation then there is no arrow between any two elements of $\{1, 2, 3, 4, 5\}$.

5. Fix $n \in$ N. Let $R = \{(x, y) : x, y \in$ Z and $y = x + nm$ for some $m \in$ Z$\}$. Then, R is a relation on Z. A picture for this relation has no arrow between any two elements of $\{1, 2, 3, . . . , n\}$.

[1] We use pictures to help our understanding and they are not parts of proof.

Definition 1.3.7. Let X and Y be two nonempty sets and let R be a relation from X to Y. Then, the inverse relation, denoted by R^{-1}, is a relation from Y to X, defined by $R^{-1} = \{(y, x) \in Y \times X : (x, y) \in R\}$. So, for all $x \in X$ and $y \in Y$

$$(x, y) \in R \text{ if and only if } (y, x) \in R^{-1}.$$

Example 1.3.8. 1. If $R = \{(1, a),(1, b),(2, c)\}$ then $R^{-1} = \{(a, 1),(b, 1),(c, 2)\}$. 2. Let $R = \{(a, b),(b, c),(a, c)\}$ be a relation on $A = \{a, b, c\}$ then $R^{-1} = \{(b, a),(c, b),(c, a)\}$ is also a relation on A.

Let R be a relation from X to Y. Consider an element $x \in X$. It is natural to ask if there exists $y \in Y$ such that $(x, y) \in R$. This gives rise to the following three possibilities: 1. (x, y) 6$\in R$ for all $y \in Y$.

2. There is a unique $y \in Y$ such that $(x, y) \in R$.

3. There exists at least two elements $y_1, y_2 \in Y$ such that $(x, y_1),(x, y_2) \in R$.

One can ask similar questions for an element $y \in Y$. To accommodate all these, we introduce a notation in the following definition.

Definition 1.3.9. Let R be a nonempty relation from X to Y. Then,

1. the set dom $R := \{x : (x, y) \in R\}$ is called the domain of R[1], and

2. the set rng $R := \{y \in Y : (x, y) \in R\}$ is called the range of R.

Notation 1.3.10. Let R be a nonempty relation from X to Y. Then,

1. for any set Z, one writes $R(Z) := \{y : (z, y) \in R$ for some $z \in Z\}$.

2. for any set W, one writes $R^{-1}(W) := \{x \in X : (x, w) \in R$ for some $w \in W\}$.

Example 1.3.11. Let a, b, c, and d be distinct symbols and let $R = \{1, a),(1, b),(2, c)\}$. Then, 1. dom $R = \{1, 2\}$, rng $R = \{a, b, c\}$,

2. $R(\{1\}) = \{a, b\}$, $R(\{2\}) = \{c\}$, $R(\{1, 2\}) = \{a, b, c\}$, $R(\{1, 2, 3\}) = \{a, b, c\}$, $R(\{4\}) = \varnothing$. 3. dom $R^{-1} = \{a, b, c\}$, rng $R^{-1} = \{1, 2\}$,

4. $R^{-1}(\{a\}) = \{1\}$, $R^{-1}(\{a, b\}) = \{1\}$, $R^{-1}(\{b, c\}) = \{1, 2\}$, $R^{-1}(\{a, d\}) = \{1\}$, $R^{-1}(\{d\}) = \varnothing$.

The following is an immediate consequence of the definition, but we give the proof of a few parts for the sake of better understanding.

Proposition 1.3.12. *Let R be a nonempty relation from X to Y, and let Z be any set. 1.* $R(Z) = R(X \cap Z) \subseteq Y$, $R^{-1}(Z) = R^{-1}(Z \cap Y) \subseteq X$.

2. dom $R = R^{-1}(Y) =$ rng $R^{-1} \subseteq X$, rng $R = R(X) =$ dom $R^{-1} \subseteq Y$.

3. *$R(Z)$ 6= ∅ if and only if* dom $R \cap Z$ 6= ∅.

4. *$R^{-1}(Z)$ 6= ∅ if and only if* rng $R \cap Z$ 6= ∅.

Proof. We prove the last two parts. The proof of the first two parts is left as an exercise. 3. Let $f(S)$ 6= ∅. There exist $a \in S \cap A$ and $b \in B$ such that $(a, b) \in f$. It implies that $a \in$ dom $f \cap S$ ($a \in S$). Converse is proved in a similar way.

4. Let rng $f \cap S$ 6= ∅. There exist $b \in$ rng $f \cap S$ and $a \in A$ such that $(a, b) \in f$. Then $a \in f^{-1}(b) \subseteq f^{-1}(S)$. Similarly, the converse follows.

[1] In some texts, the set X is referred to as the domain set of R and it should not be confused with dom R.

1.4 Functions

Definition 1.4.1. Let X and Y be nonempty sets and let f be a relation from X to Y. 1. f is called a partial function from X to Y, denoted by $f : X * Y$, if for each $x \in X$, $f(\{x\})$ is either a singleton or ∅.

2. For an element $x \in X$, if $f(\{x\}) = \{y\}$, a singleton, we write $f(x) = y$. Hence, y is referred to as the image of x under f; and x is referred to as the pre-image of y under f.

   $f(x)$ is said to be undefined at $x \in X$ if $f(\{x\}) = \varnothing$.

3. If f is a partial function from X to Y such that for each $x \in X$, $f(\{x\})$ is a singleton then f is called a function and is denoted by $f : X \to Y$.

Observe that for any partial function $f : X * Y$, the condition $(a, b),(a, b^0) \in f$ implies $b = b^0$. Thus, if $f : X * Y$, then for each $x \in X$, either $f(x)$ is undefined, or there exists a unique $y \in Y$ such that $f(x) = y$. Moreover, if $f : X \to Y$ is a function, then $f(x)$ exists for each $x \in X$, *i.e.*, there exists a unique $y \in Y$ such that $f(x) = y$.

It thus follows that a partial function $f : X * Y$ is a function if and only if dom $f = X$, *i.e.*, domain set of f is X.

Example 1.4.2. Let $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4\}$ and $X = \{3, 4, b, c\}$.

1. Consider the relation $R_1 = \{(a, 1),(b, 1),(c, 2)\}$ from A to B. The following are true. (a) R_1 is a partial function.

(b) $R_1(a) = 1$, $R_1(b) = 1$, $R_1(c) = 2$. Also, $R_1(\{d\}) = \varnothing$; thus $R_1(d)$ is undefined. (c) $R_1(X) = \{1, 2\}$.

(d) R^{-1}

$_1 = \{(1, a),(1, b),(2, c)\}$. So, R^{-1}

$_1(\{1\}) = \{a, b\}$ and R^{-1}

$_1(2) = c$. For any $x \in X$,

R^{-1}

$_1(x) = \varnothing$. Therefore, R^{-1}

$_1(x)$ is undefined.

2. $R_2 = \{(a, 1),(b, 4),(c, 2),(d, 3)\}$ is a relation from A to B. The following are true. (a) R_2 is a partial function.

   (b) $R_2(a) = 1$, $R_2(b) = 4$, $R_2(c) = 2$ and $R_2(d) = 3$.

(c) $R_2(X) = \{2, 4\}$.

(d) R^{-1}

$_2(1) = a$, R^{-1}

$_2(2) = c$, R^{-1}

$_2(3) = d$ and R^{-1}

$_2(4) = b$. Also, R^{-1}

$_2(X) = \{b, d\}$.

Convention:

Let $p(x)$ be a polynomial in the variable x with integer coefficients. Then, by writing '$f : \mathbb{Z} \to \mathbb{Z}$ is a function defined by $f(x) = p(x)$', we mean the function $f = \{(a, p(a)) : a \in \mathbb{Z}\}$. For example, the function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = x^2$corresponds to the set $\{(a, a^2) : a \in \mathbb{Z}\}$.

Example 1.4.3. 1. For $A = \{a, b, c, d\}$ and $B = \{1, 3, 5\}$, let $f = \{(a, 5),(b, 1),(d, 5)\}$ be a relation in $A \times B$. Then, f is a partial function with dom $f = \{a, b, d\}$ and rng $f = \{1, 5\}$. Further, we can define a function $g : \{a, b, d\} \to \{1, 5\}$ by $g(a) = 5$, $g(b) = 1$ and $g(d) = 5$. Also, using g, one obtains the relation $g^{-1} = \{(1, b),(5, a),(5, d)\}$.

2. The following relations $f : \mathbb{Z} \to \mathbb{Z}$ are indeed functions.

(a) $f = \{(x, 1) : x$ is even$\} \cup \{(x, 5) : x$ is odd$\}$.

(b) $f = \{(x, -1) : x \in \mathbb{Z}\}$.

(c) $f = \{(x, 1) : x < 0\} \cup \{(0, 0)\} \cup \{(x, -1) : x > 0\}$.

3. Define $f : \mathbb{Q}^+ \to \mathbb{N}$ by $f = \{(^{p}{}_{q}, 2^p3^q) : p, q \in \mathbb{N}, q\ 6{=}\ 0, p$ and q are coprime$\}$. Then, f is a function.

Remark 1.4.4. 1. If $X = \varnothing$, then by convention, one assumes that there is a function, called the empty function, from X to Y.

2. If $Y = \varnothing$ and $X\ 6{=}\ \varnothing$, then by convention, we say that there is no function from X to Y.

3. Individual relations and functions are also sets. Therefore, one can have equality between rela tions and functions, *i.e.*, they are equal if and only if they contain the same set of pairs. For exam ple, let $X = \{-1, 0, 1\}$. Then, the functions $f, g, h : X \to X$ defined by $f(x) = x$, $g(x) = x|x|$ and $h(x) = x^3$ are equal as the three functions correspond to the relation $R = \{(-1, -1),(0, 0),(1, 1)\}$ on X.

4. A function is also called a map.

5. Throughout the book, whenever the phrase 'let $f : X \to Y$ be a function' is used, it will be assumed that both X and Y are nonempty sets.

Some important functions are now defined.

Definition 1.4.5. Let X be a nonempty set.

1. The relation Id := $\{(x, x) : x \in X\}$ is called the identity relation on X.

2. The function $f : X \to X$ defined by $f(x) = x$, for all $x \in X$, is called the identity function and is denoted by Id.

3. The function $f : X \to \mathbb{R}$ with $f(x) = 0$, for all $x \in X$, is called the zero function and is denoted by 0.

Exercise 1.4.6. *1. Do the following relations represent functions? Why?*

(a) $f : \mathbb{Z} \to \mathbb{Z}$ *defined by*

i. $f = \{(x, 1) : 2$ *divides* $x\} \cup \{(x, 5) : 3$ *divides* $x\}$.

ii. $f = \{(x, 1) : x \in S\} \cup \{(x, -1) : x \in S^c\}$, *where* $S = \{n^2 : n \in \mathbb{Z}\}$ *and* $S^c = \mathbb{Z} \setminus S$. *iii.* $f = \{(x, x^3) : x \in \mathbb{Z}\}$.

(b) $f : \mathbb{R}^+ \to \mathbb{R}$ *defined by* $f = \{(x, \pm\sqrt{x}) : x \in \mathbb{R}^+\}$, *where* $\mathbb{R}^+$ *is the set of all positive real numbers.*

(c) $f : \mathbb{R} \to \mathbb{R}$ *defined by* $f = \{(x, \sqrt{x}) : x \in \mathbb{R}\}$.

(d) $f : \mathbb{R} \to \mathbb{C}$ *defined by* $f = \{(x, \sqrt{x}) : x \in \mathbb{R}\}$.

(e) $f : \mathbb{R}^- \to \mathbb{R}$ *defined by* $f = \{(x, \log_e|x|) : x \in \mathbb{R}^-\}$, *where* $\mathbb{R}^-$ *is the set of all negative real numbers.*

(f) $f : \mathbb{R} \to \mathbb{R}$ *defined by* $f = \{(x, \tan x) : x \in \mathbb{R}\}$.

2. *Let* $f : X \to Y$ *be a function. Then* f^{-1} *is a relation from* Y *to* X*. Show that the following results hold for* f^{-1}:

(a) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$ *for all* $A, B \subseteq Y$.

(b) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$ *for all* $A, B \subseteq Y$.

(c) $f^{-1}(\varnothing) = \varnothing$.

(d) $f^{-1}(Y) = X$.

(e) $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$ *for each* $B \subseteq Y$.

3. *Let* $S = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1, x \geq 0\}$. *It is a relation from* $\mathbb{R}$ *to* $\mathbb{R}$. *Draw a picture of the inverse of this relation.*

Definition 1.4.7. A function $f : X \to Y$ is said to be injective (also called one-one or an injection) if for all $x, y \in X$, $x 6= y$ implies $f(x) 6= f(y)$. Equivalently, f is one-one if for all $x, y \in X$, $f(x) = f(y)$ implies $x = y$.

Example 1.4.8. 1. Let X be a nonempty set. Then, the identity map Id on X is one-one. 2. Let X be a nonempty proper subset of Y . Then $f(x) = x$ is a one-one map from X to Y . 3. The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not one-one as $f(-1) = f(1) = 1$.

4. The function $f : \{1, 2, 3\} \to \{a, b, c, d\}$ defined by $f(1) = c$, $f(2) = b$ and $f(3) = a$, is one-one. It can be checked that there are 24 one-one functions $f : \{1, 2, 3\} \to \{a, b, c, d\}$.

5. There is no one-one function from the set $\{1, 2, 3\}$ to its proper subset $\{1, 2\}$.

6. There are one-one functions from the set $\mathbb{N}$ of natural numbers to its proper subset $\{2, 3, \ldots\}$. One of them is given by $f(1) = 4$, $f(2) = 3$, $f(3) = 2$ and $f(n) = n + 1$, for all $n \geq 4$.

Definition 1.4.9. Let $f : X \to Y$ be a function. Let $A \subseteq X$ and $A 6= \varnothing$. The restriction of f to A, denoted by f_A, is the function $f_A = \{(x, y) : (x, y) \in f, x \in A\}$.

Example 1.4.10. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 0$ if x is rational, and $f(x) = 1$ if x is irrational. Then, $f_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R}$ is the zero function.

Proposition 1.4.11. *Let* $f : X \to Y$ *be a one-one function and let* Z *be a nonempty subset of* X*. Then* f_Z *is also one-one.*

Proof. Suppose $f_Z(x) = f_Z(y)$ for some $x, y \in Z$. Then $f(x) = f(y)$. As f is one-one, $x = y$. Thus, f_Z is one-one.

Definition 1.4.12. A function $f : X \to Y$ is said to be surjective (also called onto or a surjection) if $f^{-1}(\{b\})$ 6= ∅ for each $b \in Y$. Equivalently, $f : X \to Y$ is onto if there exists a pre-image under f, for each $b \in Y$.

Example 1.4.13. 1. Let X be a nonempty set. Then the identity map on X is onto. 2. Let X be a

nonempty proper subset of Y . Then the identity map $f : X \to Y$ is not onto.

3. There are 6 onto functions from $\{a, b, c\}$ to $\{a, b\}$. For example, $f(a) = a$, $f(b) = b$, and $f(c) = b$ is one such function.

4. Let X be a nonempty subset of Y . Fix an element $a \in X$. Define $g : Y \to X$ by (
y, if $y \in X$,
a, if $y \in Y \setminus X$. $g(y) =$

Then g is an onto function.

5. There does not exist any onto function from the set $\{a, b\}$ to its proper superset $\{a, b, c\}$.

6. There exist onto functions from the set $\{2, 3, \ldots\}$ to its proper superset N. An example of such a function is $f(n) = n - 1$ for all $n \geq 2$.

Definition 1.4.14. Let X and Y be sets. A function $f : X \to Y$ is said to be bijective (also call a bijection) if f is both one-one and onto. The set X is said to be equinumerous[1] with the set Y if there exists a bijection $f : X \to Y$.

[1] If X is equinumerous with Y then X is also said to be *equivalent* to Y .

Clearly, if a set X is equinumerous with a set Y then Y is also equinumerous with X. Hence, X and Y are said to be equinumerous sets.

Example 1.4.15. 1. The function $f : \{1, 2, 3\} \to \{a, b, c\}$ defined by $f(1) = c$, $f(2) = b$ and $f(3) = a$, is a bijection. Thus, $f^{-1}: \{a, b, c\} \to \{1, 2, 3\}$ is a bijection; and the set $\{a, b, c\}$ is equinumerous with $\{1, 2, 3\}$.

2. Let X be a nonempty set. Then the identity map on X is a bijection. Thus, the set X is equinumerous with itself.

3. The set N is equinumerous with $\{2, 3, \ldots\}$. Indeed the function f : N → $\{2, 3, \ldots\}$ defined by $f(1) = 3$, $f(2) = 2$ and $f(n) = n + 1$, for all $n \geq 3$ is a bijection.

Exercise 1.4.16. *1. Let $f : X \to Y$ be a bijection. Then, for every choice of pairs x, y with $x \in X$ and $y \in Y$ there exists a bijection, say $h : X \to Y$, such that $h(x) = y$.*

2. Define f : W → Z by $f = \{x, \frac{-x}{2}$: x is even} ∪ : x is odd}. Is f one-one? Is it onto?
$\{x, \frac{x+1}{2}$

3. Define f : N → Z by $f = \{(x, 2x) : x \in$ N}, and g : Z → Z by $g = \{x, \frac{x}{2}$: x is even} ∪ {(x, 0) : x is odd}. Are f and g one-one? Are they onto?

4. Let X be a nonempty set. Give a one-one function from X to $P(P(P(X)))$.

5. *For a fixed $n \in$ N, let A_n and B_n be nonempty sets and let R_n be a one-one relation from A_n to B_n. Then, $\cap_n R_n$ is a one-one relation.*
6. *Let A be the set of subsets of {1, 2, . . . , 9} each having 5 elements and let B be the set of 5 digit numbers with strictly increasing digits. For $a \in A$, define $f(a)$ as the number obtained by arranging the elements of a in increasing order. Is f one-one and onto?*

1.5 Composition of functions

Definition 1.5.1. Let f and g be two relations such that rng $f \subseteq$ dom g. Then, the composition of f and g, denoted by $g \circ f$, is defined as

$$g \circ f = \{(x, z) : (x, y) \in f \text{ and } (y, z) \in g \text{ for some } y \in \text{rng } f \subseteq \text{dom } g\} .$$

Notice that the composition of two relations in the above definition is a relation. In case, both f and g are functions, $g \circ f$ is also a function, and $(g \circ f)(x) = g(f(x))$ as $(x, z) \in g \circ f$ implies that there exists y such that $y = f(x)$ and $z = g(y)$. Similarly, one defines $f \circ g$ if rng $g \subseteq$ dom f.

Example 1.5.2. Let $f = \{(\beta, a),(3, b),(3, c)\}$ and $g = \{(a, 3),(b, \beta),(c, \beta)\}$. Then, $g \circ f = \{(3, \beta),(\beta, 3)\}$ and $f \circ g = \{(a, b),(a, c),(b, a),(c, a)\}$.

The proof of the next result is omitted as it directly follows from definition.

Proposition 1.5.3. [Algebra of composition of functions] *Let $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ be functions.*

1. *Then, $(h \circ g) \circ f : Z \to W$ and $h \circ (g \circ f) : X \to W$ are functions. Moreover, $(h \circ g) \circ f = h \circ (g \circ f)$ (associativity holds).*
2. *If f and g are injections then $g \circ f : X \to Z$ is an injection.*
3. *If f and g are surjections then $g \circ f : X \to Z$ is a surjection.*
4. *If f and g are bijections then $g \circ f : X \to Z$ is a bijection.*

5. [Extension] *If* dom $f \cap$ dom $h = \varnothing$ *and* rng $f \cap$ rng $h = \varnothing$ *then the function $f \cup h$ from $X \cup Z$ to $Y \cup W$ defined by $f \cup h = \{(a, f(a)) : a \in X\} \cup \{(c, h(c)) : c \in Z\}$ is a bijection.*
6. *Let X and Y be sets with at least two elements each and let $f : X \to Y$ be a bijection. Then the number of bijections from X to Y is at least* 2.

Theorem 1.5.4. [Properties of the identity function] *Let X and Y be two nonempty sets and* Id *be the identity function on X. Then, for any two functions $f : X \to Y$ and $g : Y \to X$,*

$$f \circ \text{Id} = f \text{ and } \text{Id} \circ g = g.$$

Proof. By definition, $(f \circ \text{Id})(x) = f(\text{Id}(x)) = f(x)$, for all $x \in X$. Hence, $f \circ \text{Id} = f$. Similarly, the other equality follows.

We now give a very important bijection principle.

Theorem 1.5.5. [Bijection principle] *Let $f : X \to Y$ and $g : Y \to X$ be functions such that $(g \circ f)(x) = x$ for each $x \in X$. Then f is one-one and g is onto.*

Proof. To show that f is one-one, suppose $f(a) = f(b)$ for some $a, b \in X$. Then

$$a = (g \circ f)(a) = g\,(f(a)) = g\,(f(b)) = (g \circ f)(b) = b.$$

Thus, f is one-one.

To show that g is onto, let $a \in X$. Write $b = f(a)$. Now, $a = (g \circ f)(a) = g(f(a)) = g(b)$. That is, we have found $b \in Y$ such that $g(b) = a$. Hence, g is onto.

Exercise 1.5.6. *1. Let f, g :* W → W *be defined by* $f = \{(x, 2x) : x \in \mathrm{W}\}$ *and* $g = \{x, \frac{x}{2} : x$ *is even*$\} \cup \{(x, 0) : x$ *is odd*$\}$*. Verify that* $g \circ f$ *is the identity function on* W*, whereas* $f \circ g$ *maps even numbers to even numbers and odd numbers to* 0*.*

2. Let $f : X \to Y$ *be a function. Prove that* $f^{-1}: Y \to X$ *is a function if and only if f is a bijection.*

3. Define $f : \mathrm{N} \times \mathrm{N} \to \mathrm{N}$ *by* $f(m, n) = 2^{m-1}(2n - 1)$*. Is f a bijection?*

4. Let $f : X \to Y$ *be a bijection and let* $A \subseteq X$*. Is* $f(X \setminus A) = Y \setminus f(A)$*?*

5. Let $f : X \to Y$ *and* $g : Y \to X$ *be two functions such that*

(a) $(f \circ g)(y) = y$ *for each* $y \in Y$*,*

(b) $(g \circ f)(x) = x$ *for each* $x \in X$*.*

Show that f is a bijection and $g = f^{-1}$*. Can we conclude the same without assuming the second condition?*

1.6 Equivalence relation

We look at some relations that are of interest in mathematics.

Definition 1.6.1. Let A be a nonempty set. Then, a relation R on A is said to be 1.
reflexive if for each $a \in A$, $(a, a) \in R$.

2. symmetric if for each pair of elements $a, b \in A$, $(a, b) \in R$ implies $(b, a) \in R$. 3.
transitive if for each triple of elements $a, b, c \in A$, $(a, b),(b, c) \in R$ imply $(a, c) \in R$.

Exercise 1.6.2. *For relations defined in Example 1.3.6, determine which of them are*

1. reflexive.

2. symmetric.

3. transitive.

Definition 1.6.3. Let A be a nonempty set. A relation on A is called an equivalence relation if it is reflexive, symmetric and transitive. It is customary to write a supposed equivalence relation as ~ rather than R. The equivalence class of the equivalence relation ~ containing an element $a \in A$ is denoted by $[a]$, and is defined as $[a] := \{x \in A : x \sim a\}$.

Example 1.6.4. 1. Consider the relations on A of Example 1.3.6.

(a) The relation in Example 1.3.6.1 is not an equivalence relation; it is not symmetric. (b) The relation in Example 1.3.6.2a is an equivalence relation with $[a] = \{a, b, c, d\}$ as the only equivalence class.

(c) Other relations in Example 1.3.6.2 are not equivalence relations.

(d) The relation in Example 1.3.6.4 is an equivalence relation with the equivalence classes as i. $[0] = \{\ldots, -15, -10, -5, 0, 5, 10, \ldots\}$.

ii. $[1] = \{\ldots, -14, -9, -4, 1, 6, 11, \ldots\}$.

iii. $[2] = \{\ldots, -13, -8, -3, 2, 7, 12, \ldots\}$.

iv. $[3] = \{\ldots, -12, -7, -2, 3, 8, 13, \ldots\}$.

v. $[4] = \{\ldots, -11, -6, -1, 4, 9, 14, \ldots\}$.

(e) The relation in Example 1.3.6.5 is an equivalence relation with the equivalence classes as

$[0] = \{\ldots, -3n, -2n, -n, 0, n, 2n, \ldots\}$.

$[1] = \{\ldots, -3n + 1, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \ldots\}$.

$[2] = \{\ldots, -3n + 2, -2n + 2, -n + 2, 2, n + 2, 2n + 2, \ldots\}$.

$\vdots$

$[n - 2] = \{\ldots, -2n - 2, -n - 2, -2, n - 2, 2n - 2, 3n - 2, \ldots\}$.

$[n - 1] = \{\ldots, -2n - 1, -n - 1, -1, n - 1, 2n - 1, 3n - 1, \ldots\}$.

2. Consider the relation $R = \{(a, a),(b, b),(c, c)\}$ on the set $A = \{a, b, c\}$. Then R is an equivalence relation with three equivalence classes, namely $[a] = \{a\}$, $[b] = \{b\}$ and $[c] = \{c\}$.

3. The relation $R = \{(a, a),(b, b),(c, c),(a, c),(c, a)\}$ is an equivalence relation on $A = \{a, b, c\}$. It has two equivalence classes, namely $[a] = [c] = \{a, c\}$ and $[b] = \{b\}$.

Proposition 1.6.5. [Equivalence relation divides a set into disjoint classes] *Let $\sim$ be an equivalence relation on a nonempty set X. Then,*

1. any two equivalence classes are either disjoint or identical ;

2. the set X is equal to the union of all equivalence classes of $\sim$.

That is, an equivalence relation $\sim$ on X divides X into disjoint equivalence classes.

Proof. 1. Let $a, b \in X$ be distinct elements of X. If the equivalence classes $[a]$ and $[b]$ are disjoint, then there is nothing to prove. So, assume that there exists $c \in X$ such that $c \in [a] \cap [b]$. That is, $c \sim a$ and $c \sim b$. By symmetry of $\sim$ it follows that $a \sim c$ and $b \sim c$. We will show that $[a] = [b]$.

For this, let $x \in [a]$. Then $x \sim a$. Since $a \sim c$ and $\sim$ is transitive, we have $x \sim c$. Again, $c \sim b$ and transitivity of $\sim$ imply that $x \sim b$. Thus, $x \in [b]$. That is, $[a] \subseteq [b]$. A similar argument proves that $[b] \subseteq [a]$. Thus, whenever two equivalence classes intersect, they are indeed equal.

2. Notice that for each $x \in X$, the equivalence class $[x]$ is well defined, $x \in [x]$ and $[x] \subseteq X$. Thus, if we take the union of the equivalence classes over all $x \in X$, we get $X = \bigcup_{x\in X} [x]$.

Exercise 1.6.6. *Determine the equivalence relation among the relations given below. Further, for each equivalence relation, determine its equivalence classes.*

1. $R = \{(a, b) \in \mathbb{Z}^2 : a \le b\}$ *on* $\mathbb{Z}$.

2. $R = \{(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^* : a \text{ divides } b\}$ *on* $\mathbb{Z}^*$, *where* $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

3. Recall the greatest integer function $f : \mathbb{R} \to \mathbb{Z}$ *given by* $f(x) = [x]$ *and let* $R = \{(a, b) \in \mathbb{R} \times \mathbb{R} :$

$[a] = [b]\}$ *on* R.

4. *For* $\mathrm{x} = (x_1, x_2)$, $\mathrm{y} = (y_1, y_2) \in \mathrm{R}^2$ *and* $\mathrm{R}^* = \mathrm{R} \setminus \{0\}$, *let*

   (a) $R = \{(\mathrm{x}, \mathrm{y}) \in \mathrm{R}^2 \times \mathrm{R}^2 \colon x^2{}_1 + x^2{}_2 = y^2{}_1 + y^2{}_2\}$.

   (b) $R = \{(\mathrm{x}, \mathrm{y}) \in \mathrm{R}^2 \times \mathrm{R}^2 \colon \mathrm{x} = \alpha\mathrm{y}$ *for some* $\alpha \in \mathrm{R}^*\}$.

   (c) $R = \{(\mathrm{x}, \mathrm{y}) \in \mathrm{R}^2 \times \mathrm{R}^2 \colon 4x^2{}_1 + 9x^2{}_2 = 4y^2{}_1 + 9y^2{}_2\}$.

   (d) $R = \{(\mathrm{x}, \mathrm{y}) \in \mathrm{R}^2 \times \mathrm{R}^2 \colon \mathrm{x} - \mathrm{y} = \alpha(1, 1)$ *for some* $\alpha \in \mathrm{R}^*\}$.

   (e) *Fix* $c \in \mathrm{R}$. *Now, define* $R = \{(\mathrm{x}, \mathrm{y}) \in \mathrm{R}^2 \times \mathrm{R}^2 \colon y_2 - x_2 = c(y_1 - x_1)\}$.

   (f) $R = \{(\mathrm{x}, \mathrm{y}) \in \mathrm{R}^2 \times \mathrm{R}^2 \colon |x_1| + |x_2| = \alpha(|y_1| + |y_2|)\}$, *for some number* $\alpha \in \mathrm{R}^+$. (g)
   $R = \{(\mathrm{x}, \mathrm{y}) \in \mathrm{R}^2 \times \mathrm{R}^2 \colon x_1x_2 = y_1y_2\}$.

5. *For* $\mathrm{x} = (x_1, x_2)$, $\mathrm{y} = (y_1, y_2) \in \mathrm{R}^2$, *let* $S = \{\mathrm{x} \in \mathrm{R}^2 \colon x^2{}_1 + x^2{}_2 = 1\}$. *Then, are the relations given below an equivalence relation on S?*

   (a) $R = \{(\mathrm{x}, \mathrm{y}) \in S \times S : x_1 = y_1, x_2 = -y_2\}$.

   (b) $R = \{(\mathrm{x}, \mathrm{y}) \in S \times S : \mathrm{x} = -\mathrm{y}\}$.

Definition 1.6.7. Let X be a nonempty set. Then a partition of X is a collection of disjoint, nonempty subsets of X whose union is X.

Example 1.6.8. Let $X = \{a, b, c, d, e\}$.

1. Then $\{\{a, b\}, \{c, e\}, \{d\}\}$ is a partition of X.

   Consider the relation $R = \{(a, a),(b, b),(c, c),(d, d),(e, e),(a, b),(b, a),(c, e),(e, c)\}$ on X. The equivalence classes of R are $[a] = [b] = \{a, b\}$, $[c] = [e] = \{c, e\}$ and $[d] = \{d\}$, which constitute the said partition of X.

2. Consider the partition $\{\{a\}, \{b, c, d\}, \{e\}\}$ of X. Verify that the relation $R = \{(a, a),(b,$

   $$b),(c, c),(d, d),(e, e),(b, c),(c, d),(b, d),(c, b),(d, c),(d, b)\}$$

   is an equivalence relation on X with equivalence classes $[a] = \{a\}$, $[b] = \{b, c, d\}$ and $[e] = \{e\}$.

Given a partition of a nonempty set X, does there exists an equivalence relation on X such that the disjoint equivalence classes are exactly the elements of the partition? Recall that the elements of a partition are subsets of the given set.

Proposition 1.6.9. [Constructing equivalence relation from equivalence classes] *Let P be a par tition of a nonempty set X. Let ~ be the relation on X defined by*

> *for each pair of elements* $x, y \in X$, $x \sim y$ *if and only if both x and y are elements of the same subset A in P.*

Then the set of equivalence classes of ~ is equal to P.

Proof. The construction of ~ says that if A and B are two distinct elements of P, then all elements of A are related to each other by ~, all elements of B are related to each other by ~, but no element of A is related to any element of B by ~.

Let $x \in X$. Since P is a partition, $x \in A$ for some $A \in P$. Then $x \sim x$. So, ~ is reflexive. Let $x, y \in X$ such that $x \sim y$. Then, there exists $A \in P$ such that $x, y \in A$. So, $y \sim x$. Hence ~ is symmetric.

Let $x, y, z \in X$ such that $x \sim y$ and $y \sim z$. Then there exists $A \in P$ such that $x, y \in A$ and $y, z \in$

A. It follows that $x \sim z$. That is, $\sim$ is transitive.

To complete the proof, we show that

1. Each equivalence class of $\sim$ is an element of P.
2. each element of P is an equivalence class of $\sim$.

1. Let $[x]$ be an equivalence class of $\sim$ for some $x \in X$. This x is in some $A \in P$. Now, $y \in [x] \Leftrightarrow x \sim y \Leftrightarrow y \in A$. Then $[x] = A$.
2. Similarly, let $B \in P$. Take $x \in B$. Now $y \in B \Leftrightarrow y \sim x \Leftrightarrow y \in [x]$. Then $[x] = B$.

Exercise 1.6.10. *1. Let X and Y be two nonempty sets and f be a relation from X to Y . Let* Id_X *and* Id_Y *be the identity relations on X and Y , respectively. Then,*

(a) is it necessary that $f^{-1} \circ f \subseteq \mathrm{Id}_X$?

(b) is it necessary that $f^{-1} \circ f \supseteq \mathrm{Id}_X$?

(c) is it necessary that $f \circ f^{-1} \subseteq \mathrm{Id}_Y$?

(d) is it necessary that $f \circ f^{-1} \supseteq \mathrm{Id}_Y$?

2. In addition to the data in (1), suppose f is a function. Then,

(a) is it necessary that $f \circ f^{-1} \subseteq \mathrm{Id}_Y$?

(b) is it necessary that $\mathrm{Id}_X \subseteq f^{-1} \circ f$*?*

3. Take X 6= ∅. Is $X \times X$ an equivalence relation on X? If yes, what are the equivalence classes?

4. On a nonempty set X, what is the smallest equivalence relation (in the sense that every other equivalence relation will contain this equivalence relation; recall that a relation is a set)?

5. Supply the equivalence relation on R *whose equivalence classes are $\{[m, m + 1) : m \in$ Z$\}$.*

6. A relation on a nonempty set may or may not be reflexive, symmetric, or transitive. Thus there are 8 types of relations. With $X = \{1, 2, 3, 4, 5\}$, give one example for each type of such relations.

7. What is the number of all relations on $\{1, 2, 3\}$?

8. What is the number of relations f from $\{1, 2, 3\}$ to $\{a, b, c\}$ such that $\mathrm{dom}\, f = \{1, 3\}$*? 9. What is the number of relations f on $\{1, 2, 3\}$ such that $f = f^{-1}$?*

10. What is the number of partial functions on $\{1, 2, 3\}$? How many of them are functions?

11. What is the number of functions from $\{1, 2, 3\}$ to $\{a_1, a_2, \ldots, a_n\}$?

12. What is the number of equivalence relations on $\{1, 2, 3, 4, 5\}$?

13. Let f, g be two non-equivalence relations on R*. Then, is it possible to have $f \circ g$ as an equivalence relation? Give reasons for your answer.*

14. Let f, g be two equivalence relations on R*. Then, prove/disprove the following statements. (a) $f \circ g$ is necessarily an equivalence relation.*

(b) $f \cap g$ is necessarily an equivalence relation.

(c) $f \cup g$ is necessarily an equivalence relation.

(d) $f \cup g^{c}$*is necessarily an equivalence relation.* ($g^{c} = (R \times R) \setminus g$)

Chapter 2

The Natural Number System

Proofs are to mathematics what spelling is to poetry. Mathematical works do consist of proofs, just as poems do consist of words - V. Arnold.

2.1 Peano Axioms

In this section, the set of natural numbers is defined axiomatically. These axioms are credited to the Italian mathematician G. Peano and the German mathematician J. W. R. Dedekind. The goal in these axioms is to first establish the existence of one natural number and then define a function, called the successor function, to generate the remaining natural numbers. Each of these axioms, listed P1 to P3 below, is crucial to the properties that the set of natural numbers enjoy.

P1. $1 \in$ N, *i.e.*, 1 is a natural number.

P1 guarantees the existence of one natural number. We now generate more natural numbers using the successor function. So, we assume the existence of a successor function S defined on N. The existence of the successor function is a property unique to the set of natural numbers.

P2. There exists an injective function S : N → N \ $\{1\}$.

Here, for each $x \in$ N, $S(x)$ is called the successor of x.

Axiom P2 implies that 1 is not the successor of any natural number. As $S(1)$ 6= 1, denote $S(1)$ by 2. Now $S(S(1))$, which is $S(2)$, is different from both 1 and 2. Denote $S(2)$ by 3. By a similar argument, denote $S(3)$ to be 4, $S(4)$ to be 5, etc. From this argument each of the elements of the set $\{1, 2, 3, \ldots\}$ is also an element of N. Thus, the axiomatic/formal definition of N includes all the usual elements, *i.e.*, $1, 2, 3, \ldots$.

Further, to exclude versions of N that are 'too large', the last axiom, called the Axiom of Induction is stated next.

P3. [Axiom of Induction] Let $X \subseteq$ N be such that

1. $1 \in X$, and
2. for each $x \in X$, $S(x) \in X$.

Then $X =$ N.

Axioms P1 and P2 ensure that $\{1, 2, \ldots\} \subseteq$ N. Further, as $1 \in \{1, 2, \ldots\}$ and for each $n \in \{1, 2, \ldots\}$, $S(n) \in \{1, 2, \ldots, \}$, Axiom P3 ensures that that N = $\{1, 2, \ldots\}$.

The next result ensures that any natural number different from 1 has to be a successor of some other natural number. This, in effect, re-emphasizes the Axioms P2 and P3.

Lemma 2.1.1. *If $n \in$ N and n 6= 1, then there exists $m \in$ N such that $S(m) = n$.*

Proof. Let X = {$x \in$ N : x = 1 or $\exists$ $y \in$ N such that $x = S(y)$}. By the definition of X, both 1 and $S(1)$ belong to X, *i.e.*, $X \setminus \{1\}$ 6= ∅.

So, for any $x \in X \setminus \{1\}$, there must exist $y \in$ N such that $x = S(y)$. Observe that $S(y) \in$ N. Therefore, $S(x) = S(S(y))$ implies that $S(x) \in X$. Thus, by the induction axiom, P3 X = N.

The existence of the set of natural numbers has been established axiomatically. So, we now discuss the arithmetic on N, an important property of the set of natural numbers. The arithmetic in N that touches every aspect of our lives is clearly addition and multiplication. So, depending solely on the Peano axioms, we define the operation of addition on N. 1 is always a natural number by Axiom P1. First, we establish what it means to add 1 to a natural number n. Here, we define $n + 1 = S(n)$.

We now wish to add any two natural numbers n and m. Without loss of generality assume that m 6= 1. From Lemma 2.1.1, there exists $k \in$ N such that $m = S(k)$. So, to define $n + m$, it is sufficient to define $n + S(k)$. We do this by using the following recursive definition: $n + S(k) = S(n + k)$.

For example, suppose we wish to compute 1 + 2. By the paragraph after Axiom P2, 2 = $S(1)$. So, 1 + 2 = 1 + $S(1)$. By the above definition, 1 + $S(1) = S(1 + 1)$ and 1 + 1 = $S(1)$, which is 2 by the paragraph after Axiom P2. Thus, 1 + $S(1) = S(1 + 1) = S(2)$ = 3. An iteration of this process will generate the usual addition on N. In short, the definition for addition is:

Definition 2.1.2. We define addition as follows.

1. For each $n \in$ N, $n + 1 := S(n)$, and

2. for each $m, n \in$ N, $n + S(m) := S(n + m)$.

Using a similar argument, axiomatic multiplication "." can be defined. First, set $n \cdot 1$ to be n. The multiplication of arbitrary natural numbers is now defined in a recursive manner. The formal definition is:

Definition 2.1.3. The multiplication of two natural numbers is defined as follows. 1.

For all $n \in$ N, $n \cdot 1 := n$, and

2. for all $m, n \in$ N, $n \cdot S(m) := (n \cdot m) + n$.

We follow the usual convention of writing $(n \cdot m) + k$ as $n \cdot m + k$.

Using the above axiomatic definitions of both addition and multiplication, we derive the properties of the set of natural numbers N.

1. [Associativity of addition] For every $n, m, k \in$ N, $n + (m + k) = (n + m) + k$. *Proof.* Let X = {$k \in$ N : for all $m, n \in$ N, $n + (m + k) = (n + m) + k$}. We show that X = N.

   Let $n, m \in$ N. As

$$\begin{aligned} n + (m + 1) &= n + S(m) \text{ (Definition 2.1.2.1)} \\ &= S(n + m) \text{ (Definition 2.1.2.2)} \\ &= (n + m) + 1, \text{ (Definition 2.1.2.1)} \end{aligned}$$

   we get 1 $\in X$. Now, let $z \in X$ and let us show that $S(z) \in X$. As $z \in X$, by definition of X n +

$(m + z) = (n + m) + z$, for all $n, m \in$ N. (2.1)

Therefore, using the definition of X and Equation (2.1), we see that

$n+(m+S(z)) = n+S(m+z) = S(n+(m+z)) = S((n+m)+z) = (n+m)+S(z)$ for all $n, m \in$ N. Hence,

$S(z) \in X$ and thus by the induction axiom, Axiom P3, $X =$ N.

2. [Commutativity of addition] For every $x, y \in$ N, $x + y = y + x$.

Proof. Let $X = \{k \in$ N : for all $n \in$ N, $n + k = k + n\}$. We show that $X =$ N.

To show $1 \in X$, we define the set Y to be $Y = \{n \in$ N : $n + 1 = 1 + n$, for all $n \in$ N$\}$ and prove that $Y =$ N.

Firstly, $1 + 1 = 1 + 1$ and hence $1 \in Y$. Now, let $y \in Y$. To show $S(y) \in Y$. But, $y \in Y$ implies that $1 + y = y + 1$ and hence

$$1 + S(y) = S(1 + y) = S(y + 1) = S(S(y)) = S(y) + 1.$$

Thus, $S(y) \in Y$ and hence by Axiom P3, $Y =$ N. Therefore, we conclude that $1 \in X$.

Now, let $z \in X$. To show $S(z) \in X$. But, $z \in X$ implies that $n + z = z + n$, for all $n \in$ N. Thus, using $1 \in X$, $n + z = z + n$, for all $n \in$ N and associativity, one has

$n + S(z) = n + (z + 1) = (n + z) + 1 = (z + n) + 1 = 1 + (z + n) = (1 + z) + n = S(z) + n$, for all

$n \in$ N. Hence, $S(z) \in X$ and thus by Axiom P3, $X =$ N.

3. [Distributive law] For every $n, m, k \in$ N, $n \cdot (m + k) = n \cdot m + n \cdot k$.

Proof. Let $X = \{k \in$ N : for all $m, n \in$ N, $n \cdot (m + k) = n \cdot m + n \cdot k\}$. We show that $X =$ N. $1 \in X$ as for each $n, m \in$ N,

$$n \cdot (m + 1) = n \cdot S(m) = n \cdot m + n = n \cdot m + n \cdot 1.$$

Now, let $z \in X$ and let us show that $S(z) \in X$. Since $z \in X$

$n \cdot (m + z) = n \cdot m + n \cdot z$, for all $n, m \in$ N. (2.2)

Thus, by definition and Equation (2.2), we see that

$n\cdot(m+S(z)) = n\cdot S(m+z) = n\cdot(m+z)+n = (n\cdot m+n\cdot z)+n = n\cdot m+(n\cdot z+n) = n\cdot m+n\cdot S(z)$, for all $n, m \in$ N. Hence, $S(z) \in X$ and thus by Axiom P3, $X =$ N.

Exercise 2.1.4. *Prove the following using only the above properties:*

1. [Uniqueness of addition] *For every $m, n, k \in$ N, if $m = n$ then $m + k = n + k$. 2.* [Additive cancellation] *For every $x, y \in$ N, if $x + z = y + z$ for some $z \in$ N then $x = y$. 3.* [Associativity of multiplication] *For every $x, y, z \in$ N, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$. 4.* [Multiplication by 1] *For each $n \in$ N, $1 \cdot n = n$.*

5. [Second distributive law] *For every $n, m, k \in$ N, $(m + n) \cdot k = m \cdot k + n \cdot k$. 6.*

[Commutativity of multiplication] *For each m, n* ∈ N*, n · m = m · n.*

7. [Uniqueness of multiplication] *For every m, n, k* ∈ N*, whenever m = n then m · k = n · k. 8.*

[Multiplicative cancellation] *For every x, y* ∈ N*, if x · z = y · z for some z* ∈ N *then x = y.*

2.2 Other forms of Principle of Mathematical Induction

Mathematical Induction is an important and useful technique used for proofs in Mathematics. This in a sense is a reformulation of the Axiom of Induction. We discuss this principle now. Let $P(n)$ be a statement which may or may not be true for any natural number n. Consider the set $X = \{n \in$ N : $P(n)$ is true $\}$. The axiom of induction states that if $1 \in X$ and $n \in X$ implies $n + 1 = S(n) \in X$, for all $n \in$ N then $X =$ N. In other words, if $P(1)$ is true and $P(n)$ is true implies $P(n + 1)$ is true for all $n \in$ N then one concludes that $P(n)$ is true for all $n \in$ N. The formal description is given below.

[Principle of Mathematical Induction (PMI)] Let $P(n)$ be a statement (proposition) dependent on a natural number $n \in$ N such that the following hold:

1. Base step: $P(1)$ is true.
2. Induction step: for each $n \in$ N, the statement $P(n)$ is true implies $P(n + 1)$ is true.

Then, $P(n)$ is true for all $n \in$ N.

We give an analogy, to the above principle.

Observation.

Imagine a ladder with n rungs, where n can be very large. Suppose I wish to climb the ladder. The strategy that I would like to adopt is:

1. I step onto the first rung of the ladder.

2. When I am on the k-th rung of the ladder, I know how to climb to the $(k + 1)$-th rung.

Here, observe that if $k = 1$, then I am on the first rung and using 2, I climb to the second rung. When $k = 2$, by 2, I can climb to the third rung. In short, using 1, I step onto the ladder and then using 2 repeatedly, I ascend up the ladder. This is the essence of mathematical induction.

Stepping onto the ladder is referred to as the base step and the process of moving to the $(k + 1)$- th step from the k-th step is referred to as the inductive step. The above idea is formalized as the principle of mathematical induction. We now state and prove it using Peano axioms. We now present three simple examples to illustrate this.

Example 2.2.1. 1. Compute the sum of the first n natural numbers.

Let $P(n)$ be the statement that $\mathrm{P}^n{}_{i=1}$ $i = n(n + 1)$ 2.

(a) Base step: $n = 1$ $\Rightarrow \mathrm{P}^1{}_{i=1}$ $i = 1 = 1 \cdot 2$ 2.

(b) Induction hypothesis: Let us assume that $P(k)$ holds and show that $P(k + 1)$ holds. Here,

$_{k+1}$ X $i = \mathrm{X}^k$ 2+ $(k + 1) =$ $(k +$

1)(k + 2)
i=1

i + (k + 1) = k(k + 1)
i=1
2·

Thus, by PMI $P(n)$ is true for all $n \in$ N.

2. Prove that 6 divides $n^3 + 5n$ for all natural numbers.

Let $P(n)$ be the statement that 6 divides $n^3 + 5n$.

(a) Base step: $n = 1 \Rightarrow 1^3 + 5 \cdot 1 = 6$, which is clearly divisible by 6.

(b) Induction hypothesis: Let us assume that $P(k)$ holds and show that $P(k + 1)$ holds. Note that the properties of addition and multiplication implies that $(k + 1)^3 = k^3 + 3k^2 + 3k + 1$. Thus,

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

By induction hypothesis, 6 divides $k^3 + 5k$; 6 divides 6 and 6 also divides $3k(k+ 1)$ as either k or $k + 1$ is even for all natural number k.

Thus, by PMI $P(n)$ is true for all $n \in$ N.

3. Let A = 1 1 0 1 . Then prove that A^n = 1 n 0 1 , for all $n \geq$ 1.

A^n =

For $n \geq 1$, let $P(n)$ be the statement that 1 n 0 1 . Then,

= A^1 =

(a) $P(1) = A$ 1 1 0 1 holds true.

(b) So, let us assume that $P(k)$ is true and show that $P(k + 1)$ holds. Here, $P(k)$ holds true implies that A^k = 1 k 0 1 1 k + 1

. Thus, 1 k 1 1

A^{k+1} = A^kA = 0 1 0 1 = 0 1 .

Thus, by PMI $P(n)$ is true for all $n \geq 1$.

There is another form of the principle of mathematical induction, generally called the principle of strong induction, wherein the difference is in the induction step.

Theorem 2.2.2. [Principle of strong induction (PSI)] *Let $P(n)$ be a statement dependent on $n \in$ N such that the following hold:*

1. Base step: $P(1)$ *is true.*

2. Induction step: *For each $n \in$ N, $P(1)$, $P(2)$, . . . , $P(n)$ are all true implies $P(n + 1)$ is true.*

Then, $P(n)$ is true for all $n \in$ N.

Proof. Let $X = \{n \in$ N : $P(1)$ and $P(2)$ and . . . and $P(n)$ hold true$\}$. Since $P(1)$ is assumed true, $1 \in X$. Let $n \in X$. Then all of $P(1)$, $P(2)$, . . . , $P(n)$ are true. By the induction step, $P(n + 1)$ is true. That is, $n + 1 = S(n) \in X$. Thus, X is an inductive set and hence by Axiom P3, X = N. Therefore, $P(n)$ is true for all $n \in$ N.

As expected, PSI is equivalent to PMI. We now prove this equivalence.

Theorem 2.2.3. [Equivalence of PMI and PSI] *Let $P(n)$ be a statement dependent on $n \in$ N. Suppose that P means the statement ‘$P(n)$ is true for each $n \in$ N. ’ Then ‘P can be proved using PMI’ if and only if ‘P can be proved using PSI’.*

Proof. Let us assume that P has been proved using PMI. Hence, $P(1)$ is true. Further, whenever $P(n)$ is true, we are able to establish that $P(n + 1)$ is true. Therefore, we can recursively establish that $P(n + 1)$ is true if $P(1), . . . , P(n)$ are true. Hence, P can be proved using PSI.

So, now let us assume that P has been proved using PSI. Define $Q(n)$ to mean ‘P(`) holds for ` = $1, 2, . . . , n$. ’ Notice that $Q(1)$ is true. Suppose that $Q(n)$ is true, *i.e.*, P(`) is true for

` = $1, 2, . . . , n$. But, by hypothesis, we know that $P$ has been proved using PSI. Thus, $P(n + 1)$ is true whenever $P$(`) is true for ` = $1, 2, . . . , n$. This, in turn, means that $Q(n + 1)$ is true. Hence, by PMI, $Q(n)$ is true for all $n \in$ N using PMI. Thus, P can be proved using PMI.

There are many variations of PMI and PSI. One useful formulation considers the set N\{$1, 2, . . . , n_0$} (for some fixed $n_0 \in$ N) instead of N. We formulate and prove one such version of PMI below.

Theorem 2.2.4. [Another form of PMI] *Let $n_0 \in$ N. Let $P(n)$ be a statement dependent on $n \in$ N such that the following hold:*

1. *$P(n_0 + 1)$ is true.*
2. *For each $n \ge n_0 + 1$, $P(n)$ is true implies $P(n + 1)$ is true.*

Then, $P(n)$ is true for each $n \ge n_0 + 1$.

Proof. Since $n_0 \in$ N, for each $n \in$ N, $n + n_0 \in$ N. Consider the statement $Q(n) := P(n + n_0)$. Then $Q(1) = P(n_0 + 1)$.

Let $n \ge n_0 + 1$. Then, $n = n_0$ +`, for some ` ∈ N with ` ≥ 1. Let us now assume that $Q$(`) is true. Then, by definition P(` + $n_0$) = $P(n)$ holds true as $Q$(`) = P(` + $n_0$). Therefore, using the second assumption and the commutativity of addition, $P(n + 1)$ = $P$(` + n_0 + 1) = P(` + 1 + $n_0$) holds true. Thus, $Q$(` + 1) = P(` + 1 + n_0) holds true. Hence, we have shown the following:

1. $Q(1)$ is true.
2. Further, for each ` ∈ N, ` ≥ 1 the assumption Q(`) is true implies that $Q$(` + 1) is true.

Hence, by PMI, it follows that for each $m \in$ N, $Q(m)$ is true. However, $m \ge 1$ implies $n \ge n_0 + 1$. Therefore, for each $n \ge n_0 + 1$, $P(n)$ is true.

Exercise 2.2.5. *Prove the following variations of PSI and PMI.*

1. Variation of PSI*: Let $n_0 \in$ N be fixed. Let $P(n)$ be a statement dependent on $n \in$ N such that the following hold:*

   $P(n_0 + 1)$ is true.

   For each $n \ge n_0 + 1$, $P(n_0 + 1), P(n_0 + 2), . . . , P(n)$ are true implies $P(n + 1)$ is true.

Then for each $n \geq n_0 + 1$, $P(n)$ is true.

2. Variation of PMI*: Let $n_0 \in$ N and let $\mathrm{N}_0 = \{n_0 + 1, n_0 + 2, \ldots\}$. Let $X \subseteq \mathrm{N}_0$ be such that $n_0 + 1 \in X$, and for each $n \in \mathrm{N}_0$, $n_0 + 1, n_0 + 2, \ldots, n \in X$ implies $S(n) \in X$. Then $X = \mathrm{N}_0$.*

As an application, we now prove the following result.

Example 2.2.6. Every natural number greater than or equal to 2 is a product of primes.[1] Let $P(n)$ be the statement that any natural number $n \geq 2$ can be written as a product of primes.

1. Base step: Let $n = 2$. As 2 is prime, $P(2)$ is true.
2. Induction step: Assume that $P(1), P(2), \ldots, P(k)$ are all true.

   Consider the natural number $k + 1$. Then, we consider the following two cases: (a) If $k + 1$ is prime then $P(k + 1)$ holds.

[1] Refer to Definition 4.1.11 for prime numbers.

(b) $k + 1$ is not a prime. In this case, there exists $p, q \in \{2, 3, \ldots, k\}$ such that $p \cdot q = k + 1$. Since $p, q \leq k$, by PSI we already know that each of p and q can be written as product of primes, say $p = p_1 \cdots p_s$ and $q = q_1 \cdots q_t$. Thus, $k + 1 = (p_1 \cdots p_s) \cdot (q_1 \cdots q_t)$. Therefore, $P(k + 1)$ holds.

Hence by PSI, $P(n)$ is true for all $n \in$ N.

2.3 Applications of Principle of Mathematical Induction

Example 2.3.1. [Triangular numbers]

1. Show that for each $x \in$ N, $x \geq 2$, there exists a unique $t \in$ N such that $1 + 2 + \cdots + t < x \leq 1 + 2 + \cdots + t + (t + 1)$.
2. Let $S_0 = 0^1$ and let $S_t = 1 + 2 + \cdots + t$ for $t \in$ N. Show that for each $x \in$ N, there exists a unique $t \in$ W = N $\cup$ $\{0\}$ such that $S_t < x \leq S_{t+1}$.

The base steps in PMI and PSI are important, and overlooking these may result in spurious arguments. See the following example.

Example 2.3.2. [Wrong use of PSI] The following is an incorrect proof of "if a set of n balls contains a green ball then all the balls in the set are green". Find the error.

Proof. The statement holds trivially for $n = 1$. Assume that the statement is true for $n \leq k$. Take a collection B_{k+1} of $k + 1$ balls that contains at least one green ball. From B_{k+1}, pick a collection B_k

of k balls that contains at least one green ball. Then by the induction hypothesis, each ball in B_k is green. Now, remove one ball from B_k and put the ball which was left out in the beginning. Call it $B^0{}_k$. Again by induction hypothesis, each ball in $B^0{}_k$is green. Thus, each ball in B_{k+1} is green. Hence by PMI, our proof is complete.

The following result enables us to define a function on N inductively.

Theorem 2.3.3. [Inductive definition of function] *Let f be a relation from* N *to a nonempty set X* *satisfying*

1. *$f(\{1\})$ is a singleton, and*

2. *for each $n \in$ N, if $f(\{n\})$ is a singleton implies $f(\{S(n)\})$ is a singleton.*

Then, f is a function N *to X.*

Proof. By the hypothesis, f is already a partial function. Now, let A = dom f. Note that $1 \in A$ and $n \in A$ implies $S(n) \in A$. So, by the induction axiom A = N. Thus, f is a function. In the following exercises, assume the usual properties of x^n where $x \in$ C and $n \in$ N ∪ $\{0\}$.

Exercise 2.3.4. *1. Let a, a+d, a+2d, . . . , a+(n−1)d be the first n terms of an arithmetic progres*

sion, with a, $d \in$ C. Then $^n{}_2(2a + (n - 1)d)$. $_{i=0}$

^{n}X^{-1}

$(a + id) = a + (a + d) + \cdot \cdot \cdot + (a + (n - 1)d) =$

2. *Let a, ar, ar^2, . . . , ar^{n-1}be the first n terms of a geometric progression, with a, $r \in$* C, *r 6*= 1.

Then $ar^j = a + ar + \cdot \cdot {}_1\ {}_{r-1}\cdot$

^{n}X^{-1} $_{i=0}$ $\cdot + ar^{n-1} = {}_{a}r^{n} -$

3. *Prove that*

[1]The reader may refer to Section 2.6 for the construction of the set of integers.

(a) 6 *divides $n^3 - n$, for all $n \in$* N.

(b) 12 *divides $n^4 - n^2$, for all $n \in$* N.

(c) 7 *divides $n^7 - n$, for all $n \in$* N.

(d) 3 *divides $2^{2n} - 1$, for all $n \in$* N.

(e) 9 *divides $2^{2n} - 3n - 1$, for all $n \in$* N.

(f) 10 *divides $n^9 - n$, for all $n \in$* N.

(g) 12 *divides $2^{2n+2} - 3n^4 + 3n^2 - 4$, for all $n \in$* N.

(h) $1^3 + 2^3 + \cdot \cdot \cdot + n^3 = (1 + 2 + \cdot \cdot \cdot + n)^2$.

4. *Find a formula for* $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdot \cdot \cdot + (n - 1) \cdot n$ *and prove it.*

5. *Find a formula for* $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + 3 \cdot 4 \cdot 5 + \cdot \cdot \cdot + (n - 1) \cdot n \cdot (n + 1)$ *and prove it. 6. Find a formula for* $1 \cdot 3 \cdot 5 + 2 \cdot 4 \cdot 6 + \cdot \cdot \cdot + n \cdot (n + 2) \cdot (n + 4)$ *and prove it. 7. For every positive integer $n \geq 5$ prove that $2^n > n^2 > 2n + 1$.*

8. *Prove by induction that 2^n divides $(n + 1)(n + 2)\cdot \cdot \cdot(2n)$.*

9. [AM-GM inequality]

(a) *Let a_1, . . . , a_9 be non-negative real numbers such that the sum $a_1 + \cdot \cdot \cdot + a_9 = 5$. Consider the numbers* $\underline{{}^{a}{}_{1+a_2}}$

$_{2},\underline{{}^{a}{}_{1+a_2}}$

$_{2}$, a_3, . . . , a_9 *and argue that*

2

$2{+}a_1 + a_2$ $\quad a_3 \cdot \cdot \cdot a_9.$

$a_1 + a_2$

$a_1 + a_2$

$2{+}\ a_3 + \cdot \cdot \cdot + a_9 = 5,\ a_1 \cdot \cdot \cdot$

$a_9 \leq 2$

(b) Among two pairs of non-negative real numbers with equal sum, the pair with least difference has the largest product.

(c) The product of $n \geq 2$ non-negative real numbers is maximum when all numbers are equal.

(d) Let $a_1, \ldots, a_n$ be non-negative real numbers. Show that $[(a_1 + \cdots + a_n)/n]^n \geq a_1 \cdots a_n$; and equality is achieved, when $a_1 = \cdots = a_n$.

10. For all $n \geq 32$, there exist non-negative integers x and y such that $n = 5x + 9y$. 11. Prove that, for all $n \geq 40$, there exist non-negative integers x and y such that $n = 5x + 11y$. 12. Prove that for $\mu > 0$,

$$\Upsilon^{p} \quad (1 + l\mu) \geq 1 + p(p+1) \quad 4 - p(p+1)(2p+1)\ 6$$

$$2\mu + \ ^{1}\ 2\, p^2(p+1)^2 \qquad {}_{l=1} \qquad \mu^2.$$

13. By an L-shaped piece, we mean a piece of the type shown in the picture. Consider a $2^n \times 2^n$ square with one unit square cut. See the picture given below.

L-shaped piece 4 × 4 square with a unit square cut

Show that a $2^n \times 2^n$square with one unit square cut, can be tiled with L-shaped pieces.

14. Use $(k+1)^5 - k^5 = 5k^4 + 10k^3 + 10k^2 + 5k + 1$ use PMI to prove your answer. $_{k=1}$

to get a closed form expression for P^n

k^4. Then

2.4 Well Ordering Property of Natural Numbers

In this section, we introduce an ordering, denoted by <, on N. So, for any *m, n* ∈ N, we need to define what *n* < *m* means?

Definition 2.4.1. Let *m, n* ∈ N. Then, the natural number *n* is said to be strictly less than the natural number *m*, denoted by *n* < *m*, (in word, *n* is less than *m*) if there exists a *k* ∈ N such that *m* = *n* + *k*. Further, *n* ≤ *m* will imply that either *n* = *m* or *n* < *m*. When *n* < *m*, we also write *m* > *n* and read it as *m* is greater than *n*.

We prove some properties of N with the ordering <.

Lemma 2.4.2. [Transitivity] *Let x, y, z* ∈ N *such that x < y and y < z. Then x < z.*

Proof. Since *x* < *y*, there exists *k* ∈ N such that *y* = *x* + *k*. Similarly, *y* < *z* gives the existence of ` ∈ N such that *z* = *y* + `. Hence, *z* = *y* + ` = (*x* + *k*) + ` = *x* + (*k* + `) = *x* + *t*, where *t* = *k* + ` ∈ N as *k*, ` ∈

N. Since the sum of two natural numbers is a natural number, we conclude from Definition 2.4.1 that $x < z$.

Exercise 2.4.3. *Let $x, y, z \in$ N. Then prove the following:*

1. *If $x \leq y$ and $y < z$ then $x < z$.*
2. *If $x < y$ and $y \leq z$ then $x < z$.*
3. *If $x \leq y$ and $y \leq z$ then $x \leq$ z.*

4. *If $x < y$ then $x + z < y + z$ and $x \cdot z < y \cdot z$.*

Lemma 2.4.4. *For all $m, n \in$ N, $m 6= m + n$.*

Proof. Suppose there exist $m, n \in$ N such that $m = m + n$. Then $m + 1 = m + n + 1 = m + S(n)$. By additive cancellation (Exercise 2.1.4.2), $1 = S(n)$, contradicting Axiom P2.

Lemma 2.4.5. [Law of trichotomy] *For all $m, n \in$ N, exactly one of the following is true: $n <$*

m, $n = m$, $n > m$.

Proof. As a first step, we show that no two of the above can hold together. For, suppose $n < m$ and $n = m$. Then $n = m + k$ for some $k \in$ N and $n = m$. That is, $m = m + k$, which contradicts Lemma 2.4.4. As another possibility, assume that $n < m$ and $n > m$. Then there exist k, ` $\in$ N such that $n = m+k$ and $m = n+`$. So that $n = m+k = n+ (`+k)$, which again contradicts Lemma 2.4.4. Similarly, other possibilities can be ruled out and is left as an exercise for the reader.

To complete the proof, fix $n \in$ N, and define $X = \{m \in$ N $: n < m$ or $n = m$ or $n > m\}$. We show that $X =$ N.

First, we need to show that $1 \in X$. If $n = 1$ then $1 = 1$ and hence $1 \in X$. If $n 6= 1$ then there exists $y \in$ N such that $n = S(y) = y + 1 = 1 + y$ and hence by the definition of order, $1 < n$ or $n > 1$. Thus, $1 \in X$.

Next, in order to apply Axiom P3, assume that $m \in X$. Then either $n < m$ or $n = m$ or $n > m$. We will consider all three cases and in each case show that $S(m) \in X$.

If $n < m$, then $m = n +$ ` for some ` $\in$ N. Thus, $S(m) = S(n + `) = (n + `) + 1 = n + (` + 1)$; and hence $n < S(m)$. Therefore, $S(m) \in X$.

If $m = n$, then $S(m) = m + 1 = n + 1$. So, $n < S(m)$. Thus $S(m) \in X$.

If $n > m$ then $n = m + k$, for some $k \in$ N. Further, if $k = 1$, then $n = m + 1$ and $S(m) = n$. Thus, $S(m) \in X$. If $k 6= 1$, then there exists ` $\in$ N such that $S(`) = k$. Then,

$$n = m + k = m + S(`) = m + (` + 1) = m + (1 + `) = (m + 1) + ` = S(m) + `.$$

Hence $S(m) < n$ and hence $S(m) \in X$.

Thus, by Axiom P3, $X =$ N.

As an application of the law of trichotomy, we show that there does not exist any natural number between n and $S(n)$. Or equivalently, if $n \leq m < n + 1$, then it is necessarily true that $n = m$. Observe that this fact is a consequence of the following result.

Lemma 2.4.6. *For all* $m, n \in$ N*,* $m \leq n$ *if and only if* $m < n + 1$*.*

Proof. Let $m, n \in$ N. Suppose $m \leq n$. Clearly, $n < n + 1$. So, if $m = n$, then $n < n + 1$ implies that $m < n + 1$. If $m < n$, then $n < n + 1$ again implies that $m < n + 1$. Thus, in any case, $m < n + 1$. Conversely, suppose $m < n + 1$. If m 6≤ n, then by the law of trichotomy, $m > n$. That is, there exists ` ∈ N such that $m = n +$ `. It follows that $n +$ ` $< n + 1$ for some ` ∈ N. Thus, using Additive Cancellation (Exercise 2.1.4.2), one has ` < 1. However, either ` = 1 or ` = $S(k)$ for some $k \in$ N. The first case implies 1 < 1 and the second case implies that 1 is a successor of some natural number; giving us a contradiction in either case. Hence $m \leq n$.

We are now in a position to state an important principle, namely the well ordering principle.

Theorem 2.4.7. [Well Ordering Principle in N] *Every nonempty subset X of* N *contains its least element.*

Proof. By definition, a least element of a set is an element of the set. We thus need to show that every nonempty subset of N has a least element. On the contrary, suppose A is a nonempty subset of N that has no least element. Let $B =$ N \ A. If $1 \in A$, then 1 will be the least element of A. Thus 1 6∈ A so that $1 \in B$.

Suppose $1, 2, \ldots, m \in B$. Then, none of $1, 2, \ldots, m$ is in A. If $S(m) \in A$, then $S(m)$ would be the least element of A. Thus, $S(m)$ 6∈ A and hence $S(m) \in B$.

Hence, by the strong form of induction, $B =$ N. Then, $B =$ N\A implies $A = \varnothing$, a contradiction.

Exercise 2.4.8. [Variation of well ordering principle] *Let* $n_0 \in$ N *and let X be a nonempty subset of* $\{n_0 + 1, n_0 + 2, \ldots, \}$*. Then prove that X contains its least element.*

2.5 Recursion Theorem

Recall how we defined addition and multiplication in N. For any fixed $n \in$ N, we defined addition by declaring that $n + 1 := S(n)$ and $n + S(m) := S(n + m)$. Due to induction, we remarked that for each $m \in$ N, these two conditions defined $n + m$. This intuitive work requires a formal justification. Notice that + is a binary operation on N, that is, + is a function from N×N to N. We need to derive rigorously from our axioms that a function satisfying the properties $n + 1 := S(n)$ and $n + S(m) := S(n + m)$ exists, and that such a function is unique. Similarly, multiplication is to be tackled. We rather present a more general result, and view the definitions of addition and multiplication as special cases. The following result provides this general framework in N.

Theorem 2.5.1. [Recursion Theorem] *Let* $f :$ N → N *be a function. Then, for any fixed natural number* α*, there exists a unique function* $g :$ N → N *such that*

$$g(1) = \alpha \text{ and } g(S(x)) = f(g(x)) \text{ for each } x \in \mathrm{N}. \quad (2.3)$$

Proof. Define $g \subseteq$ N × N as follows

1. $(1, \alpha) \in g$, and
2. $(x, y) \in g$ implies $(S(x), f(y)) \in g$.

As 1 is not a successor of any natural number, $g(\{1\}) = \{\alpha\}$, is a singleton. Assume that $g(\{x\}) = \{y\}$. Then, $g(\{S(x)\}) = \{f(y)\}$, a singleton as f is a function. So, by Theorem 2.3.3, g is a function. To show the uniqueness of the function g, we consider two functions $g_1, g_2 : \mathbb{N} \to \mathbb{N}$, satisfying Equation (2.3). Now, define

$$V = \{n \in \mathbb{N} : g_1(n) = g_2(n)\}.$$

From Equation (2.3), $g_1(1) = g_2(1) = \alpha$. So, $1 \in V$.

Let $n \in V$. Here, $g_1(n) = g_2(n)$. Therefore, $g_1(S(n)) = f(g_1(n)) = f(g_2(n)) = g_2(S(n))$. Thus, $S(n) \in V$. By Axiom P3, $V = \mathbb{N}$. Therefore, $g_1 = g_2$.

Using the recursion theorem, we now show that the definitions of addition and multiplication are indeed well defined.

Example 2.5.2. 1. [Addition function] Let $f : \mathbb{N} \to \mathbb{N}$ be the function defined by $f(x) = S(x)$, for all $x \in \mathbb{N}$. Fix any element $y \in \mathbb{N}$. By the recursion theorem, there exists a unique function

$$g : \mathbb{N} \to \mathbb{N} \text{ such that } g(1) = S(y) \text{ and } f(g(x)) = g(S(x)), \text{ for all } x \in \mathbb{N}. \quad (2.4)$$

Define

$$\text{for all } x \in \mathbb{N},\ y + x := g(x) \quad (2.5)$$

When $x = 1$, from Equation (2.5), we get $y + 1 = g(1)$. As $g(1) = S(y)$, we get $y + 1 = S(y)$.

Further, for any $x \in \mathbb{N}$, we see that

$$\begin{aligned} y + S(x) &= g(S(x)) \text{ (using Equation (2.5))} \\ &= f(g(x)) \text{ (using } f(g(x)) = g(S(x))) \\ &= S(g(x)) \text{ (using } f(x) = S(x)) \\ &= S(y + x). \text{ (using } g(x) = y + x) \end{aligned}$$

Thus, for all $y, x \in \mathbb{N}$, $y + S(x) = S(y + x)$. Hence, both the rules of addition stated in stated in Definition 2.1.2 are satisfied.

2. [Multiplication function] Fix an element $y \in \mathbb{N}$ and consider the function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x + y$. (Observe that this is well defined by Part 1.)

   Then, by the recursion theorem, there exists a unique function $h : \mathbb{N} \to \mathbb{N}$, such that $h(1) = y$ and $f(h(x)) = h(S(x))$, for all $x \in \mathbb{N}$. Now, define $y \cdot x := h(x)$, for all $x \in \mathbb{N}$.

   Then, for $x = 1$, we get $y \cdot 1 = h(1) = y$. Further, for any $x \in \mathbb{N}$, we see that

   $$y \cdot S(x) = h(S(x)) = f(h(x)) = f(y \cdot x) = y \cdot x + y,$$

   thereby, proving both the rules of multiplication stated in Definition 2.1.3.

3. [Power function] Fix an element $m \in \mathbb{N}$ and consider the function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x \cdot m$. (Part 2 allows us to define such a function.)

   Then, by the recursion theorem, there exists a unique function $p : \mathbb{N} \to \mathbb{N}$, such that $p(1) = m$ and $f(p(x)) = p(S(x))$, for all $x \in \mathbb{N}$. Now, define $m^x := p(x)$, for all $x \in \mathbb{N}$.

Then, for $x = 1$, we get $m^1 = p(1) = m$. Further, for any $x \in$ N, $S(x) = x + 1$ gives

$$m^{x+1} = m^{S(x)} = p(S(x)) = f(p(x)) = p(x) \cdot m = (m^x) \cdot m.$$

Hence, we have obtained the required power function.

Remark 2.5.3. Recall that in Example 2.5.2.1, it was easy to show that $y + S(x) = S(y + x)$, for all $y, x \in$ N. What is more difficult to prove is that $S(y) + x = S(y + x)$, for all $x, y \in$ N which together with Example 2.5.2.1 gives us commutativity of addition.

So, we take $X = \{x \in$ N $: S(y) + x = S(y + x)\}$ and prove that X is an inductive set. By the recursion theorem, there exists a unique function $t :$ N → N such that $t(1) = S(S(y))$ and $f(t(x)) = t(S(x))$, for all $x \in$ N. Define

$$S(y) + x := t(x) \text{ for all } x \in \text{N}. \quad (2.6)$$

As $g(1) = S(y)$ (see Example 2.5.2.1) and $g(1) = y + 1$ (Equation (2.5)), we see that for $x = 1$, $S(y) + 1 = t(1) = S(S(y)) = S(g(1)) = S(y + 1)$. This implies that $1 \in X$.

To show that $X =$ N, we assume that $x \in X$. Now, consider $S(y) + S(x)$. Then, using Exam ple

2.5.2.1, $S(y) + S(x) = S(S(y) + x)$. As $x \in X$, $S(y) + x = S(y + x)$ and hence

$$S(y) + S(x) = S(S(y) + x) = S(S(y + x)) = S(y + S(x)).$$

where the last equality also follows from Example 2.5.2.1.

Therefore, $S(x) \in X$, whenever $x \in X$. Therefore, by Axiom P3, $X =$ N.

2.6 Construction of Integers

By now, the readers should have got a glimpse of the work required to axiomatically construct N, the set of natural numbers. Similarly, the construction of integers from natural numbers and the construction of rational numbers from integers require quite a lot of work. These constructions are very helpful in understanding advanced algebra. In this section and the succeeding one, we will discuss how to construct the integers and rational numbers from the natural numbers.

To start with let $X =$ N × N. We define a relation '~' on X by

$$(a, b) \sim (c, d) \text{ if } a + d = b + c \text{ for all } a, b, c, d \in \text{N}.$$

Then, verify that ~ is indeed an equivalence relation on X. Let Z denote the collection of all equiv alence classes under this relation. So, if [x], [y] $\in$ Z then [x] is an equivalence class containing x = (x_1, x_2), for some $x_1, x_2 \in$ N and [y] is an equivalence class containing y = (y_1, y_2), for some $y_1, y_2 \in$ N. Now, using the successor function S defined in Axiom P2, observe that

1. $[(1, 1)] = \{(n, n) :$ for all $n \in$ N$\}$,
2. for a fixed element $m \in$ N, $[(1, S(m))] = \{(n, m + n) :$ for all $n \in$ N$\}$, and
3. for a fixed element $m \in$ N, $[(S(m), 1)] = \{(m + n, n) :$ for all $n \in$ N$\}$.

Further, Z consists of all equivalence classes of the above forms. That is,

$$\text{Z} = [(1, 1)] \cup [(1, S(m))] : m \in \text{N} \cup [(S(m), 1)] : m \in \text{N} \cdot$$

Definition 2.6.1. Let [x] = $[(x_1, x_2)]$, [y] = $[(y_1, y_2)] \in$ Z for some $x_1, x_2, y_1, y_2 \in$ N. Define [x] ⊕ [y] = $[(x_1, x_2)] \oplus [(y_1, y_2)] = [(x_1 + y_1, x_2 + y_2)]$. (2.7) The map ⊕ : Z × Z → Z, defined above is called the addition in Z.

Note that addition, ı.e., the function ⊕ maps a pair of two nonempty sets, say $[(x_1, x_2)]$ and $[(y_1, y_2)]$ to the set $[(x_1 + y_1, x_2 + y_2)]$. Thus, we need to verify that the addition of two different representatives of the domain, give rise to the same set on the range. This process of defining a map using representatives and then verifying that the image is independent of the representatives chosen is characterized by saying that "the map is well-defined". So, let us now prove that ⊕ is well-defined.

Lemma 2.6.2. *The map ⊕ defined in Equation (2.7) is well-defined.*

Proof. Let $[(u_1, u_2)] = [(v_1, v_2)]$ and $[(x_1, x_2)] = [(y_1, y_2)]$ be two equivalence classes in Z. Then, by definition

$$[(u_1, u_2)] \oplus [(x_1, x_2)] = [(u_1 + x_1, u_2 + x_2)], \; [(v_1, v_2)] \oplus [(y_1, y_2)] = [(v_1 + y_1, v_2 + y_2)].$$

For well-definedness, we need to show that $[(u_1 + x_1, u_2 + x_2)] = [(v_1 + y_1, v_2 + y_2)]$. Or equivalently, we need to show that $u_1 + x_1 + v_2 + y_2 = u_2 + x_2 + v_1 + y_1$.

But, the equality of the equivalence classes $[(u_1, u_2)] = [(v_1, v_2)]$ and $[(x_1, x_2)] = [(y_1, y_2)]$ implies $u_1+v_2 = u_2+v_1$ and $x_1+y_2 = x_2+y_1$. Thus, adding the two and using the commutativity of addition in N, we get

$$u_1 + x_1 + v_2 + y_2 = u_2 + x_2 + v_1 + y_1.$$

Thus, the required result follows.

On similar lines, we now define multiplication among elements of Z.

Definition 2.6.3. Let [x] = $[(x_1, x_2)]$, [y] = $[(y_1, y_2)] \in$ Z, for some $x_1, x_2, y_1, y_2 \in$ N. Then, one defines multiplication in Z, denoted by , as

$$[x] \quad [y] = [(x_1, x_2)] \quad [(y_1, y_2)] = [(x_1y_1 + x_2y_2, x_1y_2 + x_2y_1)]. \tag{2.8}$$

Since we are talking about multiplication between two sets using their representatives, we need to verify that the multiplication is indeed well-defined. So, the readers are required to prove that multiplication is well-defined. Further, the following properties of of addition and multiplication in Z can be proved by using the corresponding properties of natural numbers and hence is left as an exercise for the readers.

Exercise 2.6.4. *1. Show that the multiplication defined in Equation* (2.8) *is well-defined. 2.*

Let [x], [y], [z] ∈ Z. *Write* [0] = [(1, 1)]. *Prove the following:*

(a) [Associativity of addition] ([x] + [y]) + [z] = [x] + ([y] + [z]).

(b) [Commutativity of addition] [x] + [y] = [y] + [x].

(c) [Existence of the zero element] [x] + [0] = [x].

(d) [Cancellation property] *If* [x] + [y] = [x] + [z] *then* [y] = [z]. *This implies that the zero element is unique.*

(e) [Existence of additive inverse] *for every* [x] = [(x_1, x_2)], *the equivalence class* [(x_2, x_1)], *denoted by* −[x], *satisfies* [x]⊕(−[x]) = [0]. *Now, use the cancellation property in* Z *to show that the additive inverse is unique. So, the equivalence class* −[x] *is called the* additive inverse *of* [x].

(f) [Distributive laws] ([x] + [y])   [z] = [x]   [z] ⊕ [y]   [z].

(g) [Associativity of multiplication] ([x]   [y])   [z] = [x]   ([y]   [z]).

(h) [Commutativity of multiplication] [x]   [y] = [y]   [x].

(i) [Existence of the identity element] [x]   [1] = [x], *where* [1] = [(*S*(1), 1)]. *(j)*
[Cancellation property] *If* [x]   [y] = [x]   [z] *with* [x] *6*= [0] *then* [y] = [z]. *(k)* [x]   [0]
= [0].

As a last property, we show that a copy of N naturally seats inside Z.

Lemma 2.6.5. *Define f* : N → Z *by f*(*n*) = [(*S*(*n*), 1)] *for all n* ∈ N. *Then the following are true: 1. f is one-one.*

2. For all a, b ∈ N, *f*(*a* + *b*) = *f*(*a*) ⊕ *f*(*b*).

3. For all a, b ∈ N, *f*(*a* · *b*) = *f*(*a*)   *f*(*b*).

Proof. 1. Suppose *f*(*a*) = *f*(*b*) for some *a, b* ∈ N. By definition, [(*S*(*a*), 1)] = [(*S*(*b*), 1)] or equivalently, *S*(*a*) + 1 = *S*(*b*) + 1. By the cancellation law in N, we get *S*(*a*) = *S*(*b*). Since *S* is one-one, we have *a* = *b*.

2. Let *a, b* ∈ N. By definition, *f*(*a* + *b*) = [(*S*(*a* + *b*), 1)]. So

$$f(a) \oplus f(b) = [(S(a), 1)] \oplus [(S(b), 1)] = [(S(a) + S(b), 1 + 1)] = [(S(a) + b + 1, 1 + 1)] =$$
$$[(S(a + b) + 1, 1 + 1)] = [(S(a + b), 1)] = f(a + b).$$

3. Let *a, b* ∈ N. Now, *f*(*a* · *b*) = [(*S*(*a* · *b*), 1)]. So

$$f(a) \quad f(b) = [(S(a), 1)] \quad [(S(b), 1)] = [(S(a) \cdot S(b) + 1 \cdot 1, S(a) \cdot 1 + 1 \cdot S(b))] =$$
$$[(S(a) \cdot S(b) + 1, S(a) + S(b))] = [(S(a \cdot b), 1)] = f(a \quad b)$$

as *S*(*a*)· *S*(*b*) + 1 + 1 = *S*(*a*)· *b* + *S*(*a*)· 1 + 1 + 1 = *a* · *b* + 1 · *b* + *S*(*a*) + 1 + 1 = *S*(*a* · *b*) + *S*(*b*) + *S*(*a*).

We have shown that *f*(N) ⊆ Z. Further, the map *f* commutes with the addition operation and the multiplication operation. Thus, we identify *f*(N) inside Z as a copy of N. From now on, the symbols + and · will be used for addition and multiplication in integers. Further, as *n* ∈ N is identified with *f*(*n*) = [(*S*(*n*), 1)], we would like to associate the symbol '−' as *n* = *S*(*n*) − 1 and −*n* = 1 − *S*(*n*). We proceed to do this in the next few paragraphs.

Definition 2.6.6. Let [x] = [(x_1, x_2)], [y] = [(y_1, y_2)] ∈ Z, for some x_1, x_2, y_1, y_2 ∈ N. Then, the order in Z is defined by saying that [x] < [y] if $x_1 + y_2 < y_1 + x_2$. Further, [x] ≤ [y] if either [x] = [y] or [x] < [y].

We again need to check for well-definedness. So, let [(u_1, u_2)] = [(v_1, v_2)] and [(x_1, x_2)] = [(y_1, y_2)] be two equivalence classes in Z with [(u_1, u_2)] < [(x_1, x_2)]. We need to show that [(v_1, v_2)] < [y_1, y_2)], or equivalently, $v_1 + y_2 < y_1 + v_2$. As [(u_1, u_2)] = [(v_1, v_2)] and [(x_1, x_2)] = [(y_1, y_2)], one has $u_1 + v_2 = v_1 + u_2$ and $x_1 + y_2 = y_1 + x_2$. Thus, $u_1 + v_2 + y_1 + x_2 = v_1 + u_2 + x_1 + y_2$. Hence,

$$v_1 + y_2 + x_1 + u_2 = v_1 + u_2 + x_1 + y_2 = u_1 + v_2 + y_1 + x_2 = y_1 + v_2 + u_1 + x_2 < y_1 + v_2$$
$$+ x_1 + u_2,$$

as $u_1 + x_2 < x_1 + u_2$. Therefore, by the order property in N (see Exercise 2.4.3), $v_1 + y_2 < y_1 + v_2$. Thus, the above definition is well-defined. At this stage, one would like to verify that the function *f* defined in Lemma 2.6.5 preserves the order as well.

Lemma 2.6.7. *Consider the map* $f : \mathbb{N} \to \mathbb{Z}$ *defined by* $f(n) = [(S(n), 1)]$ *for all* $n \in \mathbb{N}$. *Then, for all* $a, b \in \mathbb{N}$, $a < b$ *if and only if* $f(a) < f(b)$.

Proof. Using Exercise 2.4.3, $a < b$ if and only if $a + 1 + 1 < b + 1 + 1$, or equivalently, $a < b$ if and only if $S(a) + 1 < S(b) + 1$. Thus, $a < b$ if and only if $f(a) = [(S(a), 1)] < [(S(b), 1)] = f(b)$.

Definition 2.6.8. Let $[x] = [(x_1, x_2)] \in \mathbb{Z}$. Then, $[x]$ is said to be positive if $[0] < [x]$ and is said to be non-negative if $[0] \leq [x]$. In general, we write $[x] > [0]$ to mean $[x]$ is positive and $[x] \geq [0]$ for $[x]$ being non-negative.

Lemma 2.6.9. *Let* $[x] = [(x_1, x_2)] \in \mathbb{Z}$. *Then,* $[x] > [0]$ *if and only if* $x_1 > x_2$.

Proof. By definition, $[(x_1, x_2)] > [0] = [(1, 1)]$ if and only if $x_1 + 1 > x_2 + 1$. Or equivalently, using Exercise 2.4.3, one obtains $[(x_1, x_2)] > [(1, 1)]$ if and only if $x_1 > x_2$.

Exercise 2.6.10. *1. Prove the following results for any* $[x] \in \mathbb{Z}$.

(a) $[x] > 0$ *if and only if* $[x] = [(S(n), 1)] = f(n)$ *for some* $n \in \mathbb{N}$.

(b) $[x] > 0$ *if and only if* $-[x] < 0$.

2. $[y] > [z]$, *for some* $[y], [z] \in \mathbb{Z}$ *if and only if* $[y] + [x] > [z] + [x]$.

3. If $[y] > [z]$, *for some* $[y], [z] \in \mathbb{Z}$ *then* $[y] \cdot [x] > [z] \cdot [x]$, *whenever* $[x] > 0$.

Thus, $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$ and hence from now on, in place of using equivalence class to represent the elements of Z, we will just use natural numbers, their negatives and the zero element to represent Z, the set of integers. Thus, whenever we define functions or operations on Z then we need not worry about well-definedness. Let us now discuss the "absolute value function", namely the modulus function.

Definition 2.6.11. A function $g : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ is called an absolute/modulus function if 1. $g(n) = n$ if $n \geq 0$,

2. $g(n) = -n$, if $n < 0$.

This function is denoted by $| \cdot |$. Thus, $|m| = m$, if $m \geq 0$ and $-m$, if $m < 0$. Further, by Exer cise 2.6.10.1, observe that $|m| \geq 0$ for all $m \in \mathbb{Z}$.

For a better understanding of this function, we prove the following two results.

Lemma 2.6.12. *For any* $x \in \mathbb{Z}$, $-|x| \leq x \leq |x|$. *Further, if* $x \geq 0$ *and* $-x \leq y \leq x$ *for some* $y \in \mathbb{Z}$, *then* $|y| \leq x$.

Proof. Let $x \geq 0$. Then, by definition $|x| = x$ and hence $x \leq |x|$. As $|x| = x$, the other inequality $-|x| \leq x$ reduces to $-x \leq x$. Or equivalently, we need to show that $0 = x + (-x) \leq x + x = 2x$, which is indeed true. If $x < 0$ then we see that $|x| > 0 > x$ and hence $x \leq |x|$. Note that the condition $-|x| \leq x$ is equivalent to the condition $|x| + x \geq 0$ (use Exercise 2.6.10.2) which is indeed true as by definition $x + |x| = x + (-x) = 0$.

For the second part, we again consider two cases, namely, $y \geq 0$ and $y < 0$. If $y \geq 0$ then $|y| = y$ and hence the condition $y \leq x$ implies $|y| \leq x$. If $y < 0$ then $|y| = -y$. Further, using Exercise 2.6.10.2,

the condition $-x \leq y$ is equivalent to the condition $0 \leq y + x$ which in turn is equivalent to $-y \leq x$. Hence $|y| = -y \leq x$. Thus, the required result follows.

As a direct application of Lemma 2.6.12, one obtains the triangle inequality.

Lemma 2.6.13. [Triangle inequality in Z] *Let* $x, y \in$ Z. *Then* $|x + y| \leq |x| + |y|$. *Proof.*

Using Lemma 2.6.12, one has $-|x| \leq x \leq |x|$ and $-|y| \leq y \leq |y|$. Hence, $-|x| + (-|y|) \leq$

$$x + y \leq |x| + |y|.$$

Now, use the associativity and commutativity of addition to get

$$0 = -|x| + (-|y|) + |x| + |y| = -(|x| + |y|) + (|x| + |y|)$$

and hence the uniqueness of the additive inverse implies $-|x| + (-|y|) = -(|x| + |y|)$. Thus, the required result follows from the second part of Lemma 2.6.12.

This finishes most of the results on the basic operations related to integers. As a last note, we make the following remark.

Remark 2.6.14. Even though the well ordering principle and its extension (Exercise 2.4.8) is valid for subsets of N, it can be generalized to W, the set of whole numbers. Furthermore, if we fix an integer $z \in$ Z and take $S = \{z, z + 1, z + 2, \ldots\}$ then it can also be shown that every nonempty subset X of S contains its least element. Or equivalently, every nonempty subset X of Z which is bounded below satisfies the well ordering principle.

2.7 Construction of Rational Numbers

We will describe the construction of rational numbers in brief, and and prove a few properties, such as addition, multiplication, subtraction and division by nonzero elements.

We write Z*:= Z\{0} and define an equivalence relation on X = Z×Z* and then doing everything afresh as was done for the set of integers. Define a relation '~' on X by

$$(a, b) \sim (c, d) \text{ if } a \cdot d = b \cdot c \text{ for all } a, c \in \mathrm{Z}, b, d \in \mathrm{Z}^*.$$

Then, verify that ~ is indeed an equivalence relation on X. Let Q denote the collection of all equivalence classes under this relation. This set is called the "set of rational numbers". In this set, we define addition and multiplication, using the addition and multiplication in Z, as follows: 1. Let [x] = $[(x_1, x_2)]$, [y] = $[(y_1, y_2)] \in$ Q. Then, addition in Q, denoted as ⊕, is defined by

$$[x] \oplus [y] = [(x_1, x_2)] \oplus [(y_1, y_2)] = [(x_1 \cdot y_2 + x_2 \cdot y_1, x_2 \cdot y_2)].$$

2. Let [x] = $[(x_1, x_2)]$, [y] = $[(y_1, y_2)] \in$ Q. Then, multiplication in Q, denoted as , is defined by [x]

$$[y] = [(x_1, x_2)] \quad [(y_1, y_2)] = [(x_1 \cdot y_1, x_2 \cdot y_2)].$$

The readers are advised to verify that the above operations in Q are well-defined. Further, the map f : Z → Q defined by $f(a) = [(a, 1)]$, is one-one and it preserves addition and multiplication. Thus, Z is seating inside Q as f(Z). As earlier, we replace the symbols '⊕' and ' ' by '+' and '·'.

Sometimes, $x \cdot y$ is simply written as xy. Note that the element 0 ∈ Z corresponds to [(0, 1)] = [(0, x)] for all $x \in Z^*$. Hence, an element [(x_1, x_2)] ∈ Q with [(x_1, x_2)] 6= 0 implies that x_1 6= 0. Verify that for each [(x_1, x_2)] ∈ Q with x_1 6= 0, the element [(x_2, x_1)] ∈ Q satisfies [(x_1, x_2)] · [(x_2, x_1)] = 1. As the next operation, one defines division in Q as follows.

Definition 2.7.1. Let [x] = [(x_1, x_2)], [y] = [(y_1, y_2)] ∈ Q with y_1 6= 0. Then, the division in Q, denoted as /, is defined by

$$[x]/[y] = [(x_1, x_2)]/[(y_1, y_2)] = [(x_1y_2, x_2y_1)].$$

Note that $x_2y_1 \in Z^*$ as x_2, y_1 6= 0.

The readers are advised to verify that division is well-defined. Before proceeding further with other important properties of rational numbers, the readers should verify all the properties related with addition, subtraction, multiplication, and division by a nonzero element. The next result helps in defining order in Q.

Lemma 2.7.2. [Representation of an Element of Q] *Let* [x] ∈ Q*. Then* [x] = [(y_1, y_2)] *for some* $y_1, y_2 \in$ Z, $y_2 > 0$.

Proof. Let [x] = [(x_1, x_2)] for some $x_1, x_2 \in$ Z. If $x_2 > 0$, we are done. Else, using Exercise 2.6.10.1, we know that $-x_2 > 0$. Then, by the definition of equivalence class we have [x] = [(x_1, x_2)] = [($-x_1$, $-x_2$)]. Hence the required result follows.

Definition 2.7.3. Let [x] = [(x_1, x_2)], [y] = [(y_1, y_2)] ∈ Q for some $x_1, x_2, y_1, y_2 \in$ Z with $x_2, y_2 > 0$. Then the order in Q is defined by [x] > [y] if $x_1y_2 > x_2y_1$.

One should verify that the order in Q is indeed well-defined. Notice that as earlier, [x] ≥ [y] means either [x] = [y] or [x] > [y]. Further, it may be seen that Q is an *ordered field*, that is, the following are satisfied for all $a, b, c \in$ Q:

1. $a + b = b + a$.

2. $(a + b) + c = a + (b + c)$. 3.

$a + 0 = a$.

4. There exists an element, written as $-a$ such that $a + (-a) = 0$.

5. $a \cdot b = b \cdot a$.

6. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

7. $a \cdot 1 = a$.

8. Corresponding to a, there exists an element, written as $1/a \in$ Q such that $a \cdot (1/a) = 1$.

9. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

10. Exactly one of the conditions $a < b$ or $a = b$ or $b < a$ is true.

11. If $a < b$ and $b < c$, then $a < c$.

12. If $a < b$, then $a + c < b + c$.

13. If $a < b$ and $0 < c$, then $a \cdot c < b \cdot c$.

As a final result of this section, we prove the following result.

Lemma 2.7.4. [Existence of a Rational between two Rationals] *Let* [x], [y] ∈ Q *with* [x] < [y]*. Then there exists* [z] ∈ Q *such that* [x] < [z] < [y].

Proof. Let [x] = $[(x_1, x_2)]$ and [y] = $[(y_1, y_2)]$, for some $x_1, x_2, y_1, y_2 \in$ Z with $x_2, y_2 > 0$. Since [x] < [y], $x_1y_2 < x_2y_1$, one has $2x_1y_2 < x_1y_2 + x_2y_1 < 2x_2y_1$. Further, $2x_2y_2 > 0$ and hence let us take [z] = $[(x_1y_2 + x_2y_1, 2x_2y_2)]$. It can be easily verified that [x] < [z] < [y] as $x_2, y_2 \in$ Z and using the multiplicative cancellation (Exercise 2.1.4.8) in Z.

Chapter 3

Countable and Uncountable Sets

In this chapter, we discuss the size of sets. Intuitively, the number of elements in a set may be considered as its size. For instance, the sets $\{1\}$ has size 1 and the set $\{a, b\}$ has size 2. We will be concerned about size of sets of various kinds.

3.1 Finite and infinite sets

We first show that the intuitive notion of 'number of elements in a set' is a well defined notion, at least for finite sets. Since the set $\{1, 2, . . . , m\}$ will be used often, we give a notation for this set.

Notation: $[m] = \{1, 2, . . . , m\}$ for $m \in$ N.

We hope that this notation will not conflict with the notation of an equivalence class induced by an equivalence relation; the context will clarify which one is used.

Lemma 3.1.1. *Let $n \in$ N. There exists no one-one function from $[n]$ to any of its proper subsets.*

Proof. We use PMI to prove this result. For each $n \in$ N, let $P(n)$ be the statement that there exists no one-one function from $[n]$ to any of its proper subsets.

The statement $P(1)$ holds as there exists no one-one function from [1] to ∅. Assume the induction hypothesis that for an $m \in$ N, $P(m)$ holds. We show that $P(m + 1)$ holds.

On the contrary, suppose there exists one-one function $f : [m+ 1] \to A$, where A is a proper subset of $[m + 1]$. We consider two cases depending on whether $m + 1 \in$ rng f or not.

Case 1: $m + 1 \in$ rng f.

(a) If $f(m+1) = m+1$, then the restriction function $f_{[m]}$is a one-one function from $[m]$ to $A\backslash\{m+1\}$, which is a proper subset of $[m]$. This contradicts the induction hypothesis.

(b) If $f(m + 1)$ 6= $m + 1$, then there exist k, ` $\in [m]$ such that $f(k) = m + 1$ and $f(m + 1) =$ `. Define the function $g : [m] \to A \setminus \{m + 1\}$ by

$$g(k) = `, g(x) = f(x) \text{ for } x \ 6= k.$$

Observe that g is one-one and $A \setminus \{m + 1\}$ is a proper subset of $[m]$. This contradicts the induction hypothesis.

Case 2: $m + 1$ 6∈ rng f.

In this case, $f(m + 1) \in [m]$. Then the restriction function $f_{[m]}$is a one-one function from $[m]$ to $A \setminus \{f(m + 1)\}$, which is a proper subset of $[m]$. Again, it contradicts the induction hypothesis.

Hence, there exists no one-one function from $[m + 1]$ to any of its proper subsets so that $P(m +$

1) holds.

As an application of Lemma 3.1.1, we prove the following result.

Lemma 3.1.2. *Let $m, n \in$ N. Then the following are true:*

1. [Injection] *There exists a one-one function from* $[m]$ *to* $[n]$ *if and only if* $m \le n$. *2.*

[Bijection] *There exists a bijection from* $[m]$ *to* $[n]$ *if and only if* $m = n$.

Proof. (1) Suppose $m \le n$. Then the function Id : $[m] \to [n]$ given by Id$(x) = x$ is a one-one function. Conversely, let $f : [m] \to [n]$ be a one-one function. If $m > n$, then $[n]$ is a proper subset of $[m]$. Now, f is one-one function from $[m]$ to a proper subset of $[m]$ contradicting Lemma 3.1.1. Hence $m \le n$.

(2) Assume that $m = n$. Then the identity function on $[n]$, given by Id$(x) = x$ is a bijection. Conversely, suppose that $g : [m] \to [n]$ is a bijection. Then both g and g^{-1}: $[n] \to [m]$ are one-one functions. By (1), $m \le n$ and $n \le m$. Therefore, $m = n$.

Recall that two sets are said to be equinumerous if there is a bijection between them, and that the composition of two bijections is a bijection. Thus, if $m, n \in$ N$,$ m 6= n and A is a set equinumerous with $\{1, 2, . . . , m\}$, then A cannot be equinumerous with $\{1, 2, . . . , n\}$, *i.e.*, such a set A has a definite number of elements. This idea provides a mathematical justification of the fact that if two persons count all English words in this page correctly, then they will arrive at the same number.

Taking cue from the above results, we define the notions of finite sets, infinite sets, and the number of elements, or the cardinality of a finite set as follows.

Definition 3.1.3. 1. A set X is called finite if either $X = \varnothing$ or there exists a bijection from X to $[m]$ for some $m \in$ N; this number m is called the cardinality of X and is denoted by $|X|$. We write $|\varnothing| = 0$.

2. A set which is not finite is called an infinite set.

For instance, $[m]$ is a finite set for any $m \in$ N. Moreover, $|[m]| = m$. For any $m \in$ N, if $a_1, . . . , a_m$ are distinct objects, then $A := \{a_1, . . . , a_m\}$ is a finite set since $f : A \to [m]$ defined by $f(a_j) = j$ is a bijection; and, $|A| = m$.

If N is a finite set, then there is a bijection $f :$ N $\to [n]$ for some $n \in$ N. In that case, the restriction function $f_{[n+1]} : [n + 1] \to [n]$ is one-one. It contradicts Lemma 3.1.1. Therefore, N is an infinite set. We give some characterization of finite and infinite sets, where the requirements are seemingly weaker than those mentioned in their definitions.

Theorem 3.1.4. *1. A nonempty set X is finite if and only if there exists a one-one function $f : X \to [m]$ for some $m \in$ N.*

2. A set X is infinite if and only if there exists a one-one function $f :$ N $\to X$. 3. A set X is infinite

if and only if there exists a bijection from X to one of its proper subsets.

4. A set X is infinite if and only if there exists a one-one function from X to one of its proper subsets.

Proof. (1) Let X be a nonempty set. If X is finite, then there is a bijection $f : A \to [n]$ for some $n \in$ N. Now, f itself is a one-one function.

Conversely, let $g : X \to [m]$ be a one-one function for some $m \in$ N. We show by PMI on m that X is finite. For $m = 1$, if $g : X \to \{1\}$ is one-one, then g is onto, and hence a bijection. So, by definition

X is finite. Assume that the statement is true for $m = k$ and let $g : X \to [k + 1]$ be one-one function. If g is onto, then g is a bijection with $n = k + 1$ so that , *i.e.*, X is equinumerous with $[k + 1]$ and hence by definition, X is finite. So, assume that g is not onto.

If $k + 1$ *6*∈ rng g, then $g : X \to [k]$ is one-one, and the induction hypothesis implies that X is finite. Otherwise, there exist $x_0 \in X$ and ` ≤ $k$ such that $g(x_0) = k + 1$ and ` *6*∈ rng g. Define $h : X \to [k]$ by

(

x_0 `, if $t = x_0$.

$h(t) =$

$g(t)$, if t *6*∈

Then $h : X \to [k]$ is one-one. By the induction hypothesis, X is finite.

(2) Let X be an infinite set. Since X *6*= ∅, there exists at least one element, say, $a_1 \in X$. We show by induction that for each $n \geq 2$, there exists $a_n \in X$ different from $a_1, \ldots, a_{n-1}$. Now that a_1 has been chosen, consider the set $X \setminus \{a_1\}$. If this set is empty, then $X = \{a_1\}$, which is a finite set. As X is infinite, $X \setminus \{a_1\}$ is nonempty. So, let $a_2 \in X \setminus \{a_1\}$. This proves the basis case. So, suppose $a_1, \ldots,$ $a_m \in X$ have been chosen corresponding to the numbers $1, 2, \ldots, m$. The set $X \setminus \{a_1, a_2, \ldots, a_m\}$ is nonempty, since otherwise $X = \{a_1, a_2, \ldots, a_m\}$ would be a finite set. So, let $a_{m+1} \in X \setminus \{a_1, a_2, . .$ $. , a_m\}$. This proves the induction step.

Hence, corresponding to 1, there exists $a_1 \in X$, and for each $n \geq 2$, there exists $a_n \in X$ different from all of $a_1, a_2, \ldots, a_{n-1}$. Define the function $f : \mathrm{N} \to X$ by $f(n) = a_n$. Then f is a one-one function. (Notice that for different choices of a_ns, we get different functions f.)

Conversely, let $f : \mathrm{N} \to X$ be one-one. If X is finite, then there exists a one-one function $g : X \to [m]$ for some $m \in \mathrm{N}$. Then $g \circ f : \mathrm{N} \to [m]$ is one-one. The restriction of $g \circ f$ to $[n + 1]$ is a one-one

function from $[n + 1]$ to $[n]$. It contradicts Lemma 3.1.1. Therefore, X is infinite.

(3) Let X be an infinite set. By (2), there is a one-one function $f : \mathrm{N} \to X$. Now define the function $g :$ $X \to X \setminus \{f(1)\}$ by

(

$g(x) =$ $f(k + 1)$, if $x = f(k)$ for

x, if x *6*∈ rng f some $k \in \mathrm{N}$.

Then g is a bijection. So, we have a bijection from X to one of its proper subsets. Conversely, Let $g :$ $X \to Y$ be a bijection, where Y is a proper subset of X. On the contrary, assume that X is a finite set. Then, there is a bijection $f : X \to [m]$ for some $m \in \mathrm{N}$. Since Y is a proper subset of X, $f(Y)$ is a proper subset of $f(X)$. As $f(X) = [m]$, the function $f \circ g \circ f^{-1}$: $[m] \to f(Y)$ is a bijection from $[m]$ to a proper subset of $[m]$. This contradicts Lemma 3.1.1.

(4) Let X be an infinite set. By (3) there exists a bijection from X to one of its proper subsets. This bijection is itself a one-one function from X to that subset. Conversely, suppose that $h : X \to Y$ is one-one, where Y is a proper subset of X. Let $Z =$ rng h. We see that Z is also a proper subset of X and $h : X \to Z$ is a bijection.

Observe that Theorem 3.1.4.3 implies that a set X is finite if and only if there is no bijection from X to any of its proper subsets, if and only if, there is no one-one function from X to any of its proper subsets.

Exercise 3.1.5.

1. *A subset of a finite set is finite.*

2. *If X and Y are disjoint sets with $|X| = m$ and $|Y| = n$, then $|X \cup Y| = m + n$. In particular, if X and Y are disjoint finite sets, then $X \cup Y$ is finite.*

3. *Let X and Y be finite sets. Then $X \cup Y$ is finite.*

4. *Let X be a nonempty set with $|X| = n$. For any $x \in X$, $|X \setminus \{x\}| = n - 1$. 5. A superset of an infinite set is infinite.*

6. *Let X be an infinite set and let Y be a finite set. Then $X \setminus Y$ is an infinite set.*

7. Let X and Y be nonempty finite sets. Then $|X| \le |Y|$ if and only if there exists a one-one function $f : X \to Y$.

8. Let X and Y be nonempty finite sets. Then $|X| = |Y|$ if and only if there is a bijection from X to Y .

9. *Let X be a finite nonempty set and let α be a fixed symbol. Let $Y = \{(a, \alpha) : a \in X\}$. Then $|X| = |Y|$.*

10. *Let X be a nonempty finite set. Then, for any set Y , $|X| = |X \setminus Y| + |X \cap Y|$. 11. Let X and Y be two finite sets. Then $|X \cup Y| = |X| + |Y| - |X \cap Y|$. 12. Let A and B be finite sets. Show that $A \times B$ is a finite set, and $|A \times B| = |A| \times |B|$. 13. Let $f : A \to B$ be a function, where both A and B are finite sets. If* rng *$f = \{b_1, . . . , b_n\}$ then*

show that $|A| = P^n{}_{j=1}$ $|f^{-1}(b_j)|$. In particular, if $|f^{-1}(b_j)| = k$ for $j = 1, 2,$ . . . , n, then $|A| = nk$.

3.2 Families of sets

In this section, we extend the notation of operations on sets to sets of sets.

Definition 3.2.1. Let I be a set. For each $\alpha \in I$, take a set A_α. The set

$$\{A_\alpha\}_{\alpha \in I} := A_\alpha : \alpha \in I$$

is called a family of sets indexed by elements of I. In this case, the set I is called an index set. The family of sets $\{A_\alpha : \alpha \in I\}$ is called a nonempty family when the index set I is nonempty. Let $\{Y_\alpha\}_{\alpha \in I}$ be a nonempty family of sets. We define the union and intersection of the sets in the family as follows:

1. union : $\cup_{\alpha \in I} Y_\alpha = \{y : y \in Y_\alpha$ for some $\alpha \in I\}$;
2. intersection : $\cap_{\alpha \in I} Y_\alpha = \{y : y \in Y_\alpha$ for all $\alpha \in I\}$.

[Convention] The union of sets in an empty family is $\varnothing$. The intersection of sets in an empty family of subsets of a set S is S.[1]

Unless otherwise mentioned, we assume that the index set for a family of sets is nonempty so that the family is a nonempty family.

Example 3.2.2.

1. Take $A = \{1, 2, 3\}$, $B_1 = \{1, 2\}$, $B_2 = \{2, 3\}$ and $B_3 = \{4, 5\}$. Then the family $\{B_\alpha$:

$$\alpha \in A\} = \{B_1, B_2, B_3\} = \{\{1, 2\}, \{2, 3\}, \{4, 5\}\} .$$

Thus, $\cup$

$_{\alpha\in A}B_\alpha = \{1, 2, 3, 4, 5\}$ and $\cap$

$_{\alpha\in A}B_\alpha = \varnothing$.

[1] Consider the family $\{A_\alpha\}_{\alpha\in I}$, where each A_α is a subset of a set S. Let $x \in S$. If x 6$\in \cap_{\alpha\in I}A_\alpha$, then there exists an $\alpha \in I$ such that x 6$\in A_\alpha$. However, such an α does not exist since I is empty. Therefore, each such $x \in \cap_{\alpha\in I}A_\alpha$.

2. Take $A = \mathrm{N}$ and $B_n = \{n, n + 1, . . .\}$. Then the family

$$\{B_\alpha : \alpha \in A\} = \{B_1, B_2, . . .\} = \{\{1, 2, . . .\}, \{2, 3, . . .\}, . . .\} .$$

Thus, $\cup$

$_{\alpha\in A}B_\alpha = \mathrm{N}$ and $\cap$

3. Verify that T $_{n\in \mathrm{N}}$ $[-\frac{1}{n}, \frac{2}{n}] = \{0\}$. $\quad$ $_{\alpha\in A}B_\alpha = \varnothing$.

Proposition 3.2.3. *Let $\{A_\alpha\}_{\alpha\in I}$ be a nonempty family of subsets of X and let B be any set. For any subset Y of X, write $Y^c = X \setminus Y$. Then*

1. $B \cup$ 2. $\cap_{\alpha\in I}A_\alpha$ $\quad$ $\cup A_\alpha$),

$\cup_{\alpha\in I}A_\alpha$ $\quad$ $= \cup_{\alpha\in I}(B$

$B \cap$ $\quad$ $\cap A_\alpha$),

$= \cap_{\alpha\in I}(B$

3. 4. $\cap_{\alpha\in I}A^c$

$_\alpha$, *and*

c
=

$\cup_{\alpha\in I}A_\alpha$

$\cap_{\alpha\in I}A_\alpha$ $\quad$ $\cup_{\alpha\in I}A^c$

c $\quad$ $_\alpha$.
=

Proof. (1) Let $x \in B \cup$ $\cap_{\alpha\in I}A_\alpha$. Then $x \in B$ or $x \in \cap_{\alpha\in I}A_\alpha$. If $x \in B$, then $x \in B \cup A_\alpha$ for each $\alpha \in I$. So, $x \in \cap_{\alpha\in I}(B \cup A_\alpha)$. If $x \in \cap_{\alpha\in I}A_\alpha$, then for each $\alpha \in I$, $x \in A_\alpha$ so that $x \in B \cup A_\alpha$. Then $x \in \cap_{\alpha\in I}(B \cup A_\alpha)$. In any case, $x \in \cap_{\alpha\in I}(B \cup A_\alpha)$.

Conversely, suppose $x \in \cap_{\alpha\in I}(B \cup A_\alpha)$. Then for each $\alpha \in I$, $x \in B \cup A_\alpha$. If $x \in B$, then $x \in B \cup$ $\cap_{\alpha\in I}A_\alpha$. If x 6$\in B$ but $x \in B \cup A_\alpha$ for each $\alpha \in I$, then $x \in A_\alpha$ for each $\alpha \in I$. So that $x \in \cap_{\alpha\in I}A_\alpha$. Then $x \in B \cup$ $\cap_{\alpha\in I}A_\alpha$.

(3) Notice that both the sets are subsets of X. So, let $x \in X$. Now,

$x \in$ $\cup_{\alpha\in I}A_\alpha$ *c* $\Leftrightarrow x$ 6$\in \cup_{\alpha\in I}A_\alpha \Leftrightarrow$ for each α $\in I$, x 6$\in A_\alpha \Leftrightarrow$ for each $\alpha \in I$, $x \in A^c{}_\alpha \Leftrightarrow x \in \cap_{\alpha\in I}A^c{}_\alpha$.

Proof of (2) and (4) are similar to those of (1) and (3), respectively.

Practice 3.2.4.

1. Consider $A_x\}_{x\in \mathrm{R}}$*, where* $A_x = [x, x + 1]$*. What is* $\cup_{x\in \mathrm{R}}A_x$ *and* $\cap_{x\in \mathrm{R}}A_x$*?*

2. For $x \in [0, 1]$ *write* $Zx := \{zx : z \in Z\}$ *and* $A_x = \mathrm{R} \setminus Zx$*. What is* $\cup$

$_{x\in[0,\, 1]}A_x$ *and* $\cap$

$_{x\in[0,\, 1]}A_x$*?*

3. Write the closed interval $[1, 2]$ *as* $\cap$

$_{n\in \mathrm{N}}I_n$ *for suitable open intervals* I_n*.*

Proposition 3.2.5. *Let X and Y be nonempty sets and let f be a relation from X to Y . Let* $\{A_\alpha\}_{\alpha\in I}$ *be a family of subsets of X. Then*

$$f\cup_{\alpha\in I}A_\alpha = \cup_{\alpha\in I}f(A_\alpha) \text{ and } f\cap_{\alpha\in I}A_\alpha \subseteq \cap_{\alpha\in I}f(A_\alpha).$$

Proof. For the equality,

$$y \in f\cup_{\alpha\in I}A_\alpha \Leftrightarrow (x, y) \in f \text{ for some } x \in \cup_{\alpha\in I}A_\alpha \Leftrightarrow (x, y) \in f \text{ where } x \in A_\alpha \text{ for some } \alpha \in I \Leftrightarrow y \in f(A_\alpha) \text{ for some } \alpha \in I \Leftrightarrow y \in \cup_{\alpha\in I}f(A_\alpha).$$

For the containment, the case $\cap_{\alpha\in I}A_\alpha = \varnothing$ is obvious. So, assume that $\cap_{\alpha\in I}A_\alpha$ 6= $\varnothing$. Then

$$y \in f\cap_{\alpha\in I}A_\alpha \Leftrightarrow (x, y) \in f \text{ for some } x \in \cap_{\alpha\in I}A_\alpha \Leftrightarrow (x, y) \in f \text{ with } x \in A_\alpha \text{ for all } \alpha \in I \Rightarrow y \in f(A_\alpha) \text{ for all } \alpha \in I \Leftrightarrow y \in \cap_{\alpha\in I}f(A_\alpha).$$

Remark 3.2.6. Observe that in the proof of the containment in Proposition 3.2.5, if $y \in f(A_\alpha)$ for each $\alpha \in I$, then for each $\alpha \in I$, we can find some $x_\alpha \in A_\alpha$ such that $(x_\alpha, y) \in f$. However, such an x_α need not be the same for each α. Thus the containment need not be an equality. To see that it is indeed the case, consider the function $f : \{1, 2, 3, 4\} \to \{a, b\}$ where $f = \{(1, a),(2, a),(2, b),(3, b),(4, b)\}$. Take $A_1 = \{1, 3\}$ and $A_2 = \{1, 2, 4\}$ and verify that $f(A_1 \cap A_2)$ 6= $f(A_1) \cap f(A_2)$.

To define the product of sets in a family, we first rewrite the product of two sets in an equivalent way. Let A_1 and A_2 be nonempty sets and let $a_1 \in A_1$, $a_2 \in A_2$. The ordered pair (a_1, a_2) may be thought of as the function $f : \{1, 2\} \to A_1 \cup A_2$ with $f(1) = a_1$ and $f(2) = a_2$. Therefore, $A_1 \times A_2$ is identified with the set of all functions $f : \{1, 2\} \to A_1 \cup A_2$ with $f(1) \in A_1$ and $f(2) \in A_2$. Generalizing this observation leads to the following definition.

Definition 3.2.7. Let $\{A_\alpha\}_{\alpha\in I}$ be a nonempty family of sets. Assume that A_α is nonempty for each $\alpha \in I$. The product of the sets in the family is defined as

Y

$A_\alpha = f : f$ is a function from I to $\cup_{\alpha\in I}A_\alpha$ with $f(\alpha) \in A_\alpha$ for each $\alpha \in I$. $\alpha\in I$

In case $A_\alpha = \varnothing$ for some $\alpha \in I$, $A_\alpha := \varnothing$.

we define the product Q $\alpha\in I$

Example 3.2.8. Take $I = \mathrm{N}$ and $A_\alpha = \{0, 1\}$ for each A_α is the set of

$\alpha \in \mathrm{N}$. Then the product Q $\alpha\in I$

all functions $f : \mathrm{N} \to \{0, 1\}$. In other words, the product is the set of all 0-1 sequences.

Exercise 3.2.9.

1. Write R *as a union of infinite number of pairwise disjoint infinite sets.*

2. Write the set $\{1, 2, 3, 4\}$ *as the intersection of infinite number of infinite sets.*

3. Prove Parts 2 and 4 of Proposition 3.2.3.

4. *Let $f : X \to Y$ be a partial function, $A \subseteq X$, $B \subseteq Y$ and let $\{B_\beta\}_{\beta\in I}$ be a nonempty family of subsets of Y. Show the following.*

   (a) $f^{-1}\cap_{\beta\in I}B_\beta = \cap_{\beta\in I}f^{-1}(B_\beta)$.

   (b) $f^{-1}(B^c) = \mathrm{dom}\, f \setminus f^{-1}(B)$.

   (c) $ff^{-1}(B) \cap A = B \cap f(A)$.

   (d) $f^{-1} \cup_{\beta\in I}B_\beta = \cup_{\beta\in I}f^{-1}(B_\beta)$.

   Also, show that in (a)-(c), equality may fail if f is a relation but not a partial function. Observe that (d) is a special case of Proposition 3.2.5.

5. *Let $f : X \to Y$ be a one-one function and let $\{A_\alpha\}_{\alpha\in I}$ be a nonempty family of subsets of X. Is it true that $f\cap_{\alpha\in I}A_\alpha = \cap_{\alpha\in I}f(A_\alpha)$?*

6. *Show that each set can be written as a union of finite sets.*

7. *Give an example of an equivalence relation on* N *for which there are* 7 *equivalence classes, out of which exactly* 5 *are infinite.*

8. *Show that the union of finitely many finite sets is a finite set.*

9. *Let $I = A_1 = A_2 = A_3 = \{1, 2, 3\}$. Is the set* $\mathrm{Q}_{\alpha\in I} A_\alpha$ *equal to the set of all functions from {1, 2, 3} to {1, 2, 3}? Give reasons for your answer.*

10. *Give sets A_n, $n \in$* N, *such that* $\mathrm{Q}_{\underline{n\in \mathrm{N}}} A_n$ *has* 6 *elements. Give another.*[1]

[1] When we ask for more than one example, we encourage the reader to get examples of different types, if possible.

3.3 Constructing bijections

Though we have discussed criteria for classifying a set as finite or infinite through injections, the definitions demand creating bijections. If $f : X \to Y$ is one-one, then $f : X \to \mathrm{rng}\, f$ is a bijection. Besides this, we now discuss some general techniques to create bijections.

Experiment 1: Make a horizontal list of the elements of N using only dots instead of writing the numbers themselves. Also write Z using dots horizontally below the list for N. Draw arrows connecting the dots on the top list to dots on the bottom list to supply a bijection from N to Z. Can you supply another bijection by changing the arrows?

Experiment 2: Consider an open interval (a, b). Its center is $c = \frac{a+b}{2}$, length is ` $= b - a$, and the distance of the center from each end-point is $\frac{`}{2}$. View the open interval as a line segment on the real line. Stretch (a, b) uniformly without disturbing the center and make its length equal to L. Use this information to answer the following:

1. Where is c now (in R)?
2. Where is $c - \frac{l}{2}$?
3. Where is $c + \frac{l}{2}$?
4. Where is $c - \alpha \times \frac{l}{2}$, for a fixed $\alpha \in (-1, 1)$?

   Using these information, find a bijection from (a, b) to (s, t). [Hint: First, fix the center.]

Practice 3.3.1.

1. *Construct two bijections from* $(1, \infty)$ *to* $(5, \infty)$.
2. *Construct two bijections from* $(0, 1)$ *to* $(1, \infty)$.
3. *Construct two bijections from* $(-1, 1)$ *to* $(-\infty, \infty)$.
4. *Construct two bijections from* $(0, 1)$ *to* R.
5. *Construct two bijections from* $(0, 1) \times (0, 1)$ *to* R × R.

Experiment 3: Let $P = (0, 1)$, $T = (3, 5)$ and $f : P \to T$ be a bijection. Imagine elements of P as 'persons' and elements of T as 'seats' in a train. So, f assigns a seat to each person and the train is full.

1. Now suppose a new person 0 is arriving. He wants a seat. To manage it, let us un-seat two persons $\frac{1}{2}, \frac{1}{3}$. So, two seats $f(\frac{1}{2})$, $f(\frac{1}{3})$ are vacant. But we have 3 persons to take those seats. Giving each person a seat is not possible.
2. Suppose that we un-seat $\frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{30}$? Can we manage it?
3. Suppose that we un-seat $\frac{1}{2}, \frac{1}{3}, \cdots$? Can we manage it now?
4. What do we do if we had two new persons arriving? Fifty new persons arriving? A set $\{a_1, a_2, \cdots\}$ of new persons arriving?

It leads to the following result, which you can prove easily.

Theorem 3.3.2. [Train Seat Argument] *Let X be a set with $\{a_1, a_2, \ldots, \} \subseteq X$ and let $f : X \to Y$ be a bijection.*

1. If $c_1, \ldots, c_k$ are distinct objects not in X, then the function

$$h(x) = f(x) \text{ if } x \in X \setminus \{a_1, a_2, \ldots\}$$

$$f(a_{i+k}) \text{ if } x = a_i,\ i \in \mathbb{N}$$

$$f(a_i) \text{ if } x = c_i,\ i = 1, 2, \ldots, k$$

is a bijection from $X \cup \{c_1, \ldots, c_k\}$ to Y.

2. If $c_1, c_2, \ldots$ are distinct objects not in X, then the function

$h(x) = f(x)$ *if* $x \in X \setminus \{a_1, a_2, . . .\}$

$f(a_{2n-1})$ *if* $x = a_n$, $n \in$ N

$f(a_{2n})$ *if* $x = c_n$, $n \in$ N

is a bijection from $X \cup \{c_1, c_2, . . .\}$ *to* Y.

Example 3.3.3. In each of the following cases, give a bijection from X to Y :

1. $X = [0, 1)$ and $Y = (0, 1)$.

Ans: Map $\{0, 1/2, 1/3, . . .\}$ onto $\{1/2, 1/3, . . .\}$ and each of the rest to itself. That is, define

$1/(n + 1)$ if $x = 1/n$ with $n \in \{2, 3,$

$f : X \to Y$ by $f(x) =$

$. . .\}$

x if x 6∈ $\{1/2, 1/3, 1/4, \cdots\}$.

$1/2$ if $x = 0$

2. $X = (0, 1)$ and $Y =$ R \
N.

Ans: $f : X \to$ R given by $f(x) = \tan(\pi(x - 1/2))$ is a bijection. Define $g :$ R $\to Y$ by

$\in$ N $\cup$ $\{0\}$

x if $x \in$ R \ $-2x + 1$ if $-$

$g(x) =$

Z $-2x$ if x $\quad x \in$ N.

That is, g maps each x in R\Z to itself by the identity map, and then it maps $0, -1, 1, -2, 2, -3, 3, . . .$ to $0, -1, -2, -3, -4, -5, -6, . . .$ in that order. Clearly, g is a bijection. Hence $g \circ f : X \to Y$ is a bijection.

Exercise 3.3.4. *In each of the following, use Theorem 3.3.2 to give a bijection from X to Y . 1.*

$X = [0, 1]$ *and* $Y = (0, 1)$.

2. $X = (0, 1) \cup \{1, 2, 3, 4\}$ *and* $Y = (0, 1)$.

3. $X = (0, 1) \cup$ N *and* $Y = (0, 1)$.

4. $X = [0, 1]$ *and* $Y = [0, 1] \setminus \{^1{}_1,^1{}_3,^1{}_5, \cdots\}$.

5. $X =$ R *and* $Y =$ R \ N.

6. $X = [0, 1]$ *and* $Y =$ R \ N.

7. $X = (0, 1)$ *and* $Y = (1, 2) \cup (3, 4)$.

8. $X =$ R \ Z *and* $Y =$ R \ N.

3.4 Cantor-Schr¨oder-Bernstein Theorem

Let A and B be finite sets with $|A| = m$ and $|B| = n$. Suppose there exists a one-one function from A to B. Then we know that $m \leq n$. In addition, if there exists a one-one function from B to A, then $n \leq$

m so that $m = n$. It then follows that there is a bijection from *A* to *B*. Does the same result hold good for infinite sets? That is, given one-one functions $f : A \to B$ and $g : B \to A$ does there exist a bijection from *A* to *B*?

Experiment : *Creating a Bijection from Injections*
Let $X = Y =$ N. Take one-one functions $f : X \to Y$ and $g : Y \to X$ defined by $f(x) = x + 2$ and $g(x) = x + 1$. In the picture, we have *X* on the left and *Y* on the right. If $(x, y) \in f$, we draw a solid line joining *x* and *y*. If $(y, x) \in g$, we draw a dotted line joining *y* and *x*.

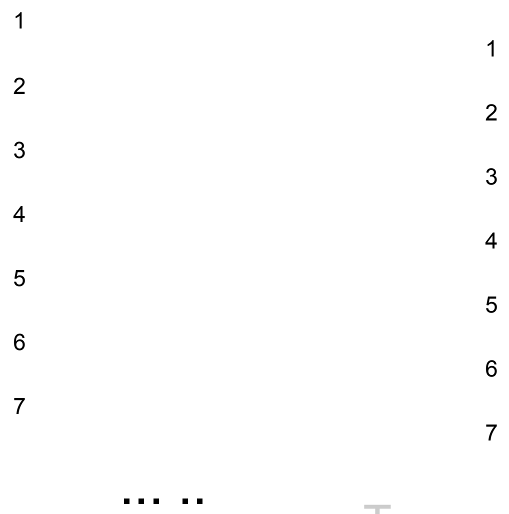

Figure 3.1: Graphic representation of functions *f* and *g*

We want to create a bijection *h* from *X* to *Y* by erasing some of these lines. Initially, we keep all solid lines and look at rng *f*. Since *f* is not an onto function, there are elements in $Y \setminus$ rng *f*. Each one of these elements must be connected by a dotted line to some element in *X*. So, we keep all those pairs $(y, x) \in g$ such that *y 6*∈ rng *f*. We follow the heuristic of keeping as many pairs in *f* as possible; and then keep a pair $(y, x) \in g$ if no pair $(z, y) \in f$ has been kept.

1. The elements $1, 2 \in Y$ but are not in rng *f*. So, the dotted lines connecting them to elements in *X* must stay. That is, the pairs $(1, 2),(2, 3) \in g$ must be kept.
2. Then the pairs $(2, 4),(3, 5) \in f$ must be deleted.
3. Now, $(1, 3) \in f$; it is kept, and then $(3, 4) \in g$ must be deleted.
4. The pair $(4, 5) \in g$ is kept; so $(5, 7) \in f$ must be deleted.
5. The pair $(4, 6) \in f$ is kept, and then $(6, 7) \in g$ must be deleted.
6. The pair $(7, 8) \in g$ is kept; so $(8, 10) \in f$ must be deleted.

Continue this scheme to realize what is happening. Then the bijection $h : X \to Y$ is given by

$$h(x) = \begin{array}{l} f(x) \text{ if } x = 3n \;\; \text{otherwise.} \\ -2, n \in \text{N} \\ g^{-1}(x) \end{array}$$

Practice 3.4.1. *Construct bijections using the given injections* $f :$ N → N *and* $g :$ N → N*. 1.*

$f(x) = x + 1$ *and* $g(x) = x + 2$.

2. $f(x) = x + 1$ *and* $g(x) = x + 3$.

3. $f(x) = x + 1$ and $g(x) = 2x$.

We use this heuristic method of constructing a bijection in proving the following theorem.

Theorem 3.4.2. [Cantor-Schr¨oder-Bernstein (CSB)] *Let X and Y be nonempty sets and let $f : X \to Y$ and $g : Y \to X$ be one-one functions. Then there exists a bijection $h : X \to Y$.*

Proof. If f is onto, then f itself is a bijection. So, assume that f is not onto. Then $f(X)$ is a proper subset of Y . Write $B = Y \setminus f(X)$, $\varphi = f \circ g$, and $A = B \cup \varphi(B) \cup \varphi^2(B) \cup \cdots = B \cup^{\infty} \cup_{n=1}\varphi^n(B)$. Then $A \subseteq Y$ and

$$\varphi(A) = \varphi(B) \cup^{\infty} \cup_{n=2}\varphi^n(B) =^{\infty} \cup_{n=1}\varphi^n(B).$$

Hence $A = B \cup \varphi(A)$. Notice that $f(X) = Y \setminus B$, $\varphi(A) = f(g(A)) \subseteq Y$, and f is one-one. Hence $f(X \setminus$

$$g(A)) = f(X) \setminus f(g(A)) = [Y \setminus B] \setminus \varphi(A) = Y \setminus [B \cup \varphi(A)] = Y \setminus A.$$

Thus, the restriction of f to $X \setminus g(A)$ is a bijection onto $Y \setminus A$. As g is one-one, its restriction to A is a bijection onto $g(A)$. That is, g^{-1}: $g(A) \to A$ is a bijection. Therefore, the function $h : X \to Y$

defined by $f(x)$, if $x \in X \setminus g(A)$, $g^{-1}(x)$, if $x \in$
$g(A)$

$h(x) =$

is a bijection.

(

Alternate. If g is onto, we have nothing to prove. So, assume that g is not onto. Then $O := X \setminus g(Y)$ 6= ∅. Write $\psi = g \circ f$ and $E = O \cup \psi(O) \cup \psi^2(O) \cup \cdots = O \cup^{\infty} \cup_{n=1}\psi^n(O)$. Observe that $O \subseteq E \subseteq X$, $\psi : X \to X$ is one-one, and g does not map any element of Y to any element of O. Hence

$=^{\infty} \cup_{n=1}\psi^n(O) = E \setminus O.$

$\psi(E) = \psi$

$O \cup^{\infty} \cup_{n=1}\psi^n(O)$

Thus the restriction of ψ to E is a bijection from E onto $E \setminus O$. Define the function $\tau : X \to X \setminus O$ by (

$\tau(x) =$ $\psi(x)$, if $x \in E$.
x, if $x \in X \setminus E$,

Then τ is a bijection. Write $h := \tau^{-1} \circ g$. Then h is one-one and $h(Y) = \tau^{-1}(g(Y)) = \tau^{-1}(X \setminus O) = X$. Therefore, h is a bijection from Y to X.

Alternate. Consider the family $F = \{T \subseteq X : g(f(T)^c) \subseteq T^c\}$ of subsets of X. Here, $T^c = X \setminus T$ and $f(T)^c = Y \setminus f(T)$.

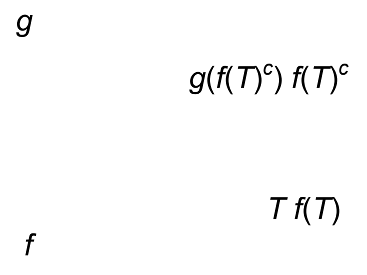

Figure 3.2: Depiction of CSB-theorem

Note that $\varnothing \in F$. Put $U = \cup$

$gf(U)^{c} = g\ f\cup$ $\quad {}_{T\in F}T$. Then

$\quad {}_{T\in F}T\ {}^{c} = g\ \cup$

$\quad {}_{T\in F}f(T)\ {}^{c} = g\ \cap$

$\quad {}_{T\in F}f(T)^{c} = \cap$

$\quad {}_{T\in F}g\,(f\,(T)^{c}) \subseteq \cap$

$\quad {}_{T\in F}T^{c} = U^{c}.$

Thus, $U \in F$; and hence U is the maximal element of F. Now that $g\,(f(U)^{c}) \subseteq U^{c}$, we want to show that $g\,(f(U)^{c}) = U^{c}$. On the contrary, assume that $U^{c}\ 6{=}\ g\,(f(U)^{c})$. Then we have an element $x \in U^{c} \setminus$

$g\,(f(U)^{c})$. Write $V = U \cup \{x\}$. Then $gf(U)^{c} \subseteq U^{c} \cap \{x\}^{c}$ and $f(U) \subseteq f(V\,)$. Thus,

$f(V\,)^{c} \subseteq f(U)^{c}$ and

$gf(V\,)^{c} \subseteq gf(U)^{c} \subseteq U^{c} \cap \{x\}^{c} = V^{c}.$

This contradicts the maximality of U in F. So, $gf(U)^{c} = U^{c}$. Hence f is a bijection from U to $f(U)$ and g is a bijection from $f(U)^{c}$to U^{c}. Define $h : X \to Y$ by

(

$f(x)$ if $x \in U,$

$h(x) =$

$g^{-1}(x)$ if $x\ 6{\in}\ U.$

Then h is a bijection.

We apply CSB-theorem to prove the following important result. Also, we give different proofs of this fact.

Theorem 3.4.3. *The set* N × N *is equinumerous with* N.

Proof. We already know that the function f : N → N×N given by $f(n) = (n,\ 1)$ is one-one. Define the function g : N × N → N by $g(m,\ n) = 2^{m}3^{n}$. Note that $g(m,\ n) = g(r,\ s)$, implies that $2^{m-r} = 3^{s-n}$. Since one is a power of 2 and the other is a power of 3, their equality ensures that the indices are 0. Hence $m = r$ and $s = n$; that is, $(m,\ n) = (r,\ s)$, and thus f is one-one. By CSB-theorem, there exists a bijection from N × N to N.

Alternate. Define the function h : N × N → N by $h(x,\ y) = 2^{x-1}(2y - 1)$. Suppose $h(x,\ y) = h(m,\ n)$. Then, $2^{x-1}(2y - 1) = 2^{m-1}(2n - 1)$. Let $x > m$. Then $2^{x-m}(2y - 1) = 2n - 1$ implies that the left hand side is an even number whereas the right hand side is an odd number; this is a contradiction. Similarly, $x < m$ leads to a contradiction. Hence $x = m$. Then the equality implies $2y - 1 = 2n - 1$ so that $y = n$. Thus, $(x,\ y) = (m,\ n)$ and hence h is a one-one function. Further, each $x \in$ N can be uniquely written as $x = 2^{r-1}(2n - 1)$, for some $r,\ n \geq 1$. So, h is an onto function.

Alternate. Define f : N × N → N by $f(m,\ n) = (m + n - 1)(m + n - 2)/2 + n$. Since $m \geq 1$, $n \geq 1$, $(m + n - 1)(m + n - 2)/2 + n \geq 1$. Hence f is well defined. Write $S_0 = 0$; and for any $r \in$ N, write $1 + 2 + \cdots + r = S_r$. Notice that $f(m,\ n) = S_{m+n-2} + n$. In Example 2.3.1.2, we have shown that corresponding to each $x \in$ N, there exists a unique $t \in$ N∪ $\{0\}$ such that $S_t < x \leq S_{t+1}$. The existence of such a t shows that f is onto, and its uniqueness shows that f is one-one. The details are as follows.

Suppose f(k, `) = f(m, n) for some choice of k, `, m, n ∈ N, *i.e.*, $x := S_{k+`-2} + ` = S_{m+n-2} + n$. Since $` \le k + ` - 1$ and $n \le m + n - 1$, we have $S_{k+`-2} < x \le S_{k+`-1}$ and $S_{m+n-2} < x \le S_{m+n-1}$. By the uniqueness of *t* corresponding to *x* it follows that $k+`-2 = m+n-2$. Therefore $S_{k+`-2} = S_{m+n-2}$ and $` = x - S_{k+`-2} = x - S_{m+n-2} = n$. This, along with $k + ` - 2 = m + n - 2$ implies that $k = m$. Hence, (k, `) = (m, n) and consequently, *f* is one-one.

To show that *f* is onto, let x ∈ N. Then there exists t ∈ N such that $S_t < x \le S_{t+1}$. Take $n = x - S_t$. The inequality $S_t < x \le S_{t+1}$ implies that $1 \le n \le t + 1$. So, take $m = t + 2 - n$. Then note that for *m, n* chosen as above $m \ge 1$, $n \ge 1$, $t = m+n-2$ and $f(m, n) = S_{m+n-2}+n = S_t+n = x$. Therefore, *f* is an onto function.

The function f(m, n) in the above proof is called *Cantor's pairing function*. Till now it is not known whether there exists another polynomial in *m* and *n* which is a bijection.

Example 3.4.4. We show that Q is equinumerous with N. For this, write $Q = Q^+ \cup Q^- \cup \{0\}$, where

$$Q^+ = {}^{\mathrm{n}m} \; n : m, n \in N, \gcd(m, n) = 1^{\mathrm{o}}, \; Q^- = \{-x : x \in Q^+\}.$$

1. Prove that Q^+ is equinumerous with N.

   Proof. Let $p_1, p_2, \ldots$ be the infinite list of prime numbers arranged in an increasing order, that is, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. The *prime factorization theorem* asserts that each n ∈ N can be written uniquely as $n = p^{a_1}$

   $_1p^{a_2}$

   $_2 \cdots$, where $a_i \in N$ only for a finite number of p_i's, and the rest of a_i's are 0. Hence each $q \in Q^+$ can be written uniquely as $q = p^{b_1}{}_1p^{b_2}$

   $_2 \cdots$, where $b_i \in Z \setminus \{0\}$ only for a finite number of p_i's, and the rest of b_i's are 0. Let $f : N \to Z$ be a bijection such as $f(n) = -n/2$ if *n* is even, and $f(n) = (n + 1)/2$ if *n* is odd. Define $g : N \to Q^+$ by $g(n) = p^{f(a_1)}$

   $_1p^{f(a_2)}$

   $_2 \cdots$ for $n = p^{a_1}$

   $_1p^{a_2}$

   $_2 \cdots$. Then *g* is a bijection.

2. Use the above to conclude that Q^- is equinumerous with N.

   Ans: The function $h : Q^+ \to Q^-$ given by $h(q) = -q$ is a bijection. Using Part 1, we see that $h \circ g : N \to Q^-$ is a bijection.

3. Use the above two parts to conclude that Q is equinumerous with N.

   Ans: Let $A = \{2n : n \in N\}$, $B = \{2n + 1 : n \in N\}$. Then $N = A \cup B \cup \{1\}$. Define $\varphi_1 : A \to N$ by $\varphi_1(n) = n/2$, and $\varphi_2 : B \to N$ by $\varphi_2(n) = (n - 1)/2$. Let $g : N \to Q^+$ and $h : Q^+ \to Q^-$ be the bijections given in Parts 1 and 2. Then $g \circ \varphi_1$ is a bijection from *A* to Q^+, and $h \circ g \circ \varphi_2$ is

a bijection from *B* to Q^-. We see that the following function $\psi : N \to Q$ is a bijection:

$(g \circ \varphi_1)(x)$ if $x \in A$

$(h \circ g \circ \varphi_2)(x)$ if $x \in B$

0 if $x = 1$.

Exercise 3.4.5.

$\psi(x) =$

1. *For each of the exercises in Exercise 3.3.4, give injections. Then use the CSB-theorem to prove that all the sets are equinumerous.*

2. *Define* $f : \mathrm{Q} \to \mathrm{N}$ *by*

0*,* $s > 0$ 5^r3^s*if* $x = \frac{-r}{s}$*,* gcd(r,

s) = 1*,* $r > 0$*,* $s > 0$

$f(x) =$

1 *if* $x = 0$.

2^r3^s*if* $x = \frac{r}{s}$*,* gcd(r, s) = 1*,* $r >$

Show that f is one-one. Apply CSB-theorem to prove that Q *is equinumerous with* N*.*

3. *Let* $X = \{(x, y) \in \mathrm{N} \times \mathrm{N} : y \le x\}$*.*

(a) Define a function $f : \mathrm{N} \times \mathrm{N} \to X$ *by* $f(x, y) = (x + y - 1, y)$*. Prove that f is a bijection. (b) Further, define* $g : X \to \mathrm{N}$ *by* $g(x, y) = {}^{x(x-1)}$

$_{2} + y$*. Prove that g is a bijection.*

Note that $g \circ f$ *is a bijection from* N × N *to* N*. Is this function the same as Cantor's pairing function?*

3.5 Countable and uncountable sets

As we have seen N × N and Q are equinumerous with N. By induction it follows that N^k, that is the product of N with itself taken k times, for any natural number k, is also equinumerous with N. Does it mean that every infinite set is equinumerous with N? With the hope of discovering an answer to this question, we introduce some related notions.

Definition 3.5.1. 1. A set which is equinumerous with N is called a denumerable set. A denumerable set is also called a countably infinite set.

2. A set which is either finite or denumerable is called a countable set.

3. A set which is not countable is called an uncountable set.

Since the identity function on N is a bijection, it follows that N is denumerable. Each finite set such as ∅ and [m], for some $m \in \mathrm{N}$, are countable; so is N.

Example 3.5.2.

1. Define $f : \mathrm{N} \to \mathrm{Z}$ and $g : \mathrm{Z} \to \mathrm{N}$, respectively by

$-x/2$ if x is odd*,* negative $1 + $e*.*

$f(x) =$ even ($x -$ $-2z$ if z is $2z$ if z is

$1)/2$ if x is $g(x) =$ non-negativ

Then, we see that $g \circ f$ and $f \circ g$ are identity functions on their respective domains. Hence f is a bijection. Therefore, Z is denumerable; and also countable.

2. By Theorem 3.4.3, there is a bijection from N × N onto N. Thus, N × N is denumerable, and countable.

3. By Example 3.4.4, Q^+, Q^-, Q are denumerable, and countable.

Before exploring other examples, we will give simpler characterizations of these notions.

Theorem 3.5.3. *Let X be a nonempty set.*

1. X is countable if and only if there exists a one-one function $f : X \to N$.

2. X is denumerable if and only if there exist one-one functions $f : X \to N$ *and* $g : N \to X$.

Proof. 1. Let X be a countable set. If X is finite, then there exists a bijection $f : X \to [m]$ for some $m \in N$. This bijection gives a one-one function $f : X \to N$. Else, X is denumerable, so that there is a bijection $g : X \to N$. In this case, the function g is one-one. Conversely, suppose there exists a one-one function $f : X \to N$. If X is finite, then it is countable. So, suppose that X is infinite. Then, by Theorem 3.1.4.2, there exists a one-one function $g : N \to X$. By CSB-theorem, there exists a bijection $h : X \to N$. Hence X is denumerable; thus countable.

2. Let X be a denumerable set. By definition there is a bijection $f : X \to N$. Thus, $f : X \to N$ and f^{-1}: N $\to X$ are one-one functions. Conversely, suppose there exist one-one functions $f : X \to N$ and g : N $\to X$. Then, by CSB-theorem, there exists a bijection $h : X \to N$. Hence X is denumerable.

Definition 3.5.4.

1. Let X be a denumerable set. Then, there is a bijection $f : N \to X$. So, we can list all the elements of X as $f(1)$, $f(2)$, ... This list is called an enumeration of the elements of X.

2. Let X be a nonempty set. An infinite sequence of elements of X is a function $f : N \to X$. Writing $f(i) = x_i$, such a sequence is represented by $x_{i\ i \in N} = x_1, x_2, \ldots$, where $x_i \in X$.

In the proof of Theorem 1, Part 2, we have essentially extracted an infinite sequence from the infinite set X.

Since Z is denumerable, its elements can be enumerated. For example, 0, 1, −1, 2, −2, 3, −3, . . . is an enumeration of Z. Similarly, all rational numbers can be enumerated; and sometimes we write such an enumeration of Q by $r_1, r_2, r_3, \ldots$. It says that there is a sequence $r_1, r_2, r_3, \ldots$) in which each rational number occurs exactly once. This is what an enumeration means. If X is a countable set, then its elements can be enumerated in a sequence; but the sequence can be finite or infinite.

By a denumerable family of sets, we mean a family of sets which is denumerable. A denumerable family of sets can be indexed by N and we may write such a family as $\{A_i\}_{i \in N}$. We also use the same notation for a countable family, where possibly only a finite number of sets A_i are nonempty. The union of sets in a countable family will be referred to as *a countable union* of sets.

Notice that a countable infinite set is denumerable. Besides this, some more facts about countable sets are listed in the following proposition.

Proposition 3.5.5. [Facts about countable sets]

1. Each subset of a denumerable set is countable.

2. Each infinite subset of a denumerable set is denumerable.

3. A set is infinite if and only if it has a denumerable subset.

4. Any subset of a countable set is countable; and any superset of an uncountable set is uncountable. 5. A countable union of countable sets is countable.

6. For any $k \in N$, *the Cartesian product* N^k *is denumerable.*

7. A finite product of countable sets is countable.

Proof. (1) Let $X \subseteq Y$, where Y is denumerable. There exists a bijection $f : Y \to$ N. The identity function Id : $X \to Y$ is one-one. So, $f \circ$ Id : $X \to$ N is one-one.

(2) Let X be an infinite subset of a denumerable set. By (1), X is countable. So, X is countably infinite, same as denumerable.

(3) Let X be an infinite set. Then, by Theorem 3.5.3, there is a one-one function f : N $\to X$. Thus, f : N $\to$ rng f is a bijection. Hence, rng f is a denumerable subset of X.

Conversely, let X be a set and let $Y \subseteq X$ be denumerable. There exists a bijection $f : Y \to$ N. The function f^{-1}: N $\to X$ is one-one. By Theorem 3.1.4, X is an infinite set.

(4) Let X be a countable set and let $Y \subseteq X$. If $Y = \varnothing$, then it is finite, thus countable. So, suppose that Y 6= $\varnothing$. As X is countable, by Theorem 3.5.3, there exists a one-one function $f : X \to$ N. The restriction of f to Y is also a one-one function from Y to N. Hence Y is countable.

Let X be an uncountable set and let $Y \supseteq X$. If X is countable, then by what we have just proved, X would be countable. Hence, Y is uncountable.

(5) Let $\{A_i\}_{i\in \mathrm{N}}$ be a countable family of sets, where each $A_i$is a countable set. Write $X = \cup_{i\in \mathrm{N}} A_i$. We show that X is countable.

If X is finite, then it is countable. So, let X be infinite. By Theorem 3.1.4.2, there is a one-one function f : N $\to X$. Now, let $x \in X$. Then, there exists at least one $i \in$ N such that $x \in A_i$. Further, since $A_i$is countable, we may assume that A_i has been enumerated. So, suppose x appears at the kth position in this enumeration of A_i. Thus, corresponding to each $x \in X$, we have a unique pair (i, k) of natural numbers. Define $g : X \to$ N by $g(x) = 2^i 3^k$, where i is the smallest natural number for which $x \in A_i$ and x appears at the k-th position in the enumeration of A_i. Then g is one-one. Therefore, by

CSB-theorem, A is equinumerous with N.

(6) For $k = 1$, the result is obvious. Suppose the result is true for $k = m$. That is, there exists a bijection f : N$^m \to$ N. From Theorem 3.4.3, we have a bijection g : N × N $\to$ N. Define h : N$^{m+1} \to$ N by $h(x_1, \ldots, x_m, x_{m+1}) = gf(x_1, \ldots, x_m), x_{m+1}$. Then h is a bijection. Thus, by the PMI the result holds.

Alternate. The function f : N $\to$ N^k given by $f(m) = (m, 1, \ldots, 1)$ is one-one. Next, let $p_1, \ldots, p_k$ be the first k number of primes, *i.e.*, $p_1 = 2, p_2 = 3$, etc. Define g : N$^k \to$ N by $g(m_1, \ldots, m_k) = {}_2\cdot \cdot \cdot$

$p^m{}_k{-}1$

${}_1p^m{}_2{-}1$

$p^m{}_1{-}1$ is one-one. So, by CSB

$_k$. The prime factorization theorem implies that g

theorem, there exists a bijection from N$^k \to$ N.

(7) Let $A_1, \ldots, A_k$ be countable sets. We need to show that $X := A_1 \times \cdots \times A_k$ is countable. If any $A_i = \varnothing$, then $X = \varnothing$; thus it is countable. So, assume that each $A_i$is nonempty. Since $A_i$is countable, there exists a one-one function f_i: $A_i \to$ N. Then the function $f : X \to$ N^k defined by $f(x_1, \ldots, x_k) = f_1(x_1), \ldots, f_k(x_k)$ is one-one. Let g : N$^k \to$ N be the one-one function given in (6). Then $g \circ f : X \to$ N is a one-one function.

We now address the question whether all infinite sets are denumerable or not. Its answer is hidden in Cantor's experiment, which we present in the following. Recall that if X is a set, then its power set $P(X)$ denotes the set of all subsets of X.

Cantor's experiment: Take a blank sheet of paper.

1. On the left draw an oval (of vertical length) and write the elements of $\{1, 2, 3, 4\}$ inside it, one below the other. On the right draw a similar but larger oval and write the elements of

$P(\{1, 2, 3, 4\})$ inside it, one below the other.

2. Now draw a directed line from 1 (on the left) to any element on the right. Repeat this for 2, 3 and 4. We have drawn a function. Call it f.
3. Notice that $f(1)$, $f(2)$, $f(3)$ and $f(4)$ are sets. Find out the set $Y = \{i : i /\in f(i)\}$. Locate this set on the right.
4. It is guaranteed that you do not have a directed line touching Y . Why?

Theorem 3.5.6. [Cantor] *There exists no surjection from a set to its power set.*

Proof. On the contrary, let X be a set and let $f : X \to P(X)$ be an onto function. For each $x \in X$, $f(x) \subseteq X$. Consider the set $Y = \{x \in X : x\ 6{\in}\ f(x)\}$. Since $Y \in P(X)$ and f is onto, there exists $s \in X$ with $f(s) = Y$.

If $s \in Y$, then s satisfies the defining property of Y , *i.e.*, $s\ 6{\in}\ f(s)$. As $f(s) = Y$, $s\ 6{\in}\ Y$. If $s\ 6{\in}\ Y$, then $f(s) = Y$ gives $s\ 6{\in}\ f(s)$. So, s satisfies the defining property of Y , and hence $s \in Y$. We thus see that $s \in Y$ if and only if $s\ 6{\in}\ Y$. This is a contradiction.

Remark 3.5.7. Cantor's theorem implies that one cannot have a bijection between a set and its power set. In particular, the sets N and P(N) cannot be equinumerous. However, f : N → P(N) given by $f(x) = \{x\}$ is one-one. Thus the set P(N) is infinite but not denumerable, *i.e.*, by Definition 3.5.1, P(N) is an uncountable set. It follows that any set equinumerous with P(N) is uncountable. In general, the following result holds.

Theorem 3.5.8. *The power set of any infinite set is uncountable.*

Proof. Let X be an infinite set. By Theorem 3.1.4, there exists a one-one function f : N → X. Define the function g : P(N) → $P(X)$ by

$$g(A) = \{f(i) : i \in A\} \text{ for each } A \in P(\mathrm{N}).$$

Then, g is one-one. As Remark 3.5.7 shows, P(N) is uncountable. Thus gP(N) is uncountable. The set $P(X)$, being a superset of gP(N) , is uncountable.

Example 3.5.9.

1. Let X be the family of all functions x : N → $\{0, 1\}$. Equivalently, let

$$X = x : x = (x_1, x_2, \ldots), x_i \in \{0, 1\} \text{ for each } i \in \mathrm{N} ,$$

the set of all 0-1 sequences. Define $f : X \to P$(N) by

$$f(x) = f(x_1, x_2, \ldots) = \{n : x_n = 1\}.$$

Then f is a bijection. Hence, X is uncountable.

2. Let $Y = .a_1a_2a_3 \cdots : a_i \in \{0, 1\}$ for each $i \in$ N · It follows from (1) that X is uncountable. We give another proof by Cantor.

   Cantor's diagonalization: On the contrary, suppose Y is countable. Clearly Y is not finite. So, let $x_1, x_2, \cdots$ be an enumeration of Y . Let $x_n = .x_{n1}x_{n2} \cdots$, where $x_{ni} \in \{0, 1\}$. We construct the numbers y_n as follows:

If $x_{nn} = 0$, then take $y_n = 1$; otherwise, take $y_n = 0$.

   Now, consider the number $y = .y_1y_2 \cdots \in X$. Notice that for each n, y 6= x_n, *i.e.*, $y \in Y$ but it is not in the enumeration of Y . This is a contradiction.

   Recall that every real number in the interval $[0, 1)$ has a unique non-terminating binary repre sentation, and also a non-terminating decimal representation. Thus we have shown that $[0, 1)$ is an uncountable set.

Theorem 3.5.10. *The set* P(N) *is equinumerous with* $[0, 1)$ *and also with* R.

Proof. By Example 3.5.9, there exists a one-one function $f : P(\mathrm{N}) \to [0, 1)$. Let $r \in (0, 1)$. Consider the non-terminating binary representation of r. Denote by F_r the set of positions of 1 in this representation. Define $g : [0, 1) \to P(\mathrm{N})$ by $g(0) = \varnothing$, and $g(r) = F_r$ if r 6= 0. Then g is one-one. Therefore, by CSB-theorem, P(N) is equinumerous with $[0, 1)$.

The next statement follows as $[0, 1)$ is equinumerous with $(0, 1)$ (see Exercise 3.3.4.1) and $(0, 1)$ is equinumerous with R (see Practice 3.3.1.4).

Exercise 3.5.11.

1. *Let X be a nonempty set. Prove by two methods that there is no injection from $P(X)$ to X; once by using CSB-theorem and once without using it.*
2. *Give a bijection from* R *to* R \ Q.
3. *Write* R *as a union of pairwise disjoint sets of size* 5.
4. *Supply a bijection from* $(0, 1)$ *to* $(1, 2) \cup (3, 4) \cup (5, 6) \cup (7, 8) \cup \cdots$.
5. *Show using CSB-theorem that* $(0, 1)$ *is equinumerous with* $(0, 1]$.

6. *Show that* $(0, 1)$ *is equinumerous with* $(0, 1) \times (0, 1)$*; and that* R × R *is equinumerous with* R.
7. *Let $A_1, A_2, \ldots$ be an infinite sequence of nonempty sets such that A_k is a proper superset of A_{k+1} for each $k \in$* N. *Show that A_1 is an infinite set.*
8. *Let X be a set such that $f :$* N $\to$ *X is an onto function. Then prove that X is countable.*
9. *Let S be the set of sequences (x_n), with $x_n \in \{0, 1, \ldots, 9\}$, for each $n \in$* N, *such that 'if $x_k < x_{k+1}$, then $x_{k+1} = x_{k+2} = \cdots$'. Is S countable?*
10. *Let S be the set of all decreasing[1]sequences made with natural numbers. Is S countable?*
11. *Let S be the set of all increasing sequences made with natural numbers. Is S*

uncountable?

12. *Let S be a countable set of points on the unit circle in* R^2. *Consider the line segments L_s with one end at the origin and the other end at a point $s \in S$. Fix these lines. We are allowed to*

rotate the circle anticlockwise (the lines do not move). Let T be another countable set of points on the unit circle. Can we rotate the circle by an angle θ so that no line L_s touches any of the points of T?

13. *A complex number is called* algebraic *if it is a root of a polynomial equation with integer coefficients. All other complex numbers are called* transcendental.

    (a) *Show that the set of algebraic numbers is countable.*

    (b) *Show that the set of transcendental numbers is uncountable.*

14. *Fix an $n \in$ N and let T_n be the set of all functions from $\{1, 2, \dots, n\}$ to* N.

    (a) *Is T_n a countable set?*

    (b) *Is the set $\bigcup_{n=1}^{\infty} T_n$ countable?*

15. *Let X be the set of all functions from* N *to* N.

    (a) *Is X uncountable? Justify your answer.*

    (b) *A function $f \in X$ is said to be* eventually constant *if there exist $m, N \in$ N such that $f(n) = m$ for all $n \geq N$. Let $S \subseteq X$ be the set all eventually constant functions. Is S countable?*

[1] A sequence (x_n) is called decreasing if $x_{m+1} \leq x_m$ for each $m \in$ N; increasing if $x_{m+1} \geq x_m$ for each $m \in$ N; strictly decreasing if $x_{m+1} < x_m$ for each $m \in$ N; and it is called strictly increasing if $x_{m+1} > x_m$ for each $m \in$ N.

Chapter 4

Elementary Number Theory

4.1 Division algorithm and its applications

In this section, we study some properties of integers. We start with the 'division algorithm'.

Lemma 4.1.1. [Division algorithm] *Let a and b be two integers with $b > 0$. Then there exist unique integers q, r such that $a = qb + r$, where $0 \leq r < b$. The integer q is called the* quotient *and r, the* remainder*.*

Proof. Existence: Take $S = \{a + bx | x \in Z\} \cap W$. Then $a + |a|b \in S$. Hence, S is a nonempty subset of W. Therefore, by the well ordering principle, S contains its minimum, say s_0. So, $s_0 = a + bx_0$, for some $x_0 \in Z$. Since $s_0 \in W$,
$s_0 \geq 0$.

If $s_0 \geq b$ then $0 \leq s_0 - b = a + b(x_0 - 1) \in S$. This contradicts the minimality of s_0. Hence $0 \leq s_0 < b$. Take $q = -x_0$ and $r = s_0$. Then $qb + r = -x_0b + s_0 = -x_0b + a + bx_0 = a$, *i.e.*, we have obtained q and r such that $a = qb + r$ with $0 \leq r < b$.

Uniqueness: Assume that there exist integers q_1, q_2, r_1 and r_2 satisfying $a = q_1b + r_1$, $0 \leq r_1 < b$, $a = q_2b+r_2$, and $0 \leq r_2 < b$. Suppose $r_1 < r_2$. Then $0 < r_2-r_1 < b$. Notice that $r_2-r_1 = (q_1-q_2)b$. So, $0 < (q_1 - q_2)b < b$. This is a contradiction since $(0, b)$ does not contain any integer which is a multiple of b. Similarly, $r_2 < r_1$ leads to a contradiction. Therefore, $r_1 = r_2$. Then, $0 = r_1 - r_2 = (q_1 - q_2)b$ and b 6= 0 imply that $q_1 = q_2$.

Definition 4.1.2. Let $a, b \in Z$ with b 6= 0. If $a = bc$, for some $c \in Z$ then b is said to divide a and we write $b|a$ (read as b divides a.) When $b|a$, we also say that b is a divisor of a, and that a is a multiple of b.

Remark 4.1.3. Let a be a nonzero integer. If b is a positive divisor of a, then $1 \leq b \leq |a|$. Hence the set of all positive divisors of a nonzero integer is a nonempty finite set.

Further, if a is a positive integer and b is a positive divisor of a, then $a = kb$ for some $k \in N$ so that $b \leq a$. It then follows that if $a, b \in N$ such that $a|b$ and $b|a$, then $a = b$.

Definition 4.1.4. 1. Let a and b be two nonzero integers. Then the set S of their common positive divisors is nonempty and finite. Thus, S contains its greatest element. This element is called the greatest common divisor of a and b and is denoted by gcd(a, b). The gcd is also called the highest common factor.

2. An integer a is said to be relatively prime to an integer b if gcd(a, b) = 1. In this case, we also say that the integers a and b are coprimes.

The next result is often stated as 'the gcd(a, b) is a linear combination of a and b'.

Theorem 4.1.5. [Bezout's identity] ´ *Let a and b be two nonzero integers and let* $d = \gcd(a, b)$*. Then there exist integers* x_0, y_0 *such that* $d = ax_0 + by_0$.

Proof. Consider the set $S = \{ax + by : x, y \in Z\} \cap N$. Then, either $a \in S$ or $-a \in S$. Thus, S is a nonempty subset of N. By the well ordering principle, S contains its least element, say d. As $d \in S$, we have $d = ax_0 + by_0$, for some $x_0, y_0 \in Z$. We show that $d = \gcd(a, b)$.

By the division algorithm, there exist integers q and r such that $a = dq + r$, with $0 \le r < d$. If $r > 0$, then

$$r = a - dq = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0) \in \{ax + by : x, y \in Z\}.$$

In this case, r is a positive integer in S which is strictly less than d. This contradicts the choice of d as the least element of S. Thus, $r = 0$. Consequently, $d|a$. Similarly, $d|b$. Hence $d \le \gcd(a, b)$. Now, $\gcd(a, b)|a$ and $\gcd(a, b)|b$. Since $d = ax_0 + by_0$ for some $x_0, y_0 \in Z$, we have $\gcd(a, b)|d$. That is, $d = k \times \gcd(a, b)$ for some integer k. However, both $\gcd(a, b)$ and d are positive. Thus k is a positive integer. Hence $d \ge \gcd(a, b)$.

Therefore, $d = \gcd(a, b)$.

We prove three useful corollaries to B´ezout's identity.

Corollary 4.1.6. *Let* $a, b \in Z$ *and let* $d \in N$*. Then,* $d = \gcd(a, b)$ *if and only if* $d|a$, $d|b$*, and each common divisor of a and b divides d.*

Proof. Suppose $d = \gcd(a, b)$. Then $d|a$ and $d|b$. By B´ezout's identity, $d = ak + bm$ for some $k, m \in Z$. Thus, any common divisor of a and b divides $d = \gcd(a, b)$.

Conversely, suppose $d|a$, $d|b$ and each common divisor of a and b divides d. Since d is a common divisor of a and b, by what we have just proved, $d| \gcd(a, b)$. Further, $\gcd(a, b)$ is a common divisor of a and b; so, by assumption $\gcd(a, b)|d$. By Remark 4.1.3, $d = \gcd(a, b)$.

Corollary 4.1.7. *Let a, b be nonzero integers. Then* $\gcd(a, b) = 1$ *if and only if there exist integers* x_0 *and* y_0 *such that* $ax_0 + by_0 = 1$.

Proof. If $\gcd(a, b) = 1$, then by B´ezout's identity, there exist integers x_0 and y_0 such that $ax_0+by_0 = 1$. Conversely, suppose there exist integers x_0 and y_0 such that $ax_0 + by_0 = 1$. If $\gcd(a, b) = k$, then k is a positive integer such that $k|1$. It follows that $k \le 1$; consequently, $k = 1$.

Corollary 4.1.8. *Let* $n_1, \ldots, n_k$ *be positive integers which are pairwise coprimes. If* $a \in Z$ *is such that* $n_1|a, \ldots, n_k|a$*, then* $n_1 \cdots n_k|a$.

Proof. The positive integers $n_1, \ldots, n_k$ are pair wise coprimes means that if i 6= j, then $\gcd(n_i, n_j) = 1$. Let $a \in Z$ be such that $n_1|a, \ldots, n_k|a$. We show by induction that $n_1 \cdots n_k|a$. For $k = 2$, it is given that $n_1|a$, $n_2|a$ and $\gcd(n_1, n_2) = 1$. By B´ezout's identity, there exist $x, y \in Z$ such that $n_1x+n_2y = 1$. Multiplying by a, we have $a = an_1x + an_2y = n_1n_2x(\frac{a}{n_2}) + y(\frac{a}{n_1})$.

Since $n_2|a$ and $n_1|a$, we see that $\frac{a}{n_2}, \frac{a}{n_1} \in Z$ so that $x(\frac{a}{n_2}) + y(\frac{a}{n_1}) \in Z$. Hence $n_1n_2|a$. Assume the induction hypothesis that the statement is true for $k = m$. Let each of $n_1, \ldots, n_{m+1}$ divide a and that they are pairwise coprimes. Let $n_1 \cdots n_m$ = `. Then gcd(`, n_{m+1}) = 1. By the induction hypothesis,

`$|a$. By the basis case, ($k = 2$ as proved), we conclude that ` $n_{m+1}|a$. That is, $n_1 \cdots n_{m+1}|a$.

The division algorithm helps to algorithmically compute the greatest common divisor of two nonzero integers, commonly known as the Euclid's algorithm.

Let a, and b be nonzero integers. By the division algorithm, there exists integers q and r with $0 \leq r < |b|$ such that $a = |b|q + r$. We apply our observation that a common divisor of two integers divides their gcd.

Now, gcd($|b|, r$) divides both $|b|$ and r; hence it divides a. Again, gcd($|b|, r$) divides both a and $|b|$. Hence gcd($|b|, r$)| gcd($a, |b|$).

Similarly, with $r = a - |b|q$, we see that gcd($a, |b|$) divides both a and $|b|$; hence gcd($a, |b|$)$|r$. Consequently, gcd($a, |b|$)| gcd($|b|, r$).

Further, the gcd of any two integers is positive. Thus, gcd(a, b) = gcd($a, |b|$). So, we obtain

$$\gcd(a, b) = \gcd(a, |b|) = \gcd(|b|, r).$$

Euclid's algorithm applies this idea repeatedly to find the greatest common divisor of two given nonzero integers, which we now present.

Euclid's algorithm

Input: Two nonzero integers a and b; Output: gcd(a, b).

$$a = b\, q_0 + r_0 \text{ with } 0 \leq r_0 < b$$
$$b = r_0\, q_1 + r_1 \text{ with } 0 \leq r_1 < r_0$$
$$r_0 = r_1\, q_2 + r_2 \text{ with } 0 \leq r_2 < r_1$$
$$r_1 = r_2\, q_3 + r_3 \text{ with } 0 \leq r_3 < r_2$$
$$\ddots$$

$$r_{`-1} = r_{`}\, q_{`+1} + r_{`+1} \text{ with } 0 \leq r_{`+1} < r_{`}$$
$$r_{`} = r_{`+1}\, q_{`+2}.$$
$$\gcd(a, b) = r_{`+1}$$

The process will take at most $b - 1$ steps as $0 \leq r_0 < b$. Also, note that $r_{`+1}$ can be expressed in the form $r_{`+1} = a\, x_0 + b\, y_0$ for integers x_0, y_0 using backtracking. That is,

$$r_{`+1} = r_{`-1} - r_{`}q_{`+1} = r_{`-1} - q_{`+1}\,(r_{`-2} - r_{`-1}q_{`}) = r_{`-1}\,(1 + q_{`+1}q_{`}) - q_{`+1}r_{`-2} = \cdots.$$ Example

4.1.9. We apply Euclid's algorithm for computing gcd(155, −275) as follows.

$$-275 = (-2) \cdot 155 + 35 \text{ (so, } \gcd(-275, 155) = \gcd(155, 35))$$
$$155 = 4 \cdot 35 + 15 \text{ (so, } \gcd(155, 35) = \gcd(35, 15))$$
$$35 = 2 \cdot 15 + 5 \text{ (so, } \gcd(35, 15) = \gcd(15, 5))$$
$$15 = 3 \cdot 5 \text{ (so, } \gcd(15, 5) = 5).$$

To write 5 = gcd(155, −275) in the form $155x_0 + (-275)y_0$, notice that

$$5 = 35-2 \cdot 15 = 35-2(155-4 \cdot 35) = 9 \cdot 35-2 \cdot 155 = 9(-275 + 2 \cdot 155)-2 \cdot 155 = 9 \cdot(-275) + 16 \cdot 155.$$

Also, note that $275 = 5 \cdot 55$ and $155 = 5 \cdot 31$ and thus, $5 = (9 + 31x)\cdot(-275) + (16 + 55x)\cdot 155$, for all $x \in$ Z. Therefore, we see that there are infinite number of choices for the pair $(x, y) \in$ Z^2, for which

$d = ax + by$.

Exercise 4.1.10. *1. Let a, b* ∈ N *with* gcd(*a, b*) = *d. Then* gcd($^a{}_d, ^b{}_d$) = 1*. 2. Prove that the system* 15*x* + 12*y* = *b has a solution for x, y* ∈ Z *if and only if* 3 *divides b.*

3. [Linear Diophantine equation] *Let a, b, c* ∈ Z \ *{*0*}. Then the linear system ax* + *by* = *c, in the unknowns x, y* ∈ Z *has a solution if and only if* gcd(*a, b*) *divides c. Furthermore, determine all pairs* (*x, y*) ∈ Z × Z *such that ax* + *by is indeed c.*

4. *Prove that* gcd(*a, bc*) = 1 *if and only if* gcd(*a, b*) = 1 *and* gcd(*a, c*) = 1*, for any three nonzero integers a, b and c.*

5. *Euclid's algorithm can sometimes be applied to check whether two numbers which are dependent on an unknown integer n, are relatively prime or not. For example, we can use the algorithm to prove that* gcd(2*n* + 3, 5*n* + 7) = 1 *for every n* ∈ Z*.*

6. *Suppose a milkman has only* 3 *cans of sizes* 7*,* 9 *and* 16 *liters. What is the minimum number of operations required to deliver* 1 *liter of milk to a customer? Explain.*

To proceed further, we need the following definitions.

Definition 4.1.11. 1. The integer 1 is called the unity (or the unit element) of Z. 2. An integer *p* > 1 is called a prime, if *p* has exactly two positive divisors, namely, 1 and *p*. 3. An integer *r* > 1 is called composite if *r* is not a prime.

We are now ready to prove an important result that helps us in proving the fundamental theorem of arithmetic.

Lemma 4.1.12. [Euclid's Lemma] *Let a, b* ∈ Z *and let p be a prime. If p*|*ab then p*|*a or p*|*b.*

Proof. Suppose *p*|*ab*. If *p*|*a*, then there is nothing to prove. So, assume that *p* - *a*. As *p* is a prime, gcd(*p, a*) = 1. Thus there exist integers *x, y* such that 1 = *ax* + *py*. Then *b* = *abx* + *pby*. Since *p*|*ab* and *p*|*pb*, we see that *p*|*b*.

One also has the following result.

Proposition 4.1.13. *Let a, b, n* ∈ Z *be such that n*|*ab. If* gcd(*n, a*) = 1*, then n*|*b.*

Proof. Suppose gcd(*n, a*) = 1. There exist x_0, y_0 ∈ Z such that $nx_0 + ay_0 = 1$. Then $b = aby_0 + nbx_0$. Since *n*|*ab* and *n*|*nb*, we have *n*|*b*.

Now, we are ready to prove the fundamental theorem of arithmetic that states that 'every positive integer greater than 1 is either a prime or is a product of primes. This product is unique, except for the order in which the prime factors appear'.

Theorem 4.1.14. [Fundamental theorem of arithmetic] *Let n* ∈ N *with n* ≥ 2*. Then there exist prime numbers* $p_1 > p_2 > \cdots > p_k$ *and positive* $_2 \cdots p^{s_k}$
integers $s_1, s_2, \ldots, s_k$ *such that* $n = p^{s_1}$
$_2 \cdots q^{t_\cdot}$ $_1p^{s_2}$ $_k$*, for*
some $k \geq 1$*. Moreover, if n also equals* $q^{t_1}{}_1q^{t_2}$
$_\cdot$*, for distinct primes* $q_1 > q_2 > \cdots > q_\cdot$ *and positive*
integers $t_1, t_2, \ldots, t_\cdot$ *then k* = ` *and for each i* ∈ *{*1*, . . . , k}*, $p_i = q_i$ *and* $s_i = t_i$*.*

Proof. See Example 2.2.6 for a proof.

Theorem 4.1.15. [Euclid: Infinitude of primes] *The number of primes is infinite.*

Proof. On the contrary assume that the number of primes is finite, say $p_1 = 2, p_2 = 3, \ldots, p_k$. Consider the positive integer $N = p_1p_2 \cdots p_k + 1$. We see that none of the primes $p_1, p_2, \ldots, p_k$ divides N. This contradicts Theorem 4.1.14.

Proposition 4.1.16. [Primality testing] *Let $n \in$ N with $n \geq 2$. If no prime $p \leq \sqrt{n}$ divides n, then n is prime.*

Proof. Suppose $n = xy$, for $2 \leq x, y < n$. Then, either $x \leq \sqrt{n}$ or $y \leq \sqrt{n}$. Without loss of generality, assume $x \leq \sqrt{n}$. If x is a prime, we are done. Else, take a prime divisor p of x. Now, $p \leq \sqrt{n}$ and p divides n.

Exercise 4.1.17. *1. Prove that there are infinitely many primes of the form $4n - 1$. 2. Fix N $\in$ N, N $\geq$*

2. Then, there exists a consecutive set of N natural numbers that are composite.

Definition 4.1.18. The least common multiple of integers a and b, denoted as lcm(a, b), is the smallest positive integer that is a multiple of both a and b.

Lemma 4.1.19. *Let a, b $\in$ Z and let ` $\in$ N. Then, ` = lcm(a, b) if and only if a|`, b|` and ` divides each common multiple of a and b.*

Proof. Let ` = lcm($a, b$). Clearly, $a$|` and b|`. Let $x$ be a common multiple of both $a$ and $b$. If ` - x, then by the division algorithm, x = ` $\cdot$ $q + r$ for some integer $q$ and some $r$ with $0 < r <$ `. Notice that $a|x$ and a|`. So, $a|r$. Similarly, $b|r$. That is, $r$ is a positive common multiple of both $a$ and $b$ which is less than lcm($a, b$). This is a contradiction. Hence, ` = lcm(a, b) divides each common multiple of a and b.

Conversely, suppose a|`, $b$|` and ` divides each common multiple of $a$ and $b$. By what we have just proved, lcm($a, b$)|`. Further, lcm(a, b) is a common multiple of a and b. Thus `| lcm($a, b$). By Remark 4.1.3, we conclude that ` = lcm(a, b).

Theorem 4.1.20. *Let a, b $\in$ N. Then* gcd(a, b) $\cdot$ lcm(a, b) = ab. *In particular,* lcm(a, b) = ab *if and only if* gcd(a, b) = 1.

Proof. Let d = gcd(a, b). Then $a = a_1d$ and $b = b_1d$ for some $a_1, b_1 \in$ N. Further,

$$ab = a_1d\,b_1d = (a_1b_1d) \cdot \gcd(a, b).$$

Thus, it is enough to show that lcm(a, b) = a_1b_1d.

Towards this, notice that $a_1b_1d = ab_1 = a_1b$, that is, $a|a_1b_1d$ and $b|a_1b_1d$. Let $c \in$ N be any common multiple of a and b. Then $\frac{c}{a}, \frac{c}{b} \in$ Z. Further, by B´ezout's identity, $d = as + bt$ for some $s, t \in$ Z. So,

$$a_1b_{1d}=cd$$

$$c$$

$$(a_1d) \cdot (b_{1d})=c(as + bt)$$

$$ab = \overset{c}{}bs + \overset{c}{}at \in Z.$$

Hence $a_1b_1d|c$. That is, a_1b_1d divides each common multiple of a and b. By Lemma 4.1.19, a_1b_1d = lcm(a, b).

4.2 Modular arithmetic

Definition 4.2.1. Fix a positive integer n. Let $a, b \in$ Z. If n divides $a{-}b$, we say that a is congruent to b modulo n, and write $a \equiv b$ (mod n).

Example 4.2.2. 1. Notice that $2|(2k - 2m)$ and also $2|[(2k - 1) - (2m - 1)]$. Therefore, any two even integers are congruent modulo 2; and any two odd integers are congruent modulo 2.

2. The numbers ±10 and 22 are congruent modulo 4 as $4|(22 - 10)$ and $4|(22 - (-10))$. 3. Let n be a fixed positive integer. Recall the notation $[n - 1] := \{0, 1, 2, . . . , n - 1\}$. (a) Then, by the division algorithm, for any $a \in$ Z there exists a unique $b \in [n - 1]$ such that $a \equiv b$ (mod n). The number b is called the residue of a modulo n.

(b) Further Z $=^{n}$S$^{-1}{}_{a=0}$ $\{a + kn : k \in$ Z$\}$, *i.e.*, every integer is congruent to an element of $[n - 1]$.

The set $[n - 1]$ is taken as the standard representative for the set of residue classes modulo n.

Theorem 4.2.3. *Fix $n \in$ N, and let $a, b, c, d \in$ Z. Then the following are true:*

1. *If $a \equiv b$ (mod n) and $b \equiv c$ (mod n), then $a \equiv c$ (mod n).*

2. *If $a \equiv b$ (mod n), then $a + c \equiv b + c$ (mod n), $a - c \equiv b - c$ (mod n) and $ac \equiv bc$ (mod n).*

3. *If $a \equiv b$ (mod n) and $c \equiv d$ (mod n), then $a + c \equiv b + d$ (mod n), $a - c \equiv b - d$ (mod n) and $ac \equiv bd$ (mod n). In particular, $a \equiv b$ (mod n) implies $a^m \equiv b^m$ (mod n) for all $m \in$ N.*

4. *If $ac \equiv bc$ (mod n) for nonzero a, b, c, and $d =$ gcd(c, n), then $a \equiv b$ (mod n/d). In particular, if $ac \equiv bc$ (mod n) for nonzero a, b, c, and gcd$(c, n) = 1$, then $a \equiv b$ (mod n).*

Proof. We will only prove two parts. The readers should supply the proof of other parts. 3. Note that $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d)$. Thus, $n|ac - bd$, whenever $n|a - b$ and $n|c - d$. In particular, taking $c = a$ and $d = b$ and repeatedly applying the above result, one has $a^m \equiv b^m$ (mod n), for all $m \in$ N.

4. Let gcd$(c, n) = d$. Then, there exist nonzero $c_1, n_1 \in$ Z with $c = c_1d, n = n_1d$. Then $n|ac - bc$ implies $n_1d|c_1d(a{-}b)$, which implies $n_1|c_1(a{-}b)$. By Proposition 4.1.13, $n_1|a{-}b$, *i.e.*, $\frac{n}{\gcd(c,n)}|a{-}b$.

Example 4.2.4. 1. Note that $3 \cdot 9 + 13 \cdot (-2) \equiv 1$ (mod 13). If x satisfies $9x \equiv 4$ (mod 13) then

$$\begin{aligned} x &\equiv x \cdot 1 \equiv x \cdot (3 \cdot 9 + 13 \cdot (-2)) && \text{as } 3 \cdot 9 + 13 \cdot (-2) \equiv 1 \pmod{13} \\ &\equiv 3 \cdot 9x && \text{as } 13 \equiv 0 \pmod{13} \\ &\equiv 3 \cdot 4 && \text{as } 9x \equiv 4 \pmod{13} \\ &\equiv 12 \pmod{13}. \end{aligned}$$

To verify, if $x \equiv 12$ (mod 13), then $9x \equiv 108 \equiv (13 \times 8 + 4) \equiv 4$ (mod 13). Therefore, the congruence equation $9x \equiv 4$ (mod 13) has solution $x \equiv 12$ (mod 13).

2. Verify that $9 \cdot (-5) + 23 \cdot (2) = 1$. Hence, the equation $9x \equiv 1 \pmod{23}$ has the solution x

$$\equiv x \cdot 1 \equiv x\,(9 \cdot (-5) + 23 \cdot (2)) \equiv (-5) \cdot (9x) \equiv -5 \times 1 \equiv 18 \pmod{23}.$$

3. Verify that the equation $3x \equiv 15 \pmod{30}$ has solutions $x = 5, 15, 25$; where as the equation $7x = 15 \pmod{30}$ has only one solution $x = 15$; and that the equation $3x \equiv 5 \pmod{30}$ has no solution.

Theorem 4.2.5. [Linear Congruence] *Let n be a positive integer and let a, b be nonzero integers. Then the congruence equation $ax \equiv b \pmod{n}$ has at least one solution if and only if* $\gcd(a, n)|b$. *Moreover, if $d = \gcd(a, n)|b$, then $ax \equiv b \pmod{n}$ has exactly d number of solutions $r_1, \ldots, r_d \in \{0, 1, 2, \ldots, n-1\}$, where $r_i \equiv r_j \pmod{n/d}$ for all $i, j = 1, 2, \ldots, d$.*

Proof. Write $d = \gcd(a, n)$. Let x_0 be a solution of $ax \equiv b \pmod{n}$. Then, by definition, $ax_0 - b = nq$, for some $q \in Z$. Thus, $b = ax_0 - nq$. Since $d|a$ and $d|n$, we have $d|ax_0 - nq = b$. Conversely, suppose $d|b$. Then, $b = b_1 d$, for some $b_1 \in Z$. By B´ezout's identity, there exist $x_0, y_0 \in Z$ such that $ax_0 + ny_0 = d$. Hence,

$$a(x_0 b_1) \equiv b_1(ax_0) \equiv b_1(ax_0 + ny_0) \equiv b_1 d \equiv b \pmod{n}.$$

That is, $x_0 b_1$ is a solution of $ax \equiv b \pmod{n}$. This proves the first statement. To proceed further, assume that $d|b$. By what we have just proved, there exists a solution x_1 of $ax \equiv b \pmod{n}$. By the division algorithm, there exist $p, r \in Z$ with $0 \le r < n$ such that $x_1 = pn+r$. Now, $ar \equiv a(x_1 - pn) \equiv ax_1 \equiv b \pmod{n}$. Thus, r is also a solution of $ax \equiv b \pmod{n}$, *i.e.*, there exists $r \in \{0, 1 \ldots, n-1\}$ satisfying $ar \equiv b \pmod{n}$.

If $x_2 \in \{0, 1, \ldots, n-1\}$ is any other solution of $ax \equiv b \pmod{n}$, then $ax_2 \equiv b \equiv ar \pmod{n}$. Thus, by Theorem 4.2.3.4, $x_2 \equiv r \pmod{n/d}$. Conversely, if $x_2 \equiv r \pmod{n/d}$, then $x_2 = r+m(n/d)$ for some $m \in Z$. Then $ax_2 = ar + am(n/d) = ar + mn(a/d)$. as $d|a$, the number a/d is an integer. Hence, $ax_2 \equiv ar \pmod{n}$ so that x_2 is a solution of $ax \equiv b \pmod{n}$.

Therefore, all solutions of $ax \equiv b \pmod{n}$ in $\{0, 1, \ldots, n-1\}$ are of the form $r + k(n/d)$ for $k \in Z$. However, there are exactly d number of integers in $\{0, 1, \ldots, n-1\}$ which are congruent to r modulo (n/d). Hence there are d number of solutions of $ax \equiv b \pmod{n}$ in $\{0, 1, \ldots, n-1\}$.

Remark 4.2.6. Observe that a solution of the congruence $ax \equiv b \pmod{n}$ is a number in $\{0, 1, \ldots, n-1\}$. This set is not to be confused with the congruence class $[n-1]$. When $d = \gcd(a, n)$, we may write the distinct solutions in $[n-1]$ in increasing order as $r_1 = r$, $r_2 = r + n/d$, $r_3 = r + 2n/d, \ldots, r_d = r + (d-1)n/d$. It means that the solutions are $x_i \equiv r_i \pmod{n}$ for $i = 1, 2, \ldots, d$.

Exercise 4.2.7. *1. Complete the proof of Theorem 4.2.3.*

2. Determine the solutions of the system $3x \equiv 5 \pmod{65}$.

3. Determine the solutions of the system $5x \equiv 95 \pmod{100}$.

4. Prove that the system $3x \equiv 4 \pmod{28}$ *is equivalent to the system* $x \equiv 20 \pmod{28}$.

5. Consider the congruence pair $3x \equiv 4 \pmod{28}$ *and* $4x \equiv 2 \pmod{27}$.

(a) Prove that the given pair is equivalent to the pair $x \equiv 20 \pmod{28}$ *and* $x \equiv 14 \pmod{27}$.

(b) Prove that solving the congruence pair in (a) is equivalent to solving one of the congruences

$20 + 28k \equiv 14 \pmod{27}$ *or* $14 + 27k \equiv 20 \pmod{28}$ *for the unknown quantity* k. *(c) Verify that* $k = 21$ *is the solution for the first case in (b) and* $k = 22$ *for the second case. (d) Conclude that* $x = 20 + 28 \cdot 21 = 14 + 27 \cdot 22$ *is a solution for the given congruence pair.* *6. Prove that if p is a prime,*

then $p|C(p, k) :=$ $p!$

$k!(p - k)!$ *for* $1 \leq k \leq p - 1$.

7. *Let p be a prime. Write* $Z_p := \{0, 1, 2, . . . , p - 1\}$ *and* $Z^*_p := \{1, 2, . . . , p - 1\} = Z_p \setminus \{0\}$. *Show that* Z_p *has the following properties:*

(a) *For all* $a, b \in Z_p$, $a + b \pmod{p} \in Z_p$.

(b) *For all* $a, b \in Z_p$, $a + b = b + a \pmod{p}$.

(c) *For all* $a, b, c \in Z_p$, $a + (b + c) \equiv (a + b) + c \pmod{p}$.

(d) *For all* $a \in Z_p$, $a + 0 \equiv a \pmod{p}$.

(e) *For all* $a \in Z_p$, $a + (p - a) \equiv 0 \pmod{p}$.

(f) *For all* $a, b \in Z^*_p$, $a \cdot b \pmod{p} \in Z^*_p$.

(g) *For all* $a, b \in Z^*_p$, $a \cdot b = b \cdot a \pmod{p}$.

(h) *For all* $a, b, c \in Z^*_p$, $a \cdot (b \cdot c) \equiv (a \cdot b) \cdot c \pmod{p}$.

(i) *For all* $a \in Z^*_p$, $a \cdot 1 \equiv a \pmod{p}$.

(j) *For each* $a \in Z^*_p$, *there exists* $b \in Z^*_p$ *such that* $a \cdot b \equiv 1 \pmod{p}$.

(k) *For all* $a, b, c \in Z_p$, $a \cdot (b + c) \equiv (a \cdot b) + (a \cdot c) \pmod{p}$.

Any nonempty set containing at least two elements such as 0 and 1, in which ‘addition’ and ‘multiplication’ can be defined in such a way that the above properties are satisfied, is called a field. So, $Z_p = \{0, 1, 2, . . . , p - 1\}$ is an example of a field. The well known examples of fields are:

(a) Q, the set of rational numbers.

(b) R, the set of real numbers.

(c) C, the set of complex numbers.

8. *Let p be an odd prime. Prove the following:*

(a) *The equation* $x^2 \equiv 1 \pmod{p}$ *has exactly two solutions in* Z_p.

(b) *Corresponding to any* $a \in \{2, 3, . . . , p-2\}$, *if there exists* $b \in Z^*_p$ *such that* $a \cdot b \equiv 1 \pmod{p}$, *then* $b \in \{2, 3, . . . , p - 2\}$ *and b 6= a.*

(c) *If* $a, b, c, d \in \{2, 3, . . . , p - 2\}$ *satisfy a 6= c,* $a \cdot b \equiv 1 \pmod{p}$ *and* $c \cdot d \equiv 1 \pmod{p}$, *then b 6= d.*

(d) *Let* $p > 3$. *Write* $q = (p - 3)/2$. *There exist two-element sets* $\{a_1, b_1\}, \{a_2, b_2\}, . . . , \{a_q, b_q\}$

that are pairwise disjoint satisfying $a_i \cdot b_i \equiv 1$ $\{a_i, b_i\} =$

$\pmod{p}$ *for* $1 \leq i \leq q$, *and* S^q

$i=1$

$\{2, 3, . . . , p - 2\}$.

(e) *If* $p > 3$, *then* $2 \cdot 3 \cdot \cdot \cdot \cdot \cdot (p - 2) \equiv 1 \pmod{p}$.

9. [Wilson’s Theorem] *If p is any prime, then* $(p - 1)! \equiv -1 \pmod{p}$.

10. [Primality Testing] *Any integer $n > 1$ is a prime if and only if* $(n - 1)! \equiv -1 \pmod{n}$.

4.3 Chinese Remainder Theorem

Theorem 4.3.1. [Chinese remainder theorem] *Fix a positive integer m. Let $n_1, n_2, \ldots, n_m$ be pairwise coprime positive integers. Write $M = n_1 n_2 \cdots n_m$. Then, the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_m \pmod{n_m} \end{aligned}$$

has a unique solution modulo M.

Proof. For $1 \leq k \leq m$, define $M_k = M$

n_k. Then, $\gcd(M_k, n_k) = 1$ and hence there exist integers x_k, y_k such that $M_k x_k + n_k y_k = 1$ for $1 \leq k \leq m$. Let $1 \leq i, j \leq m$. Then

$$M_i x_i \equiv M_i x_i + n_i y_i \equiv 1 \pmod{n_i};\ i\ 6= j \Rightarrow n_i | M_j \Rightarrow M_j x_j \equiv 0 \pmod{n_i}.$$

a solution to the given

Now, $x_0 := \text{P}^m{}_{k=1}$

$M_k x_k a_k \equiv M_i x_i a_i \equiv 1 \cdot a_i \equiv a_i \pmod{n_i}$. That is, x_0 is

system of congruences.

If y_0 is any solution to the system of congruences, then for each integer k with $0 \leq k \leq m$, we have $y_0 \equiv a_k \pmod{n_k}$ so that $y_0 - x_0 \equiv a_k - a_k \equiv 0 \pmod{n_k}$. Since $n_1, \ldots, n_k$ are pairwise coprimes and their product is M, Corollary 4.1.8 implies that $y_0 - x_0 \equiv 0 \pmod{M}$. Therefore, x_0 is the unique solution of the system of congruences module M.

Example 4.3.2. Consider the system of congruences $x \equiv 20 \pmod{28}$ and $x \equiv 14 \pmod{27}$ in Exercise 4.2.7.5. In this case, $a_1 = 20$, $a_2 = 14$, $n_1 = 28$ and $n_2 = 27$ so that $M = 28 \cdot 27 = 756$, $M_1 = 27$ and $M_2 = 28$. Then, $x_1 = -1$ and $x_2 = 1$ show that $M_1 x_1 + M_2 x_2 = 27 \cdot -1 + 28 \cdot 1 = 1$. Hence

$$x_0 = 27 \cdot -1 \cdot 20 + 28 \cdot 1 \cdot 14 \equiv -540 + 392 \equiv -148 \equiv 608 \pmod{756}.$$

Exercise 4.3.3. *1. Find the smallest positive integer which when divided by* 4 *leaves a remainder* 1 *and when divided by* 9 *leaves a remainder* 2.

2. Find the smallest positive integer which when divided by 8 *leaves a remained* 4 *and when divided by* 15 *leaves a remainder* 10.

3. Does there exist a positive integer n such that $n \equiv 4 \pmod{14}$ *and* $n \equiv 6 \pmod{18}$? *Give reasons for your answer. What if we replace* 6 *or* 4 *with an odd number?*

4. Let n be a positive integer. Show that the set $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$ *has the following properties:*

(a) For all $a, b \in \mathbb{Z}_n$, $a + b \pmod{n} \in \mathbb{Z}_n$.

(b) For all $a, b \in \mathbb{Z}_n$, $a + b = b + a \pmod{n}$.

(c) For all $a, b, c \in Z_n$, $a + (b + c) \equiv (a + b) + c \pmod{n}$.

(d) For all $a \in Z_n$, $a + 0 \equiv a \pmod{n}$.

(e) For all $a \in Z_n$, $a + (n - a) \equiv 0 \pmod{n}$.

(f) For all $a, b \in Z_n$, $a \cdot b \pmod{n} \in Z_n$.

(g) For all $a, b \in Z_n$, $a \cdot b = b \cdot a \pmod{n}$.

(h) For all $a, b, c \in Z_n$, $a \cdot (b \cdot c) \equiv (a \cdot b) \cdot c \pmod{n}$.

(i) For all $a \in Z_n$, $a \cdot 1 \equiv a \pmod{n}$.

(j) For all $a, b, c \in Z_n$, $a \cdot (b + c) \equiv (a \cdot b) + (a \cdot c) \pmod{n}$.

Any set, say R, with $0, 1 \in R$, 0 6= 1, in which ‘addition’ and ‘multiplication’ can be defined in such a way that the above properties are satisfied, is called a commutative ring with unity. So, $Z_n = \{0, 1, 2, . . . , n - 1\}$ is an example of a commutative ring with unity. The well known examples of commutative ring with unity are:

(a) Z, the set of integers.

(b) Q, the set of rational numbers.

(c) R, the set of real numbers.

(d) C, the set of complex numbers.

5. *Let m and n be two coprime positive integers. By Exercise 4.3.3.4, the sets Z_m, Z_n, and Z_{mn} are commutative rings with unity. Now, define addition and multiplication in $Z_m \times Z_n$ component wise. Also, define the function*

$$f : Z_{mn} \to Z_m \times Z_n \text{ by } f(x) = (x \pmod{m}, x \pmod{n}) \text{ for all } x \in Z_{mn}.$$

Then, prove the following:

(a) $Z_m \times Z_n$ is a commutative ring with unity. What are the 0 and 1 here?

(b) For all $x, y \in Z_{mn}$, $f(x + y) = f(x) + f(y)$.

(c) For all $x, y \in Z_{mn}$, $f(x \cdot y) = f(x) \cdot f(y)$.

(d) For each $(a, b) \in Z_m \times Z_n$ there exists a unique $x \in Z_{mn}$ such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

(e) $|Z_m \times Z_n| = |Z_{mn}| = mn$.

Such a function f is called a ring isomorphism, and thus, the two rings $Z_m \times Z_n$ and Z_{mn} are isomorphic.

Chapter 5

Combinatorics - I

Combinatorics can be traced back more than 3000 years to India and China. For many centuries, it primarily comprised the solving of problems relating to the permutations and combinations of objects. The use of the word “combinatorial” can be traced back to Leibniz in his dissertation on the art of combinatorial in 1666. Over the centuries, combinatorics evolved in recreational pastimes. These include the K¨onigsberg bridges problem, the four-colour map problem, the Tower of Hanoi, the birthday paradox and Fibonacci’s ‘rabbits’ problem. In the modern era, the subject has developed both in depth and variety and has cemented its position as an integral part of modern mathematics. Undoubtedly part of the reason for this importance has arisen from the growth of computer science and the increasing use of algorithmic methods for solving real-world practical problems. These have led to combinatorial applications in a wide range of subject areas, both within and outside mathematics, including network analysis, coding theory, and probability.

5.1 Addition and multiplication rules

We first consider some questions.

1. How many possible crossword puzzles are there?
2. Suppose we have to select 4 balls from a bag of 20 balls numbered 1 to 20. How often do two of the selected balls have consecutive numbers?
3. How many ways are there of rearranging the letters in the word ALPHABET?

4. Can we construct a floor tiling from squares and regular hexagons?

We observe various things about the above problems. A priori, unlike many problems in math ematics, there is hardly any abstract or technical language. Despite the initial simplicity, some of these problems will be frustratingly difficult to solve. Further, we notice that despite these problems appearing to being diverse and unrelated, they principally involve selecting, arranging, and counting objects of various types. We will first address the problem of counting. Clearly, we would like to be able to count without actually counting. In other words, can we figure out how many things there are with a given property without actually enumerating each of them. Quite often this entails deep mathematical insight. We now introduce two standard techniques which are very useful for counting without actually counting. These techniques can easily be motivated through the following examples.

Example 5.1.1.

1. Let the cars in New Delhi have license plates containing 2 alphabets followed by two numbers. What is the total number of license plates possible?

   Ans: Here, we observe that there are 26 choices for the first alphabet and another 26 choices for the second alphabet. After this, there are two choices for each of the two numbers in the license plate. Hence, we have a maximum of 26 × 26 × 10 × 10 = 67*,* 600 license plates.

2. Let the cars in New Delhi have license plates containing 2 alphabets followed by two numbers with the added condition that "in the license plates that start with a vowel the sum of numbers should always be even". What is the total number of license plates possible?

   Ans: Here, we need to consider two cases.
   Case 1: The license plate doesn't start with a vowel. Then using the previous example, the number of license plates equals 21 × 26 × 10 × 10 = 54600.

   Case 2: The license plate starts with a vowel. Then the number of license plates equals 5 × 26 × (5 × 5 + 5 × 5) = 6500.

   Hence, we have a maximum of 54600 + 6500 = 61100 license plates.

Generalization of the first example leads to what is referred to as the rule of product and that of the second leads to the rule of addition. To understand these rules, we explain the involved ideas. Suppose we have a task to complete and that the task has some parts (subtasks). Assume that each of the parts can be completed on their own and completion of one part does not result in the completion of any other part. We say the parts are compulsory to mean that each of the parts must be completed to complete the task. We say the parts are alternative to mean that exactly one of

the parts must be completed to complete the task. With this setting we state the two basic rules of combinatorics.

Discussion 5.1.2. [Basic counting rules] Let $n, m_1, \ldots, m_n \in \mathbb{N}$.

1. [Multiplication/Product rule] If a task consists of *n compulsory* parts and the *i*-th part can be completed in m_i ways, $i = 1, 2, \ldots, n$, then the task can be completed in $m_1 m_2 \cdots m_n$ ways. 2. [Addition rule] If a task consists of *n alternative* parts, and the *i*-th part can be completed in m_i

ways, $i = 1, \dots, n$, then the task can be completed in $m_1 + m_2 + \cdots + m_n$ ways.

To illustrate these rules once again let us consider the following examples.

Example 5.1.3. 1. How many three digit natural numbers can be formed using digits $0, 1, \cdots, 9$? Identify the number of parts in the task and the type of the parts (compulsory or alternative). Which rule applies here?

Ans: The task of forming a three digit number can be viewed as filling three boxes kept in a horizontal row. Our task has three compulsory parts. Part 1: choose a digit for the leftmost place. Part 2: choose a digit for the middle place. Part 3: choose a digit for the rightmost place.

Multiplication rule applies. Ans: $9 \times 10 \times 10$.

2. How many three digit natural numbers with distinct digits can be formed using digits $1, \cdots, 9$ such that each digit is odd or each digit is even? Identify the number of parts in the task and the type of the parts (compulsory or alternative). Which rule applies here?

Ans: The task has two alternative parts. Part 1: form a three digit number with distinct digits using digits from $\{1, 3, 5, 7, 9\}$. Part 2: form a three digit number with distinct digits using digits from $\{2, 4, 6, 8\}$. Observe that Part 1 is a task having three compulsory subparts. Using multiplication rule, we see that Part 1 can be done in $5 \times 4 \times 3$ ways. Part 2 is a task having three compulsory subparts. So, it can be done in $4 \times 3 \times 2$ ways. Since our task has alternative parts, addition rule applies. Ans: 84.

Remark 5.1.4. There is another way to formulate the above rules. Let A_i be the set of all possible ways in which the i-th part can be completed. In this setting, the multiplication rule can be re-written as: *if $A_1, A_2, \dots, A_n$ are nonempty finite sets, then* $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|$. For the addition rule, note that, as the completion of one part does not result in the completion of any other part, $A_1, A_2, \dots, A_n$ are disjoint. Thus, the addition rule can be re-written as: *if $A_1, A_2, \dots, A_n$ are disjoint, nonempty finite sets, then* $|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$.

5.2 Permutations and combinations

This section is primarily devoted to introduce some very common combinatorial objects and develop ment of methods to count them using the addition rule and multiplication rule.

5.2.1 Counting words made with elements of a set S

The first fundamental combinatorial object one commonly studies is a function $f : [k] \to S$. The set

of all functions from A to B will be denoted by Map(A, B).

Discussion 5.2.1. 1. Let $k \in$ N and let $f \in$ Map($[k]$, S). Then, we may view f as the ordered k-tuple $(f(1), \dots, f(k))$. Thus f is an element of $S^k = S \times S \times \cdots \times S$, k times.

2. Consider an ordered k-tuple $(x_1, x_2, \ldots, x_k)$ of elements of X. If we remove the brackets and the commas, then what we get is $x_1x_2 \ldots x_k$, which is called a word of length k made with elements of X. Thus, the word corresponding to the tuple (a, a, b) is *aab*.

3. Consider a function $f : [3] \rightarrow \{a, b, \ldots, z\}$, defined by $f(1) = a$, $f(2) = a$ and $f(3) = b$. Technically, $f = \{(1, a),(2, a), 3, b)\}$ and the ordered tuple it gives is (a, a, b) and the word related to it is *aab*. Because of this natural one-one correspondence, people use them interchangeably.

Theorem 5.2.2. *Let* $n, r \in$ N *be fixed. Then* $|\text{Map}([n], [r])| = r^n$.

Proof. Forming such a function is a task with n compulsory parts, where each part can be done in r many ways. So, by the product rule, the number of such functions is r^n.

Example 5.2.3. 1. How many functions are there from [9] to [12]?

Ans: 12^9. This task has 9 compulsory parts, where is each part can be done in 12 ways. 2.

Determine the number of words of length 9 made with alphabets from $\{a, b, \ldots, z\}$? Ans: 26^9.

This task has 9 compulsory parts, where each part can be done in 26 many ways.

3. Suppose 3 distinct coins are tossed and the possible outcomes, namely H and T, are recorded. For example, the word $T\ T\ H$ means that the first two coins have shown T and the third coin has shown H. Determine the number of possible outcomes.

Ans: It is the same as the number of words of length 3 made using T and H. So, it is 2^3.

Practice 5.2.4. *1. Let* $n, r \in$ N. *In how many ways can r distinct balls be placed into n distinct boxes?*

2. How many ways are there to make 5*-letter words (words of length* 5*) using the ENGLISH alphabet such that the vowels do not appear at even positions?*

3. Determine the number of possible outcomes if three distinct coins and five distinct dice are tossed?

Discussion 5.2.5. [Use of complements] A simple technique which is used very frequently is counting the complement of a set, when we know the size of the whole set. For example, consider the following question.

How many 5-letter words can be made using the letters *A, B, C, D* that do not contain the string "ADC"? For example, *ADCDD, BADCB* are not counted but *DACAD* is counted. Ans: Let X be the set of all 5-letter words that can be made using *A, B, C, D*. Then $|X| = 4^5$. Consider the sets $A = \{$words in X of the form $ADC * *\}$, $B = \{$words in X of the form $* ADC*\}$, and $C = \{$words in X of the form $* * ADC\}$. We see that $|A| = |B| = |C| = 4^2$. As the sets A, B, C are disjoint, we see that $|A \cup B \cup C| = 3\times4^2$. Hence our answer to the original question is $4^5 - 3\times4^2$. Practice 5.2.6. *1. Determine the number of functions* $f : [6] \rightarrow [5]$ *satisfying* $f(i)$ *6= i for at least two values of i?*

2. How many 5 *digit natural numbers are there that do not have the digit* 9 *appearing exactly* 4 *times?*

5.2.2 Counting words with distinct letters made with elements of a set *S*

We now discuss the next combinatorial object namely the one-one functions. For $n \in$ N, the term *n*-set is used for 'a set of size *n*'. Further, *n*! = 1 · 2 · · · · · *n* and by convention, 0! = 1.

Discussion 5.2.7. [Injections] Let *n, r* ∈ N and *X* be a non-empty set.

1. An injection *f* : [*r*] → *X* can be viewed as an ordered *r*-tuple of elements of *X* with distinct entries. It can also viewed as a word of length *r* with distinct letters made with elements of *X*. The set of all injections from *A* to *B* will be denoted by Inj(*A, B*).
2. If |*X*| = *r*, then a bijection *f* : *X* → *X* is called a permutation of *X*. If *X* = {x_1, . . . , x_r}, then *f*(x_1), . . . , *f*(x_r) is just a rearrangement of elements of *X*.
3. We define P(n, r) := |Inj([*r*], [*n*])|. As a convention, *P*(*n,* 0) = 1 for *n* ≥ 0.

Example 5.2.8. How many one-one maps *f* : [4] → {*A, B, . . . , Z*} are there? Ans: The task of forming such a one-one map has 4 compulsory parts: selecting *f*(1), *f*(2), *f*(3) and *f*(4). Further, *f*(2) 6= *f*(1), *f*(3) 6= *f*(1), *f*(2) and so on. So, by the product rule, the number of one-one map equals 26 · 25 · 24 · 23 = 26!

22! ·

Theorem 5.2.9. [Number of injections *f* : [*r*] → *S*] *Let n, r* ∈ N *and* |*S*| = *n. Then the number P*(*n, r*) = *n*!

(*n*−*r*)!·

Proof. The task is to from an *r*-tuple (*f*(1), . . . , *f*(*r*)) of distinct elements. It has *r* compulsory parts, namely selecting *f*(1), *f*(2), . . ., *f*(*r*) with the condition that *f*(*k*) 6∈ {*f*(1), *f*(2), . . . , *f*(*k* − 1)}, for 2 ≤ *k* ≤ *r*. So, using the product rule, *P*(*n, r*) = |Inj([*r*], [*n*])| = *n*(*n* − 1)· · ·(*n* − *r* + 1) = *n*!

(*n*−*r*)! ·

Practice 5.2.10. *1. How many ways are there to make* 5 *letter words using the ENGLISH alpha bet if the letters must be different?*

2. How many ways are there to arrange the 5 *letters of the word ROY AL?*

3. How many bijections f : [12] → [12] *are there if a multiple of* 3 *is mapped to a multiple of* 3*?*

5.2.3 Counting words where letters may repeat

Consider the word *AABAB*. We want to give subscripts 1*,* 2*,* 3 to the *A*'s and subscripts 1*,* 2 to the *B*'s so that we create words made with A_1, A_2, A_3, B_1, and B_2. For example, one such word is $A_2A_3B_2A_1B_1$. How many such words can we create? Fill the following table to get all such words. Notice that each of these words become *AABAB* when we erase the subscripts.

$A_1A_2B_1A_3B_2$	$A_1A_2B_2A_3B_1$
$A_1A_3B_1A_2B_2$	$A_1A_3B_2A_2B_1$
$A_3A_2B_1A_1B_2$	$A_3A_2B_2A_1B_1$

The following is another useful principle. It is a special case of Exercise 3.1.5.13.

Proposition 5.2.11. [Principle of disjoint pre-images of equal size] *Let A, B be nonempty finite sets and f : $A \to B$ be a function satisfying $|f^{-1}(i)| = k = |f^{-1}(j)|$, for each $i, j \in B$. Then, $|A| = k|B|$. In particular, for $k = 1$ this principle is also called the principle of bijection.*

Let $n_1, \dots, n_k \in$ N. Suppose, we are given n_i copies of the symbol A_i, for $i = 1, \dots, k$. Then, by

an arrangement of these $n_1 + \cdots + n_k$ symbols, we mean a way of placing them in a row. It is a word made with the symbols $A_1, \dots, A_k$ containing the symbol A_i exactly n_i times, $i = 1, \dots, k$. For example, *ABBAA* is an arrangement of 3 copies of *A* and 2 copies of *B*.

Example 5.2.12. 1. How many words of size 5 can be formed using three *A*'s and two *B*'s?

Ans: Let $A = \{$arrangements of $A_1, A_2, A_3, B_1, B_2\}$ and $B = \{$words of size 5 which use three *A*'s and two *B*'s$\}$. For each arrangement $a \in A$, define $Er(a)$ to be the word in B obtained by erasing the subscripts. Then, the function $Er : A \to B$ satisfies:

'for each $b, c \in B$, b 6= c, we have $|Er^{-1}(b)| = |Er^{-1}(c)| = 3!2!$'.

Thus, by Proposition 5.2.11, $|B| = ^{|A|}$

3!2! $=\underline{5!}$

3!2! ·

2. Determine the number of ways to place 4 couples in a row if each couple sits together.

Ans: Let X be the set of all arrangements of A, B, C, D. Let Y be the set of all arrangements of A, A, B, B, C, C, D, D in which both the copies of each letter are together. For example *AACCDDBB* $\in Y$ but *ABBCCDDA* 6$\in Y$. Let Z be the set of all arrangements of $A_h, A_w, B_h, B_w, C_h, C_w, D_h, D_w$ in which A_h, A_w are together, B_h, B_w are together, C_h, C_w are together, and D_h, D_w are together.

In this setting, we need to find the size of Z. So, define $Er : Z \to Y$ by $Er(z)$ equals the arrangement obtained by erasing the subscripts, namely h and w, that appear in z. Notice that each $y \in Y$ has 2^4 pre-images in Z. Now, define $Mrg : Y \to X$ by $Mrg(y)$ equals the arrangement obtained by merging the two copies of the same letters into one single letter. For example, *Mrg*(*BBAADDCC*) = *BADC*. Notice that each x in X has exactly one pre image in Y. By applying the principle of disjoint pre-images of equal size twice, we see that $|Z| = 2^4|Y| = 2^4|X| = 2^4 4!$, as $|X| = 4!$.

Alternate. Instead of writing it in such a laborious way as the above, let us adopt a more reader friendly way of writing the same. A couple can be thought of as one cohesive group (they are to be seated together). So, the 4 cohesive groups can be arranged in 4! ways. But a couple can sit either as "wife and husband" or "husband and wife". So, the total number of arrangements is 2^4 4!.

Theorem 5.2.13. [Arrangements] *Let $n, n_1, n_2, \dots, n_k \in$ N and suppose that we have n_i copies of the symbol (object) A_i, for $i = 1, \dots, k$ and that $n = n_1 + \cdots + n_k$. Then the number of arrangements of these n symbols is* $n!$

$n_1!n_2! \cdots n_k!$.

The formula remains valid even if we take some of the n_i's to be 0.

Proof. Let S be set of all arrangements of the $n_1 + n_2 + \cdots + n_k$ symbols and let T be the set of all arrangements of the symbols $A_{1,1}, \ldots, A_{1,n1}, A_{2,1}, \ldots, A_{2,n2}, \ldots, A_{k,1}, \ldots, A_{k,nk}$. Define a function $Er : T \to S$ by $Er(t)$ equals the arrangement obtained by erasing the second subscripts that appear in t. Notice that each $s \in S$ has $n_1!n_2! \cdots n_k!$ many pre-images. Hence, by the principle of disjoint pre-images of equal size, we have $|T| = n_1! \cdots n_k!|S|$. As $|T| = (n_1 + n_2 + \cdots + n_k)!$, we obtain the desired result.

Assume that some n_i's are 0 (all cannot be 0 as $n \in$ N). Then our arrangements do not involve the corresponding A_i's. Hence we can use the argument in the previous paragraph and get the number of arrangements. As $0! = 1$, we can insert some $0!$ in the denominator.

We have an immediate
special case.

Corollary 5.2.14. *Let $m, n \in$ N. Then the number of arrangements of m copies of A and n copies of B is* $^{(m+n)!}$

$m!n!\cdot$

5.2.4 Counting subsets

As an immediate application of Corollary 5.2.14, we have the following result which counts the number of subsets of size k of a given set S.

Theorem 5.2.15. *Let $n \in$ N and $k \in \{0, 1, \ldots, n\}$. Then the number of subsets of* $[n]$ *of size k is* $\underline{n!}$

$k!(n-k)!\cdot$

Proof. If $k = 0$ or n, then we know that there is only one subset of size k and the formula also gives us the same value. So, let $1 \le k \le n - 1$ and let X be the set of all arrangements of k copies of T's and $n - k$ copies of F's. For an arrangement $x = x_1x_2 \ldots x_n \in X$, define $f(x_1 \ldots x_n) = \{i \mid x_i = T\}$, *i.e.*, the set of positions where a T appears in x. Then, f is a bijection between X and the set of all k-subsets of $[n]$. Hence, the number of k-subsets of $[n] = |X| = |X| =^{\underline{n!}}$

$k!(n-k)!$, by Corollary 5.2.14.

Discussion 5.2.16. 1. For $n \in$ N and $r \in \{0, 1, \ldots, n\}$, the symbol $C(n, r)$ is used to denote the number of r-subsets of $[n]$. The value of $C(0, 0)$ is taken to be 1. Many texts use the word 'r-combination' for an r-subset.

2. Using Theorem 5.2.15, we see that for $n \in$ N$_0$ and $r = 0, 1, \ldots, n$, $C(n, r) = ^{\underline{n!}}$

$r!(n-r)!$. Also it follows from the definition that $C(n, r) = 0$ if $n < r$, and $C(n, r) = 1$ if $n = r$.

3. Let $n \in$ N and $n_1, n_2, \ldots, n_k \in$ N$_0$ such that $n = n_1 + \cdots + n_k$. Then by $C(n; n_1, \ldots, n_k)$ we denote the number $^{\underline{n!}}$

$n_1!n_2!\cdots n_k!$. By Theorem 5.2.13, it is the number of arrangements of n objects where n_i are of type i, $i = 1, \ldots, k$. By convention, $C(0; 0, \ldots, 0) = 1$.

4. If $n \in$ N and $n_1, \ldots, n_{k-1} \in$ N$_0$ with $n_1 + \cdots + n_{k-1} < n$, we also use $C(n; n_1, \ldots, n_{k-1})$ to mean $C(n; n_1, \ldots, n_{k-1}, n - n_1 - \cdots - n_{k-1})$.

5.2.5 Pascal's identity and its combinatorial proof

We aim to supply a combinatorial proof of a very well known identity called the Pascal's identity.

Theorem 5.2.17. [Pascal] *Let n and r be non-negative integers. Then*

$$C(n, r) + C(n, r + 1) = C(n + 1, r + 1).$$

Proof. (This is not the combinatorial proof.) If $r > n$, then by definition all the three terms are zero. So, we have the identity. If $r = n$, then the first and the third terms are 1 and the second term is 0. So, again we have the identity. So, let us take $r < n$. Now we can use the formulas for $C(n, r)$, $C(n, r + 1)$ and $C(n + 1, r + 1)$ to verify the identity.

Sometimes, we want to supply a combinatorial proof of an identity, *i.e.*, by associating the terms on the left hand side (LHS) and the right hand side (RHS) with some objects and by showing a one to one correspondence between them. Before we supply a combinatorial proof of Pascal's identify, the reader is advised to go through the following experiment to discover that proof on their own.

Experiment

Complete the following list by filling the left list with all 3-subsets of $\{1, 2, 3, 4, 5\}$ and the

right

list with 3-subsets of $\{1, 2, 3, 4\}$ as well as with 2-subsets of $\{1, 2, 3, 4\}$ as shown below. Can you match the sets in the left with the sets in the right in some natural way?

$\{1, 2, 3\}$

$\{1, 2, 3\}$

$C(4, 3)$

$\{2, 3, 4\}$

$\{2, 3, 4\}$

$\{1, 2, 5\}$

$\{1, 2\}$

$C(5, 3)$

$C(4, 2)$

$\{3, 4, 5\}$

$\{3, 4\}$

We now present the combinatorial proof of Theorem 5.2.17.

Proof. If $r > n$, then by definition all the three terms are zero. So we have the identity. If $r = n$, then the first and the third terms are 1 and the second term is 0. So, again we have the identity. So, assume that $r < n$.

Let $S = \{1, 2, . . . , n, n + 1\}$ and A be an $(r + 1)$-subset of S. Then, by definition, there are $C(n + 1, r + 1)$ such sets with either $n + 1 \in A$ or $n + 1\ 6\in A$.

Note that $n + 1 \in A$ if and only if $A \setminus \{n + 1\}$ is an r-subset of $\{1, 2, . . . , n\}$. So, the number of $(r + 1)$-subsets of $\{1, 2, . . . , n, n + 1\}$ which contain the element $n + 1$ is, by definition, $C(n, r)$. Also, n

+ 1 ∈/ *A* if and only if *A* is an (*r* + 1)-subset of *{*1*,* 2*, . . . , n}*. So, a set *A* which does not contain *n* + 1 can be formed in *C*(*n, r* + 1) ways.

Therefore, using the above two cases, an (*r* + 1)-subset of *S* can be formed, by definition, in *C*(*n, r*) + *C*(*n, r* + 1) ways. Thus, the required result follows.

5.2.6 Counting in two ways

Let *R* and *C* be two nonempty finite sets and take a function *f* : *R* × *C* → R. View the function written as a matrix of real numbers with rows indexed by *R* and columns indexed by *C*. Then the total sum of the entries of that matrix can be obtained either 'by first taking the sum of entries in each row and then summing them' or 'by first taking the sum of the entries in each column and then summing them', *i.e.*,

x∈*R* *y*∈*C*

X X *x*∈*R* .

f(*x, y*) =X *f*(*x, y*)

(*x,y*)∈*R*× X *f*(*x, y*) *y*∈*C* !

C = X

This is known as 'counting in two ways' and it is a very useful tool to prove some combinatorial identities. Let us see some examples.

Example 5.2.18. 1. [Newton's Identity] Let *n* ≥ *r* ≥ *k* be natural numbers. Then *C*(*n, r*)*C*(*r,*

k) = *C*(*n, k*)*C*(*n* − *k, r* − *k*)*.*

In particular, for *k* = 1, the identity becomes *rC*(*n, r*) = *nC*(*n* − 1*, r* − 1). Ans: Let us use the method of 'counting in two ways'. So, we take two appropriate sets *R* = *{*all *r*-subsets of [*n*]*}* and *C* = *{*all *k*-subsets of [*n*]*}* and define *f* on *R* × *C* by *f*(*A, B*) = 1 if *B* ⊆ *A*, and *f*(*A, B*) = 0 if *B* 6⊆ *A*.

Then given a set *A* ∈ *R*, it has *C*(*r, k*) many subsets of *A*. Thus,

! *C*(*r, k*) = *k*)*.*

X

X *f*(*A, B*) =X *C*(*n, r*)*C*(*r,*

A∈*R*

B∈*C*

A∈*R*

Similarly, given a set *B* ∈ *C*, there are *C*(*n* − *k, r* − *k*) subsets of [*n*] that contains *B*. Hence,

X *B*∈*C* X *A*∈*R* *f*(*A, B*) *k*)*C*(*n* − *k, r* − *k*)*.*

! *C*(*n* − *k, r* −

=X *B*∈*C* *k*) = *C*(*n,*

Hence, the identity is established.

Alternate. We now present the same argument in a more reader friendly manner.

Select a team of size *r* from *n* students (in *C*(*n, r*) ways) and then from that team select *k* leaders (in *C*(*r, k*) ways). So, there are *C*(*n, r*)*C*(*r, k*) ways of selecting a team and it's leaders from the team itself. Alternately, select the leaders first in *C*(*n, k*) ways and out of the rest select another *r* − *k* to form the team in *C*(*n* − *k, r* − *k*) ways. So, using this argument, the number of ways of doing this is *C*(*n, k*)*C*(*n* − *k, r* − *k*).

2. [Important] Let *n, r* ∈ N, *n* ≥ *r*. Then

C(1*, r*) + *C*(2*, r*) + · · · + *C*(*n, r*) = *C*(*n* + 1*, r* + 1)*.* (5.1)

The RHS stands for the class F of all the subsets of $[n + 1]$ of size $r + 1$. Let $S \in F$. Note that S has a maximum element. A moments thought tells us that the maximum element of such a set can vary from $r + 1$ to $n + 1$. If the maximum of S is $r + 1$, then the remaining elements of S have to be chosen in $C(r, r)$ ways. If the maximum of S is $r + 2$, then the remaining elements of S has to be chosen in $C(r + 1, r)$ ways and so on. If the maximum of S is $n + 1$, then the remaining elements of S has to be chosen in $C(n, r)$ ways. Thus, $C(n + 1, r + 1) = C(r, r) + C(r + 1, r) + \cdots + C(n + 1, r) = C(1, r) + C(2, r) + \cdots + C(n, r)$.

Observe that for $r = 1$, it gives us $1 + 2 + \cdots + n =^{n(n+1)}$

2·

Exercise 5.2.19. *1. In a school there are* 17 *girls and* 20 *boys. A committee of* 5 *students is to be formed to represent the class.*

(a) Determine the number of ways of forming a committee consisting of 5 *students. (b) Suppose the committee also needs to choose two different people from among themselves, who will act as "spokesperson" and "treasurer". In this case, determine the number of ways of forming a committee consisting of* 5 *students and selecting a treasurer and a spokesperson among them. Note that two committees are different if*

i. either the members are different, or

ii. even if the members are the same, they have different students as spokesperson and/or treasurer.

(c) Due to certain restrictions, it was felt that the committee should have at least 3 *girls. In this case, determine the number of ways of forming the committee consisting of* 5 *students.*

2. Prove that $C(pn, pn - n)$ is a multiple of p directly from its expression.

3. Determine the number of arrangements of the letters of the word ABRACADABARAARCADA.

4. Prove the following identities using combinatorial arguments.

(a) $C(n, r) = C(n, n - r)$, for non-negative integers n and r.

(b) $C(n, r) = C(r, r)C(n - r, 0) + C(r, r - 1)C(n - r, 1) + \cdots + C(r, 0)C(n - r, r)$ for natural numbers $n \geq r$.

(c) $C(n, 0)^2 + C(n, 1)^2 + \cdots + C(n, n)^2 = C(2n, n)$ for all $n \in$ N.

5. Determine the number of ways of selecting a committee of m people from a group consisting of n_1 women and n_2 men, with $n_1 + n_2 \geq m$.

6. How many anagrams (rearrangements of letters) of MISSISSIP P I are there so that no two S are adjacent?

7. How many rectangles are there in an $n \times n$ square? How many squares are there? 8. Supply combinatorial proofs of the following statements.

(a) For each $n \in$ N, prove that $n!$ divides the product of n consecutive natural numbers. (b) For $m, n \in$ N, the number $(m!)^n$ divides $(mn)!$.

(c) For $n, p \in$ N, the number $C(pn, pn - n)$ is a multiple of p.

(d) Prove combinatorially that $2^n|(n+1)\cdots(2n)$.

9. *If n points are placed on the circumference of a circle and all the lines connecting them are joined, what is the largest number of points of intersection of these lines inside the circle that can be obtained?*

10. *How many ways are there to form the word MATHEMATICIAN starting from any side and moving only in horizontal or vertical directions?*

```
                                  M
                                MAM
                              MATAM
                            MATHTAM
                          MATHEHTAM
                        MATHEMEHTAM
                      MATHEMAMEHTAM
                    MATHEMATAMEHTAM
                  MATHEMATITAMEHTAM
                MATHEMATICITAMEHTAM
MATHEMATICICITAMEHTAMMATHEMATICIAICITAMEHTAMMATHEMATICIANAICITAMEHTAM
```

5.3 Solutions in non-negative integers

There are 3 types of ice-creams available in the market: *A, B, C*. We want to buy 5 ice-creams in total. In how many ways can we do that? For example, we can buy 5 of type *A* or we can buy 3 of *A* and 2 of *C*. In general, suppose we are buying n_1 of type *A*, n_2 of type *B* and n_3 of type *C*. Then, we must have $n_1 + n_2 + n_3 = 5$. So, we want to know the number of different possible tuples (n_1, n_2, n_3) satisfying certain condition(s).

Let us discuss it in a general setup. Recall that $\mathrm{N}_0 := \mathrm{N} \cup \{0\}$. A point $\mathrm{p} = (p_1, \ldots, p_k) \in \mathrm{N}_0^k$ with $p_1 + \cdots + p_k = n$ is called a solution of $x_1 + \cdots + x_k = n$ in non-negative integers or a solution of $x_1 + \cdots + x_k = n$ in N_0. Two solutions $(p_1, \ldots, p_k)$ and $(q_1, \ldots, q_k)$ are said to be the same if $p_i = q_i$, for each $i = 1, \ldots, k$. Thus, $(5, 0, 0, 5)$ and $(0, 0, 5, 5)$ are two different solutions of $x + y + z + t = 10$ in N_0.

Theorem 5.3.1. [Solutions in N_0] *The number of solutions of* $x_1 + \cdots + x_r = n$ *in* N_0 *is* $C(n+r-1, n)$.

Proof. Each solution $(x_1, \ldots, x_r)$ may be viewed as an arrangement of n dots and $r - 1$ bars. 'Put x_1 many dots; put a bar; put x_2 many dots; put another bar; continue; and end by putting x_r many dots.'

For example, $(0, 2, 1, 0, 0)$ is associated to $|\bullet\bullet|\bullet||$ and vice-versa. As there are $C(n + r - 1, r - 1)$ arrangements of n dots and $r - 1$ bars, we see that the number of solutions of $x_1 + \cdots + x_r = n$ in N_0 is $C(n + r - 1, n)$.

Example 5.3.2. Determine the number of words that can be made using all of 3 copies of *A* and 6 copies of *B*.

Ans: Note that this number equals the number of arrangements of 3 copies of *A* and 6 copies of *B*. Hence, this number is $C(9, 3)$.

Alternate. First put the three *A*'s in row. Now put x_1 *B*'s to the left of the first *A*, x_2 *B*'s between the first and the second *A*, x_3 *B*'s between the second and the third *A* and x_4 *B*'s after the third *A*. Thus, we need to find number of solutions of $x_1 + x_2 + x_3 + x_4 = 6$ in N_0. By Theorem 5.3.1, the number is $C(6 + 4 - 1, 6) = C(9, 6)$.

Discussion 5.3.3. The question of finding non-negative integers solutions can also be asked in some other styles.

1. In how many ways can we place 6 indistinguishable balls into 4 distinguishable boxes?

Taking n_i as the number of balls to be put in the *i*-th box, it is asking us to find number of solutions of $n_1 + n_2 + n_3 + n_4 = 6$ in N_0.

2. A multiset is a generalization of a set where elements are allowed to repeat. For example, *{a, b, a}* and *{a, a, b}* mean the same multisets (imagine carrying all of them in a bag). A set is also a multiset. How many multisets of size 6 can be made using the symbols *a, b, c, d*?

   Taking n_a as the number of *a*'s to be put in the multiset and so on, it is asking us to find solutions of $n_a + n_b + n_c + n_d = 6$ in N_0.

Example 5.3.4. 1. Suppose there are 5 kinds of ice-creams available in our market complex. In how many ways can we buy 15 of them for a party?

Ans: Suppose we buy $x_i$ice-creams of the *i*-th type. Then, the problem reduces to finding the number of solutions of $x_1 + \cdot\cdot\cdot + x_5 = 15$ in non-negative integers.