# 1

# SET THEORY



> "The question for the ultimate foundations and the ultimate meaning of mathematics remains open; we do not know in which direction it will find its final solution nor even whether a final objective answer can be expected at all.
>
> "Mathematizing" may well be a creative activity of man, like language or music, of primary originality, whose historical decisions defy complete objective rationalization."
>
> H. Weyl[1]

## 1.1 INTRODUCTION

The fact that you chose to read this book makes it likely that you might have heard of Kurt Gödel,[2] the greatest logician since Aristotle,[3] whose arguably revolutionary discoveries influenced our views on mathematics, physics, and philosophy,

[1] Hermann Klaus Hugo Weyl (1885–1955), German mathematician, Yearbook of the American Philosophical Society, 1943 (copyright 1944).
[2] Kurt Gödel (1906–1978), Austrian–American logician, mathematician, and philosopher.
[3] J.A. Wheeler said that "if you called him the greatest logician since Aristotle you'd be downgrading him" (quoted in Bernstein, J., *Quantum Profiles*, Princeton University Press, 1991. Also in Wang, H. *A Logical Journey,* MIT Press, 1996).

*Principles of Mathematics: A Primer*, First Edition. Vladimir Lepetic.

comparable only to the discoveries of quantum mechanics. Well, even if you have not heard of him I want to start by rephrasing his famous theorem:

*Mathematics is inexhaustible!*

Notwithstanding the lack of a definition of what mathematics is, that still sounds wonderful, doesn't it? At this point, you may not fully understand the meaning of this "theorem" or appreciate its significance for mathematics and philosophy. You may even disagree with it, but I suppose you would agree with me that mathematics is the study of abstract structures with enormous applications to the "real world." Also, wouldn't you agree that the most impressive features of mathematics are its certainty, abstractness, and precision? That has always been the case, and mathematics continues to be a vibrant, constantly growing, and definitely different discipline from what it used to be. I hope you would also agree (at least after reading this book) that it possesses a unique beauty and elegance recognized from ancient times, and yet revealing its beauty more and more with/to every new generation of mathematicians. Where does it come from? Even if you accept the premise that it is a construct of our mind, you need to wonder how come it represents/reflects reality so faithfully, and in such a precise and elegant way. How come its formalism matches our intuition so neatly? Is that why we "trust" mathematics (not mathematicians) more than any other science; indeed, very often we define truth as a "mathematical truth" without asking for experimental verification of its claims? So, it is definitely reasonable to ask at the very beginning of our journey (and we will ask this question frequently as we go along): Does the world of mathematics exist outside of, and independently of, the physical world and the actions of the human mind? Gödel thought so. In any case, keep this question in mind as you go along – it has been in the minds of mathematicians and philosophers for centuries.

The set theory that we start with comes as a culmination of 2000 years of mathematics, with the work of the German mathematician George Cantor[4] in the 1890s. As much as the inception of set theory might have had (apparently) modest beginnings, there is virtually no mathematical field in which set theory doesn't enter as the very foundation of it. And it does it so flawlessly, so naturally, and in such a "how-could-it-be-otherwise" way, that one wonders why it took us so long to discover it. And arguably, there is no concept more fundamental than the concept of the set. (Indeed, try to answer the question: What is a real number without referring to set theory?) Be it as it may, now we have it. We start our journey through the "Principles," with the basic formalism of set theory.

No one shall be able to drive us from the paradise that Cantor created for us.[5]
D. Hilbert

[4]Georg Ferdinand Ludwig Philipp Cantor (1845–1918), German mathematician, the "father" of Set Theory.
[5]David Hilbert (1862–1943), German mathematician.

## 1.2 SET THEORY – DEFINITIONS, NOTATION, AND TERMINOLOGY – WHAT IS A SET?

You are probably familiar with the notion in mathematics of a set as a collection, an aggregate or a "group"[6] of certain "(some)things," or a collection of certain "objects"[7] that form a whole. We assume the existence of some domain of those "objects," out of which our mind will build a "whole." Cantor suggested that one should *imagine a set as a collection into a whole A of definite and separate objects of our intuition or our thought.* These objects are called members or elements of a set. For example, we can consider the set of all planets in the solar system,[8] or the set of all living people on Earth. Or, we can consider the set of all living females on this planet. Those would be well-defined sets, and by the very "definition," that is, the description of the set, our mind effortlessly constructs the concept of a "whole." On the other hand, calling for a set of all tall men, or a set of all big planets, triggers a similar concern. What is "a tall man" or "a big planet?" Obviously, describing a set of real objects by means of their characteristics can be problematic due to the imprecision of everyday language. So, it is fair to say that once the nature of objects defining a set is unambiguously stated, the whole entity, and not the individual elements, becomes the object of our study. Consequently, what we care about is the relationship between different sets as well as the very consistency of the "set" concept.

As you can see, at the very beginning of our discussion, we are introducing a concept that looks, to say the least, pretty vague, especially since we are doing mathematics, which we expect to be the epitome of precision. So, at this point in the process of devising our theory – *The Naïve Set Theory* – we will use the words "*set*" and "*is an element of*" without properly defining them. We will simply assume that we know exactly what they mean and hope that we won't run into any inconsistencies and paradoxes. In addition, we need the basic logical vocabulary consisting of "*not,*" "*and,*" "*or,*" and "*if … then …*." That's it! With so little, how can one satisfy the credo of modern mathematics – a "philosophy" by the name of Cantorism – that *everything (mathematical) is a set*? This idea is not as outlandish as you may think, so I suggest you wait for a while before deciding whether to accept this doctrine or not. Remember the Pythagoreans[9] who thought that everything is a natural number. You can imagine their dismay upon

[6]To be precise, we want to make sure that here by the "group" we do not mean the mathematical term "group" as in Group Theory, but simply a group of certain objects or elements.

[7]The term "object" could be misleading too, for sometimes by the "object" people instinctively think of "(some)thing" that is, a "thing" that can be touched, seen, and so on. Since objects of a set theory can be ordinary things, like pencils, chairs, people, or animals, and they can also be very abstract in nature, like numbers, functions, and ideas, maybe the term "entity" instead of the "object" would be more appropriate.

[8]Of course, "all" in this case, by mathematical standards, might be a somewhat imprecise quantifier, but let's assume at this point that there will be no surprises of striping off a "planetary status" of an object in our solar system, as we have recently witnessed in the case of Pluto.

[9]Religious sect founded by Pythagoras of Samos (ca. 570–495) Ionian–Greek philosopher.

learning of the incommensurability of the side and the diagonal of a square. The discovery of $\sqrt{2}$ must have been a catastrophe for this secluded sect, let alone the pain of disclosing the findings to the uninitiated. Legend has it that for his unfortunate discovery Hippasus[10] was drowned by the members of this mystic brotherhood. Later, we learned about certain other sets of numbers – the set of real numbers, for instance – which is fundamentally more "infinite" than anything we knew before. To understand those we definitely need sets.[11] We may continue on this rather vague path and also say that a set is a "thing" that is a collection of other things (which themselves could be sets) called the elements of the set. These hazy definitions by synonym suffice for most purposes, for our mind is able to grasp (the essence of) the concept regardless of the abstractness of the definition. Indeed, we want these concepts to be sufficiently abstract in order to avoid contradictions, especially when dealing with the foundation of mathematics. At the same time, very few so "simple" ideas in mathematics proved to be so fecund with the repercussions to almost all fields of mathematics. Not surprisingly, Mathematical Logic and Philosophy of Mathematics in particular became exceptionally interesting and rich fields notwithstanding the paradoxes spurred by much ingenious work on the foundations of mathematics and set theory.

So, before we start with the formalism of set theory, I want to tell you something rather funny and interesting, something that will keep showing up over and over again in the foundation of mathematics. This will certainly provoke some curiosity in you and at the same time show you the richness of ideas that set theory contains, and how our mind detects paradoxes in apparently simple concepts – concepts that this very mind came up with. The following is known as the Russell[12] Paradox. (Remember, the notion of "*elementhood*" or "*membership*" does not prevent us from thinking of sets as being elements of (i.e., belonging to) other sets.) So, let's follow Cantor and imagine all the *definite distinguishable concepts of your/our intellect.* One of them could be the idea of unicorns – it doesn't matter that you/we know they don't "exist." (They do exist in your mind, right?) Well, let's think about the collection of definite concepts of our intellect that doesn't contain itself. Let me explain. It is easy to think of, say, a set of all horses (or unicorns if you wish) on Earth. This set obviously represents a set that does not contain itself as a member. A set of horses is not a horse, of course. Now, can you think of a set that would be a member of itself? How about a set of all ideas? It is an idea, right? So is it a member of itself? Or, how about a set of all sets? It is a reasonable idea too. But, it is again also a set, hence a member of itself. Well, let's think about it. Let's call any set that doesn't contain itself

[10]Hippasus of Metapontum (ca. fifth century BC), Pythagorean philosopher.

[11]Could it be that even sets are not "everything"? Well, yes! It is possible that we may need an even more fundamental structure to address, among other things, the even "greater," Absolute Infinities. The discussion of those we leave for some other time.

[12]Bertrand Arthur William Russell (1872–1970), British philosopher, logician, and mathematician.

as one of its elements an ordinary set, say, $\mathcal{O}$ and the one that does – an extraordinary, $\mathcal{E}$. Now, here is what Russell said: Consider a set of all ordinary sets $\mathcal{O}$. It exists – Cantor said so – since it is a distinguishable concept of one's intuition or one's thought. So we could safely claim:

1. $\mathcal{O}$ is an ordinary set!
   Suppose not. Suppose it is extraordinary and thus contains itself as one of its elements. But every set in $\mathcal{O}$ is ordinary. Thus $\mathcal{O}$ is ordinary. But this is a contradiction! Therefore, our assumption was wrong; $\mathcal{O}$ is definitely ordinary. Well, is it? No!? What if we say:
2. $\mathcal{O}$ is an extraordinary set!
   Suppose not. Suppose $\mathcal{O}$ is ordinary. Since $\mathcal{O}$ contains all ordinary sets, it has to contain itself as one of its members. But that makes it extraordinary. This is a contradiction. Our assumption that $\mathcal{O}$ is ordinary was wrong. Therefore, $\mathcal{O}$ is extraordinary.

Obviously (1) and (2) are contradictory.
Here is another well-known example of a finite set, which we cannot properly make out[13]:

Consider two sets of adjectives: set $\mathcal{A}$ of self-descriptive adjectives we call *autologous* (*autological)* and set $\mathcal{H}$ of nonself-descriptive adjectives, called *heterologous* (*heterological*), that is, the set of all adjectives not belonging to $\mathcal{A}$. For example, set $\mathcal{A}$ contains adjectives such as *English*, *finite*, *derived*, and *pentasyllabic*. That is, they do have the properties they describe. On the other hand, set $\mathcal{H}$ contains adjectives such as *German*, *French*, *black, white*, and *monosyllabic*, that is, obviously none of them belongs to $\mathcal{A}$. Now, what about "*heterologous*"? Which set does it belong to? What I am asking is this: Is "*heterologous*" heterologous?

If this sounds confusing to you, and it's perfectly all right if it does, for it is confusing indeed. Here is Russell again with an analogous "story" (and I assure you this is not some silly game of words) to help us out:

> *There is a small town with only one (strange) barber. The strange thing about him is that he shaves all men in town that do not shave themselves. Now, does he shave himself or not?*

So, what are we to make of it? At the very beginning, we are dealing only with two concepts, "*set*" and "*an element of*," and we are faced with a fundamental problem of definitions that seems irresolvable. We cannot allow a seed of contradictions sitting at the very concept we want as our foundation. How do we start?

[13]Due to Kurt Grelling (1886–1942) and Leonard Nelson (1882–1927), German mathematicians and philosophers.

How do we build a fundamental structure of mathematics, a structure precise enough and rich enough, to encapsulate "all of mathematics" and all the rules of inference, without contradictions and without any ambiguities? Mathematicians and philosophers have been thinking about these questions for thousands of years, going back to Euclid's[14] axiomatic treatment of geometry, to Leibnitz's[15] ideas of mathematical logic, to Hilbert's dream of unifying all of mathematics under the umbrella of a formal axiomatic system, to the works of Cantor, Russell, and Whitehead,[16] and many others. In any case, the theory that Cantor developed, indeed a mathematical theory unlike any before, proved to be the best candidate to fulfill that. Mathematics arose on a system of axioms and precise formalism, which we want to be

1. consistent;
2. complete; and
3. decidable.

That a formal system is "consistent" means that we should not be able to prove, in finitely many steps, an assertion and its negation at the same time. *A* and *not-A* cannot (should not) be true at the same time. By "complete" we mean a system that is rich enough to allow us to determine whether *A* or *not-A* is a theorem, that is, a true statement. And finally, "decidable" refers to what is known as "the decision problem" (the famous "Entscheidungsproblem" in German), that is, a procedure, an algorithm by which we can (always) determine, in a finite number of steps, whether something is a theorem or not. That's what we want. Not much to ask for, wouldn't you say? After all, consistent and complete should imply that a decision procedure is at hand. Well, it's not. It can't be done! Mr Gödel said so.[17]

Here is how Hilary Putnam[18] "illustrates" Gödel's theorem:

(i) *That, even if some arithmetical (or set-theoretical) statements have no truth value, still, to say of any arithmetical (or set-theoretical) statement that it has (or lacks) a truth value is itself always either true or false (i.e. the statement either has a truth value or it doesn't).*

[14]Euclid (of Alexandria) (ca. 325–270 BC), Greek mathematician/geometer.
[15]Gottfried Wilhelm Leibniz (1646–1716), German mathematician and philosopher.
[16]Alfred North Whitehead (1861–1947), British mathematician, logician, and philosopher.
[17]"The human mind is incapable of formulating all its mathematical intuitions, that is, if it has succeeded in formulating some of them, this very fact yields new intuitive knowledge, for example, the consistency of this formalism. This may be called the 'incompletability' of mathematics." Kurt Gödel, *Collected Works,* Oxford University Press, 2001.
[18]Putnam, H., *Mathematics Without Foundation,* in Philosophy of Mathematics, 2nd ed., Cambridge University Press, 1983.

(ii) *All and only decidable statements have a truth value.*

*For a statement that a mathematical statement $\mathcal{S}$ is decidable may itself be undecidable. Then, by (ii), it has no truth value to say "$\mathcal{S}$ has a truth value" (in fact falsity; since if $\mathcal{S}$ has a truth value, then $\mathcal{S}$ is decidable, by (ii), and if $\mathcal{S}$ is decidable, then "$\mathcal{S}$ is decidable" is also decidable). Since it is false (by the previous parenthetical remark) to say "$\mathcal{S}$ has a truth value" and since we accept the equivalence of "$\mathcal{S}$ has a truth value" and "$\mathcal{S}$ is decidable", then it must also be false to say "$\mathcal{S}$ is decidable". But it has no truth value to say "$\mathcal{S}$ is decidable". Contradiction.*

Did you get it? Think about it. It literally grows on you. The whole point of all of "this" is that you start getting a "feel" for what mathematics really is and where we are actually "going." Anyway, after this "warm-up," let's start slowly and from the beginning.

First, we assume that there is a *domain,* or *universe* $\mathcal{U}$, of objects, some of which are sets.

Next, we need the formalism in which all our statements about sets can be precisely written – let's call it ***the language of set theory*** $\mathcal{L}$. This formal language contains a specific *alphabet,* that is, a list of symbols that we judiciously use and a number of specific statements that are called *axioms.* What are they? Well, in order to start somewhere and in order to avoid an infinite regress, we choose (there has to be (?)) a set of propositions that are not proved (not provable) but can be used in sound construction of our formalism. In addition, we create a basis for (all?) mathematics, which is inherently beautiful, and thus we can use it as an aesthetical criterion that all other sciences can measure up to. Similarly, there exists a collection of (mathematical) words or symbols that we do not define in terms of others – undefined does not mean meaningless – but simply take as given. Those we call primitives. This idea is as old as mathematics itself. Remember Euclid? The first lines of his *Elements* read as follows:

1. A point is that which has no parts.
2. A curve is length without width.
3. The extremity of a curve is a point.
4. A surface is that which has only a length and a width.
5. The extremity of a surface is a curve, and so on.

Surely, you feel some uneasiness about these statements. Still, the whole gigantic structure of Euclidean geometry, unquestioned for 2000 years, is based on these axioms. Putting aside the controversy among mathematicians on how fundamental these axioms are in general, as well as the question of their effectiveness, these axioms are needed and they are here to stay.

We also need the *formal rules of inference* so that the *language* we use is precise enough to derive all the theorems of our theory.

In addition to the aforementioned four basic symbols, we will soon need some more. So, we list the somewhat extensive alphabet of the language we are going to use throughout the book:

$\in$ : element; a member; $x \in A$ : $x$ is an element of set $A$
$\notin$ : not an element; not a member; $x \notin A$ : $x$ is not an element of set $A$
$\ni$ : such that; sometimes "s.t."
$^c$ : complement; $A^c$: complement of set $A$
$\setminus$ : difference; $A \setminus B$: $A$ difference $B$; sometimes just: $A$ "minus" $B$
$\Delta$ : symmetric difference: $A \Delta B$: symmetric difference of $A$ and $B$
$\subseteq$ : subset; $A \subseteq B$: $A$ is a subset of $B$
$\subset$ : proper subset: $A \subset B$
$\cap$ : intersection: $A \cap B$
$\cup$ : union: $A \cup B$
$\varnothing$ : the empty set
$\times$ : Cartesian product; $A \times B$: Cartesian product of sets $A$ and $B$
$\mathbf{N}$ : the natural numbers
$\mathbf{Z}$ : the integers
$\mathbf{Q}$ : the rational numbers
$\mathbf{R}$ : the real numbers
$\mathbf{Z}^+$ : the nonnegative integers
$\mathbf{Q}^+$ : the nonnegative rational numbers
$\mathbf{R}^+$ : the nonnegative real numbers
$|A|$ : the cardinal number (cardinality) of $A$
$\forall$ : for all; for every; for any; $\forall x \in A$: for every $x$ from $A$
$\exists$ : there exists
$\exists!$: there exists a unique …
$\nexists$ : (same as $\sim \exists$) does not exist
$\wedge$ : and; sometimes also "&"
$\vee$ : or
$\rightarrow$ : "conditional"; "implication"; $a \rightarrow b$ if $a$ then $b$. Sometimes same as "$\Rightarrow$"
$\leftrightarrow$ : "biconditional"; $a \leftrightarrow b$ $a$ if and only if $b$; "iff"; Sometimes same as "$\Leftrightarrow$"
$\sim$ : "negation"; "it is not the case that"; "opposite of"
$=$ : equal
$\equiv$ : equivalent
iff: "if and only if"; "$\Leftrightarrow$"; "$\leftrightarrow$"

**Definition 1.1** A set is said to be a well-defined set iff there is a method of determining whether a particular object is an element of that set.

The precise "description" of a set and its elements is based on the following axioms.

**Axiom 0 (Set Existence)**[19] There exists a *set*, that is, $\exists A\ (A = A)$. In other words, we postulate that there exists something, a "thing," an entity, we call a *set.*

Once a set $A$ is given, we say that "*a is an element of A*" or that "*a is a member of A,*" and we write $a \in A$. Similarly, if $a$ is not a member of $A$, we simply write $a \notin A$.

It is worth mentioning again that the expression "*an element of,*" that is, an elementhood relation, is also the elemental concept for which it is difficult to find a suitable alternative, so we also take it as an undefined predicate.

**Example 1.1**

$$A = \{a, b, c, d, e, f\}$$

is a set whose elements are $a, b, c, d, e, f,$ that is, $a \in A, b \in A, c \in A,$ and so on. This is nicely illustrated by the Venn diagram (Figure 1.1).

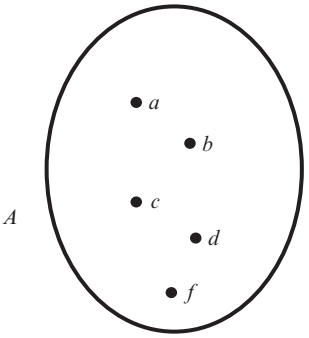



**Figure 1.1** Venn diagram

Often it is convenient, especially when it is impossible to list all the elements of a set, to introduce a set using the so-called set-builder notation. We write

$$A = \{x | P(x)\}$$

and we read: $A$ is a set of all $x$, such that $P(x)$, where $P(x)$ designates some property that all $x$'*s* possess, or $P$ is a condition that specifies some property of all objects $x$.

[19] We will have more to say about these axioms later.

For instance, if we want $A$ to be a set of all natural numbers greater or equal to 5 we write:

$$A = \{x |\, x \geq 5, \quad x \in \mathbf{N}\}$$

Certainly nothing prevents us from considering a set whose elements are also sets. In other words, we can have a set $X = \{x, y, w, z\}$, where $x$, $y$, $w$, and $z$ are sets themselves. ■

**Example 1.2** Suppose we consider

$$X = \{\text{Alice}, \text{Bob}\}$$

as a set whose two elements are persons Alice and Bob. *Set X* is definitely different from set, say,

$$Y = \{\text{Alice}, \{\text{Bob}\}\}$$

which also has two elements, but this time the elements are: Alice and $\{Bob\}$, that is, the element $\{Bob\}$ is itself a set containing one element – *Bob*.

Formally, we write:

$$\text{Alice} \in Y, \text{Bob} \notin Y, \text{but} \{\text{Bob}\} \in Y$$

Of course, we could have constructed a set

$$Z = \{\{\text{Alice}, \{\text{Bob}\}\}\}$$

which has only one element, namely, $Y$. Do you see why? It may help if we represent sets by Venn diagrams, where $X, Y$, and $Z$ (Figure 1.2) look as follows:

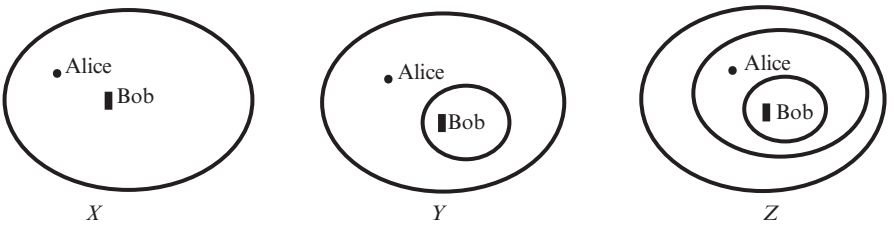



**Figure 1.2** Sets *X, Y,* and *Z*

■

**Axiom 1 (Axiom of extensionality)** A set is uniquely determined by the elements it contains, that is, two sets are considered equal if they have the same elements. Less clearly but often said: a set is determined by its extension.

**Example 1.3** Sets $A = \{a, b, c, d\}$ and $B = \{d, a, a, a, b, c, c, d\}$ are considered the same, that is, we say that $A = B$. ■

So, we have

**Definition 1.2** Given sets $A$ and $B$, we say that $A$ equals $B$, and we write $A = B$ if and only if every element of $A$ is an element of $B$ and every element of $B$ is an element of $A$. For the sake of completeness and more precision (at this point maybe prematurely[20]), using formal logic notation, we express this as follows:

$$A = B \leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)$$

**Definition 1.3** Given two sets $A$ and $B$, we say that $A$ is a subset of $B$, and we write $A \subseteq B$ if and only if every element of $A$ is also an element of $B$ (Figure 1.3), that is,

$$A \subseteq B \leftrightarrow (\forall \ x \in A, x \in B)$$

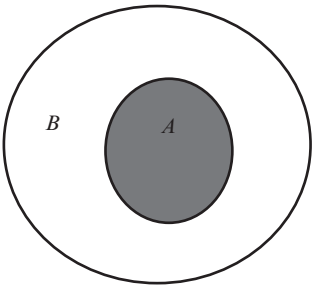



**Figure 1.3** Subset $A \subseteq B$

Note that $B$ could be "larger" than $A$, that is, that all elements of $A$ are elements of $B$, but not all elements of $B$ are elements of $A$. To distinguish between these subtleties, we state the following

**Definition 1.4** Given two sets $A$ and $B$, we say that $A$ is a proper subset of $B$, $A \subseteq B$, if and only if every element of $A$ is an element of $B$, but not all elements of $B$ are elements of $A$.

Equality of sets can now be restated as

$$A = B \leftrightarrow A \subseteq B \& B \subseteq A$$

[20]This formalism will become more clear after you have studied Chapter 2.

What we are saying here is that two sets are considered equal solely on the basis of their elements (i.e., what's in the sets and how many) and not on the "arrangement" or a repeat of some of the elements in the respective sets.

**Example 1.4** Show that, if a set $A$ is a set of all integers $n$, where every $n$ is expressible as $n = 2p$, with $p \in \mathbf{Z}$, that is,

$$A = \{n \in \mathbf{Z} | n = 2p, \quad p \in \mathbf{Z}\}$$

and $B$ analogously described as

$$B = \{m \in \mathbf{Z} \, | m = 2q - 2, \quad q \in \mathbf{Z}\}$$

then $A = B$.

**Solution** Set $A$ is the set of all even integers. We would like to see whether any integer of the form $2p$, for some $p \in \mathbf{Z}$, can also be written in the form $2q–2$, for some $q \in \mathbf{Z}$. Suppose there is an $n \in \mathbf{Z}$, such that $n = 2p$, for some integer $p$ we want to find an integer $q$, so that $n = 2q - 2$. Thus,

$$\begin{aligned} 2q - 2 &= 2p \\ 2q &= 2p + 2 = 2(p + 1) \\ q &= p + 1 \end{aligned}$$

Therefore, for $n = 2p$, and $p \in \mathbf{Z}$, $q = p + 1$. It follows that

$$2q - 2 = 2(p + 1) - 2 = 2p + 2 - 2 = 2p$$

Hence, $A \subseteq B$.

Let's now assume that an integer can be expressed as $m = 2q - 2$, for some $q \in \mathbf{Z}$. Suppose, furthermore, that

$$2p = 2q - 2 = 2(q - 1)$$

that is,

$$p = q - 1$$

So, if $m = 2q - 2$, with $q \in \mathbf{Z}$, we write

$$2p = 2(q - 1) = 2q - 2$$

We conclude that $B \subseteq A$. Since $A \subseteq B$ and $B \subseteq A$, it follows that $A = B$ by definition of set equality. ■

**Example 1.5** Let $A$ be a set of all solutions of the equation $x^2 = 2x$, and let $B$ be a set of all solutions of the equation $(x-1)^2 = 1$. Then, it is easy to see that $A = B$. ■

**Axiom 2 (Comprehension axiom)**[21]

(i) For any *reasonable*[22] property $P$, there exists a set containing exactly those elements that are defined by that property; In particular, mathematical entities that have a certain property in common constitute a set.

Certainly nothing prevents us from considering a set whose elements are also sets. In other words, we can have a set $X = \{x, y, w, z\}$, where $x, y, w$, and $z$ are sets themselves. So we postulate:

(ii) Sets are mathematical entities, and, hence, they may in turn appear as elements of a set.

This is one of the reasons why one should not restrict oneself on a style of letters that represent sets. Thus, although we will most frequently use capitals to designate sets, occasionally it will be more convenient to use lowercase letters.

**Example 1.6** Let $x_1, x_2, \ldots, x_n$ be a collection of $n$ sets, then

$$X = \{x_1, x_2, \ldots, x_n\}$$

is also a set (Figure 1.4).

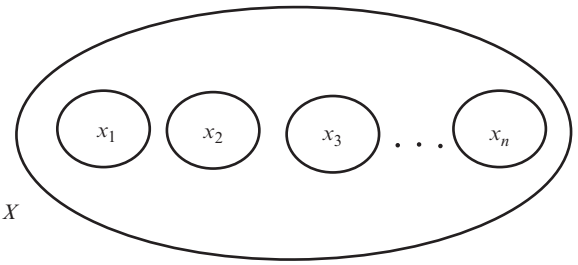



**Figure 1.4**

[21] This is sometimes called the Comprehensive principle.

[22] What is "*reasonable*" is debatable, and in any case a rather vague concept. We won't be discussing these subtleties here.

Having elements of a set being sets themselves gives us more flexibility in dealing with only one kind of object. Thus, we don't need to postulate the existence of every possible element of the various structures we intend to study. It follows, let's emphasize this again, that every set $x$ is a unique element of another set, namely, $\{x\}$.

After accepting the fact that the elements of a set are sets, let's take a closer look at Axiom 2: Let $X$ be a set, and let $Y$ be a set whose elements are exactly those elements $x \in X$ with a property $P$, that is,

$$Y = \{x \in X | P(x)\}$$

So, let the particular property be $x \notin x$. (Remember, $x$ is a set.) In other words, whatever set $X$ may be, if

$$Y = \{x \in X | x \notin x\}$$

then for every $y$,

$$y \in Y \quad \text{iff} \quad y \in X \ \text{ and } \ y \notin y \tag{*}$$

Is it possible that $Y \in X$? Let's see. If $Y \in X$, we have two possibilities: either $Y \in Y$ or $Y \notin Y$. Suppose $Y \in Y$. Then, from $Y \in X$ and (*) it follows that $Y \notin Y$ – obviously a contradiction. Suppose that $Y \notin Y$. Then, again, from $Y \in X$ and (*) it follows that $Y \in Y$ – a contraction again. We conclude that it is impossible that $Y \in X$. (You may remember this argument from before.)

Now, let me digress a bit and say something about two very important concepts that will be discussed in much more detail in Chapter 4. Many readers are familiar with the concepts of *relations* and *function*: For the time being, let's just say that:

A *relation* $R$ is uniquely determined by pairs of elements $x$ and $y$ that are somehow related.

A *function* $f : X \to Y$ is uniquely determined by the pairs of two objects, an argument $x \in X$ and a functional value $f(x) \in Y$.

Now let's look at these via Axioms 1 and 2: For instance, the usual relation $\leq$ on the set of natural numbers describes a particular property, so we can construct a set $R$ consisting of pairs of natural numbers $(a, b)$ where $a \leq b$, that is

$$R = \{(a, b) | a \leq b, a, b \in \mathbf{N}\}$$

Similarly, we think of a function $f$ as the following set of pairs:

$$f = \{(x, f(x)) | x \in X, f(x) \in Y\}$$

■

**Axiom 3** There exists a set $\mathcal{U}$, called the universal set, such that for all sets $A$, if $x$ is an element of $A$, then $x$ is an element of $\mathcal{U}$ (Figure 1.5). Symbolically,

$$\forall A \ (x \in A \rightarrow \ x \in \mathcal{U})$$

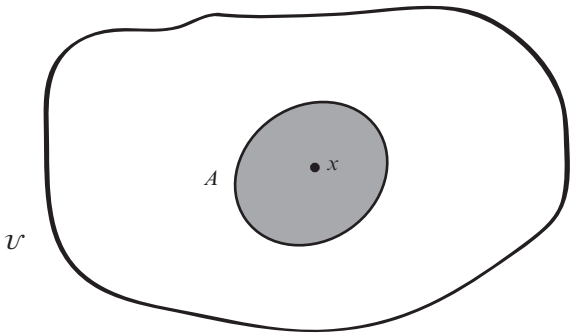



**Figure 1.5**

**Axiom 4** If $x \in \mathcal{U}$ and $A$ is a set, the statement $x \in A$ is a proposition that can either be true or false, but not both.

Saying something so "obvious" is not that trivial, as will become evident shortly.

**Example/Exercise 1.7**

(i) Is $a = \{a\}$?
(ii) Is $a \in \{a\}$?
(iii) Is $a \subseteq \{\{a\}\}$?
(iv) Is $a \in \{\ a, \{a\}\}$?

## 1.3 SETS GIVEN BY A DEFINING PROPERTY

As we have seen in the previous section, we often describe sets the following way:

$$A = \{x | P(x)\}$$

and we say: $A$ is a set of all $x$ such that $P(x)$, where $P(x)$ designates some property that all $x$'s possess, or $P$ is a condition that specifies some property of all objects $x$. In other words, $x \in A \leftrightarrow P(x)$. (see Axiom 2).

*Note:* Some sets have a universally accepted notation, so let's just agree at this point, without further explanation, to denote the set of natural numbers[23]

$$\mathbf{N} = \{\ 0, 1, 2, 3,\ \ldots\ \}$$

the set of integers

$$\mathbf{Z} = \{\ \ldots\ -3, -2,\ -1, 0, 1, 2, 3,\ \ldots\ \}$$

the set of rational numbers (which we will define later) $\mathbf{Q}$, and the set of real numbers (also to be defined later), $\mathbf{R}$.

**Example 1.8** If, for instance, we say

$$P(x)\ :\ x \in \mathbf{N} \quad \text{and}\ \ x\ \ \text{is even}$$

then, in set-builder notation, we write

$$\{x | P(x)\}$$

by which we mean the set of all natural even numbers. ■

**Example 1.9** $A = \{x \in \mathbf{N} | 10 \leq x \leq 25\} = \{10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25\}$, that is, the set $A$ is a set of all natural numbers greater than or equal to 10, and less than or equal to 25. ■

**Definition 1.5 (The empty set)** A set with no elements is called the **empty set**, denoted by the symbol $\varnothing = \{\}$.

**Definition 1.5′** A set $\varnothing$ is said to be an empty set if

$$\varnothing = \{x | x \neq x\}$$

Equivalently, we can argue as follows: let $X$ be a set and let there be a set $A = \{X | X \neq X\}$. Then, $X \in A \Rightarrow X \neq X$, which is a contradiction. Thus, $A$ is empty.

The "existence" of the empty set is postulated by

**Axiom 5 (Empty set (null set) axiom)** There is a set with no elements.

[23]Many authors do not include 0 in $\mathbf{N}$ (in particular, for historical reasons) and, indeed sometimes that may be more convenient, and they reserve the following notation for nonnegative integers: $\mathbf{Z}^+ = \{0, 1, 2, 3, \ldots\} = \mathbf{N} \cup \{0\}$.

**Example 1.10** Here are some examples of empty sets:

(i) $\{ n \in \mathbf{N} | n < 0\} = \varnothing$
(ii) $\{x \in \mathbf{Q} | x^2 = 2\} = \varnothing$
(iii) $\{x \in \mathbf{R} | x = x + 1\} = \varnothing$
(iv) $\{x \in \mathbf{R} | x^2 < 0\} = \varnothing$ ■

**Example/Exercise 1.11** Determine whether or not, and why, are any of the following sets empty:

(i) $A = \{\{\varnothing\}, \{\{\varnothing\}\}\}$
(ii) $B = \{\{\{\varnothing\}\}, \{\varnothing\}, \{\{\{\varnothing\}\}\}\}$
(iii) $C = \{\{\{\{\varnothing\}\}\}\}$

A remarkable property of the empty set is given by the following:

**Theorem 1.1** A set with no elements is a subset of any set, that is, if $A$ is any set, and $\varnothing$ is the empty set, then

$$\varnothing \subseteq A$$

***Proof*** Suppose that is not true, that is, suppose that there exists a set $\varnothing = \{\ \}$ (with no elements), and a set $A$ such that $\varnothing \nsubseteq A$. That would mean, by definition of a subset, that there would be an element of $\varnothing$, which is not an element of $A$. But there can be no such element, since $\varnothing$ has no elements by definition. This contradiction leads us to conclude that the assumption $\varnothing \nsubseteq A$ was wrong; therefore, the theorem is true. ■

**Example/Exercise 1.12** Show that $\{\varnothing\} \subseteq A$ for every set $A$.

You can think of this yet another way. *Any* set $X$ is defined by a property $P$, possessed by all of its members, that is, if $x \in X$, then $x$ has a property $P$. In particular, all elements of $\varnothing$ have to be defined by a certain property $P$, that is, if $x \in \varnothing$, then $x$ has a property $P$. But, it is false to say that $x$ is an element of $\varnothing$ (since $\varnothing$ has no elements), and since a false statement implies any proposition, it is true that if $x \in \varnothing$, then $P$ holds for all the elements of $\varnothing$. Now, since $P$ is a property defining a set $X$, it follows that $\varnothing \subseteq X$. All of this, as much as it may sound confusing to you now, will become more clear after you have studied Chapter 2.

Now you can try to prove the following:

**Corollary 1.1** The empty set is unique, that is, there is only one set with no elements.

If you accept Axioms 3 and 4, then it is fun to contemplate the next claim, which might otherwise sound as an outrageous doctrine of set theory.

**Claim** Everything (mathematical?) is a set.

The "Proof" would go something like this:

Suppose there is a (mathematical) object $X$ that is not a set. Then, $X$ has no elements hence, $X$ is equal to an empty set by Axiom 3, which contradicts the assumption that it is not a set. ■

This is pretty cute, don't you think? And, as a very fundamental concept, it will prove to be very useful. However, as a little exercise, try to think how you would dispute the aforementioned proof.

**Axiom 6 (Pairing axiom)** For any two sets $X$ and $Y$, there is a set whose elements are these two sets, namely $\{X, Y\}$. We call the set $\{X, Y\}$ the **unordered pair** or **doubleton** of $X$ and $Y$, that is

$$\{X, Y\} = \{Z | Z = X \text{ or } Z = Y\}$$

**Theorem 1.2** Given two sets $X$ and $Y$ there is a *unique* set $Z$ whose elements are $X$ and $Y$.

***Proof*** Since Axiom 6 established the existence of at least one set $Z$, whose elements are $X$ and $Y$, the only thing we need to show is its uniqueness. Suppose then that there is another set $Z'$ whose elements are also $X$ and $Y$. But if $X$ and $Y$ are the elements of both $Z$ and $Z'$, by the axiom of extensionality, we have that $Z = Z'$. ■

The axiom of pairing gave us enough means to construct more sets, starting from just the empty set.

**Example 1.13** One way of constructing many simple sets, each having at most two elements, is as follows:

$$\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\{\varnothing\}, \{\{\varnothing\}\}\}, \ldots$$ ■

From Axiom 6, it also follows that if $X = Y$, then $\{X, X\} = \{X\}$. For obvious reasons, we call this set the **singleton** $\{X\}$, or singleton of $X$. This is formalized by

**Theorem 1.3** For any set $X$, there is a set whose only element is $X$.

As you can see, the key feature of set theory is that following Axioms 1–6 we can, in principle, construct a set from any object, or collection of objects, satisfying a certain property $P$ and consider that as a mathematical object in its own right. In other words, we could consider a set $X$, which is a set of all sets $x$ with a property $P$, that is

$$X = \{x | x \text{ is a set with property } P\}$$

As much as this principle is powerful, it has some fatal flaws. Consider this:

Let ***One*** be a set of all one-element sets, that is

$$\mathbf{One} = \{x | x \text{ is a one-element set}\}$$

Then nothing prevents us from forming the one-element set $\{\mathbf{One}\}$ whose only element is **One**. Immediately you recognize a Russell-like paradox:

$$\mathbf{One} \in \{\mathbf{One}\} \in \mathbf{One}$$

This can get even more intriguing. By Axiom 1, we can construct a set of (all) sets

$$\mathbf{U} = \{x | x \text{ is a set}\}$$

Since **U** is a set, it follows that $\mathbf{U} \in \mathbf{U}$. Obviously, in order to avoid circularities such as this one, we cannot treat **U** as any other "normal" set. We will have to say more about this later.

For now, let me incite your curiosity a bit more, especially in case you still have some doubts about the existence of the empty set. Let's assume the existence of the so-called **pure sets**, that is, sets that would exist even if there was nothing else but sets – no you and me, no people, no stars and planets, and so on, and simply refer to them as *Sets* (with a capital "*S*"). While the existence of the empty set $\varnothing$ becomes evident right away, we can immediately conceive the set whose only member is the empty set, that is, $\{\varnothing\}$ and, unsurprisingly, the next would be $\{\{\varnothing\}\}$, followed by $\{\varnothing, \{\varnothing\}\}$, and so on and so forth. So, we recognize the collection of sets mentioned in the previous example as pure sets – *Sets*. Observe that their "nature" is rather unique. That is, all *Sets* are sets but sets are not *Sets.* (The set of horses is not a *Set*.) After inaugurating the concept of *Sets* why not construct additional (particular) ones, respectively, assign familiar names to them, and thus obtain "something" from "nothing." One way to do it would be:

$$\varnothing = \mathbf{0}$$

$$\{\varnothing\} = \mathbf{1}$$

$$\{\{\varnothing\}\} = \mathbf{2}$$

$$\{\{\{\varnothing\}\}\} = \mathbf{3}$$

and so on.

The other way would be:

$$\mathbf{0} = \varnothing$$
$$\mathbf{1} = \{\varnothing\}$$
$$\mathbf{2} = \{\varnothing, \{\varnothing\}\}$$
$$\mathbf{3} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$$

and so on.

Certainly, you can think of some other way to construct "something" from "nothing."

However, before continuing, do

**Example/Exercise 1.14** Prove that $\varnothing \neq \{\varnothing\}$.

**Definition 1.6** Given sets $X$ and $Y$, we say that

$$\langle X, Y\rangle = \{\{X\}, \{X, Y\}\}$$

is an ordered pair.

Analogously, we define an ordered $n$-tuple:

**Definition 1.7** Let $X_1, X_2, X_3, \ldots, X_n$ be sets where $n \in \mathbf{N}, n \geq 3$. We define an ordered $n$-tuple recursively as follows:

$$\langle X_1, X_2, X_3, \ldots, X_n\rangle = \langle X_1, \langle X_2, X_3, \ldots, X_n\rangle\rangle$$

**Theorem 1.4** For any sets $X, Y, U, V, \langle X, Y\rangle = \langle U, V\rangle$ iff $X = U$ and $Y = V$.

***Proof*** That $X = U$ and $Y = V$ implies $\langle X, Y\rangle = \langle U, V\rangle$ is trivial, so we need to examine only that $\langle X, Y\rangle = \langle U, V\rangle$ implies $X = U$ and $Y = V$.

Suppose that $\langle X, Y\rangle = \langle U, V\rangle$ which by definition means that

$$\{\{X\}, \{X, Y\}\} = \{\{U\}, \{U, V\}\} \qquad (*)$$

We should consider two cases: (i) $X = Y$ and (ii) $X \neq Y$.

(i) If $X = Y$ then

$$\langle X, Y\rangle = \{\{X\}, \{X, Y\}\} = \{\{X\}, \{X, X\}\} = \{\{X\}, \{X\}\} = \{\{X\}\}$$

is a singleton, so $\langle U, V\rangle$ has to be a singleton too. Thus, $U = V$. But that means that

$$\{\{U\}, \{U, V\}\} = \{\{U\}, \{U, U\}\} = \{\{U\}, \{U\}\} = \{\{U\}\}$$

With the assumption that equality in $(*)$ holds, we have that $\{\{X\}\} = \{\{U\}\}$, that is, $X = U$ hence,

$$X = Y = U = V$$

(ii) If $X \neq Y$ then from (*) it follows that the singleton $\{X\}$ must correspond to the singleton $\{U\}$ and, likewise, the doubleton $\{X, Y\}$ corresponds to the doubleton $\{U, V\}$. We conclude that

$$X = U \quad \text{and} \quad Y = V$$ ■

**Definition 1.8 (Cardinal number)** Let $A$ be a set. If there are exactly $n$ *distinct* elements in $A$, where $n$ is a finite natural number, we say that the set $A$ is a **finite set** and that $n$ is the **cardinality** of $A$, or that $n$ is the **cardinal number** of $A$, and we denote cardinality by $|A|$, (Figure 1.6).

You may have an uneasy feeling about this definition. Considering the fact that $A$ was said to be a finite set, the definition seems to be too restrictive. Everything is fine if a set has, say, 3175 elements – the cardinal number is 3175. Naturally, one would ask: what about sets that have infinitely many elements? How would we characterize the "number" of elements of an infinite set? After all, the issue of infinities (as we will see shortly) is *the* issue of set theory. It turns out that this is one of the most intuitively difficult mathematical concepts of the theory. Can we "enumerate" a set with infinitely many members regardless of their "nature?" Cantor used the symbol $\overline{\overline{A}}$ to indicate the cardinal number of set $A$, emphasizing double abstraction: first from the nature of elements and second from their order, and he said:

> *Every set A has a definite* ***"power" which we will call its "cardinal number."*** *We will call by this name the general concept, which by means of our active faculty of*

*thought arises from the set A when we make abstraction of its various elements x and of the order in which they are given.*

*… This number has an existence in our minds as an intellectual image or projection of the given set.*

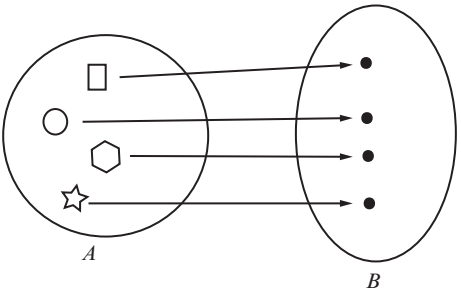



**Figure 1.6** The concept of cardinality for a four-element set A à la Cantor

With all that said, and with tongue-in-cheek, let's say for the time being that the *cardinality* of a set means the "number" of the elements of a set or, even better, the "size" of a set.

**Example 1.15** Let $A$ be the set from Example 1.9, then $|A| = 16$. ■

**Example 1.16** What is $|\varnothing|$?
Well, since the empty set $\varnothing$ has no elements, it follows that $|\varnothing| = 0$. ■

**Definition 1.9** A set is said to be **infinite** if it is not finite.

The existence of the "infinite" set is provided by

**Axiom 7 (Axiom of infinity)** There exists a set $I$ that contains the empty set $\varnothing$ and the singleton of each of its members, that is

$$\varnothing \in I \;\&\forall x \in I, \{x\} \in I$$

**Example 1.17** Let $I$ be a set defined in Axiom 7. Observe that $\varnothing \in I$, but also, $\{\varnothing\} \in I$, $\{\{\varnothing\}\} \in I$, …. So, with this family of complex singletons, we have indeed obtained an infinite set of more abstract nature:

$$I = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \ldots\}$$ ■

**Example 1.18** Here is how Dedekind[24] argued that at least one infinite set exists: *Given some arbitrary thought $\tau_1$, there is a separate thought $\tau_2$, namely that $\tau_1$ is an object of thought. But there also exists a thought $\tau_3$, that is, a thought of $\tau_1$ and $\tau_2$. And so on ad infinitum. Thus, set of thoughts is infinite.* ■

The claims of the next two examples are usually accepted as obvious.

**Example 1.19** A set of all natural numbers **N** is infinite. ■

**Example 1.20** A set of all integers **Z** is infinite. ■

We will discuss the intricacies of infinite sets in a little while.

**Definition 1.10** We say that two sets $A$ and $B$ are **equivalent** (or **equinumerous**) or that they have the same cardinality, and we write

$$A \sim B \quad \text{iff} \quad |A| = |B|$$

Following Cantor, we say that cardinal number of a set $A$ is what $A$ has in common with all sets equivalent to $A$.

**Example 1.21** Given sets $A = \{1, 2, 3\}, B = \{a, b, c\}$, and $C = \{b, c, a\}$, we say that $A \sim B$, and $A \sim C$, but only $B = C$. ■

**Theorem 1.5** Given three sets $A, B, C$, such that $A \sim B$, and $B \sim C$, then $A \sim C$.

***Proof*** Easy. You should do it! ■

Now that we have a rudimentary knowledge of sets, in order to finish this section and have some fun, I have to tell you something else. Something about those strange sets I have mentioned in the introduction. In a sense, you may think of what follows as a "historical" progress toward the paradoxes Russell pointed out to us.

With the concept of a set handy, and assuming also that the attributes that apply to a set are not mutually contradictive, then, by an *extension* of such an idea, we can easily contemplate a set that contains sets as its elements. Why not, right? For example, the concept of a finite set $F$ is easily conceivable. Its extension $\mathcal{F}$ would be a set of all sets with finitely many elements, that is

$$\mathcal{F} = \{F | F \text{ is a finite set}\} \tag{1.1}$$

[24] Julius Wilhelm Richard Dedekind (1831–1916), German mathematician.

Similarly, with the idea of an infinite set $I$ (say, a set $\mathbf{N}$) let's define its extension as a set

$$\mathcal{I} = \{ I \,|I \text{ is an infinite set}\} \tag{1.2}$$

Observe that, while all the elements of $\mathcal{F}$ are finite sets, $\mathcal{F}$ itself is an infinite set. That makes $\mathcal{F}$ not a member of itself, but a member of $\mathcal{I}$. Symbolically,

$$\mathcal{F} \notin \mathcal{F}, \text{ and } \mathcal{F} \in \mathcal{I}$$

On the other hand, it is clear that

$$\mathcal{I} \in \mathcal{I}$$

Again, do you see where we are going? Let's call on Russell again. Consider the concept of a "*set that is not a member of itself,*" and let's call its extension

$$\mathcal{R} = \{X|X \text{ is a set } \& \, X \in X\} \tag{1.3}$$

From (1.1) – (1.3), we see that $\mathcal{F} \in \mathcal{R}$ and $\mathcal{I} \notin \mathcal{R}$. But how about $\mathcal{R}$? Is it a member of itself or not? From the aforementioned discussion, it follows that

$$\mathcal{R} \in \mathcal{R} \text{ iff } \mathcal{R} \notin \mathcal{R} \tag{1.4}$$

But this is impossible! Either $\mathcal{R}$ is a member of itself or not. Claim (4) is a contradiction par excellence. Thus, we state (we are forced to state):

**Theorem 1.6** There is no set $\mathcal{R}$ such that

$$\mathcal{R} = \{X \,|X \text{ is a set } \& \, X \notin X\}$$

The reason I keep on mentioning this quintessential paradox is because of its profound mathematical/philosophical importance. I'll stop here abruptly, again quoting Russell: "*Whatever involves all of a collection must not be one of the collection.*" What he actually said was: just forget about those "crazy" sets, consider only those sets that are ordinary.[25] Can you do that? Can you just forget about the "crazy" sets? I could never do that. They keep coming up in many different branches of mathematics, physics, and philosophy. It seems our mind, once having become aware of them, simply cannot let go. In any case, we continue our discussion of sets by introducing the formalism that will enable us to "calculate" and discover even more interesting "stuff."

[25] At this point, you may want to revisit the discussion on ordinary and extraordinary sets on pages 4 and 5.

## 1.4 THE ALGEBRA OF SETS

In order to reasonably carry on a mathematical discussion in the context (a set) of specific elements, we can often visualize the entity whose existence we postulated in Section 1.2 by Axiom 1. For example, we may consider a set of all students at the university, or we may consider a set of all books in your school library, a set of all animals in the zoo, or a set of all real numbers, and so on. In each of these cases, we call this a universe of discourse, or the universal set of the given discourse. So, we formally state

**Definition 1.11** By universal set $\mathcal{U}$, we mean the set of all the elements *under discussion* (all the objects under consideration).

Note the important qualification "*under discussion*" in the aforementioned definition. Without it, the concept of a universal set would create a rather difficult problem. Namely, one could be tempted to consider the universal set $\mathcal{U}$ as a set of all "objects," that is, a set of everything. Why not, right? But then, in particular, $\mathcal{U}$ would contain itself as a member, and that would be a problem indeed as we have indicated at the beginning of this chapter.

**Definition 1.12** Given a universal set $\mathcal{U}$, and $A$ and $B$ the two subsets of $\mathcal{U}$, we define the **union** of $A$ and $B$, denoted $A \cup B$, as a set of all the elements $x \in \mathcal{U}$, such that $x$ is an element of $A$ or $x$ is an element of $B$ (Figure 1.7), that is

$$A \cup B = \{x \in \mathcal{U} | x \in A \text{ or } x \in B\}$$

Note that in this definition "or" is the inclusive "or" (as opposed to "either–or").

**Example 1.22** Let $A$ be a set of all even whole numbers, that is, all even integers, and let $B$ be a set of all odd whole numbers, that is, all odd integers. Then, $A \cup B$ represents the set of all whole numbers, that is, the set of all integers. Recall, we denoted that set by the symbol $\mathbf{Z}$. ■

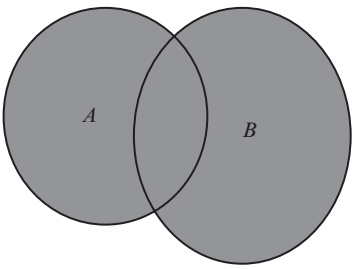



**Figure 1.7** $A \cup B$

**Example 1.23** Given two sets $X = \{a, b, c, d, e\}$ and $Y = \{@, \#, \$, \&\}$, then

$$X \cup Y = \{a, b, c, d, e, @, \#, \$, \&\}$$ ■

The union of an infinite sequence of sets is defined in the same way.

**Definition 1.12′**

$$\cup A = \bigcup_{n=0}^{\infty} A_n = A_0 \cup A_1 \cup A_2 \ \ldots \ = \ \{x | x \in \ A_n, n \in \mathbf{N}\}$$

In general, considering the abstract nature of a set, the existence of the union as a set is postulated by

**Axiom 8 (Union axiom)** For any set $X$, there is a set that is the union of all the elements of $X$.

As much as the concept of the union of two sets is easy to understand, Axiom 8 might take some time to absorb, so you can skip it until you have studied Chapter 2. For now let's just say that one can think of the expression in Definition 1.12′ as $\cup\{A_n | n \in \mathbf{N}\}$.

**Example 1.24** Let's take just two sets, $A_1$ and $A_2$, and consider $\{A_1, A_2\}$. Suppose $x \in \cup\{A_1, A_2\}$. That is true iff $x \in X$ for some $X \in \{A_1, A_2\}$. But the only $X'$s in $\{A_1, A_2\}$ are $A_1$ and $A_2$. Thus $x \in \cup\{A_1, A_2\}$ iff $x \in A_1$ or $x \in A_2$. But that's exactly what we are saying with $x \in A_1 \cup A_2$. ■

**Example 1.25** Suppose we have three sets $A$, $B$, $C$. Then, there is a set with these sets as its elements:

$$\{A\} \cup \{B\} \cup \{C\} = \{A, \ B\} \cup \{C\} = \{A, B, C\}$$ ■

**Example 1.26** The next simple fact is that

$$\cup\{X | X \in \{A\}\} = A$$ ■

Following the aforementioned three examples, it should not be difficult to work out:

**Example/Exercise 1.27** Determine whether the following is true:

(i) $\cup\{X\} = X$

(ii) $\cup\varnothing = \cup\{\varnothing\} = \varnothing$
(iii) $\{\varnothing\} \cup \varnothing = \{\varnothing\}$

**Definition 1.13** Let $A$ and $B$ be sets. The **intersection** of $A$ and $B$, denoted $A \cap B$, is the set of all elements $x \in \mathcal{U}$, such that $x$ is an element of $A$ and $x$ is an element of $B$ (Figure 1.8), that is

$$A \cap B = \{x \in \mathcal{U} | x \in A \ \& \ x \in B\}$$

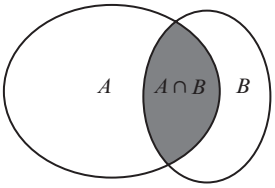



**Figure 1.8** $A \cap B$ intersection

**Example 1.28** Given two sets $A = \{1, 2, 3, a, b, c\}$ and $B = \{3, b, x, y\}$, then

$$A \cap B = \{3, b\}$$ ■

**Example/Exercise 1.29** Show that for all sets $A$, $B$, and $C$

(i) $A \subseteq A \cup B$ and $B \subseteq A \cup B$
(ii) If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$

The intersection of an infinite sequence of sets is defined analogously

**Definition 1.13′**

$$\cap_{n=0}^{\infty} A_n = A_0 \cap A_1 \cap A_2 \cdots = \{x | (\forall n \in \mathbf{N})x \in A_n\}$$

**Example/Exercise 1.30** Show that

$$A \cap B \subseteq A \quad \text{and} \quad A \cap B \subseteq B$$

**Example/Exercise 1.31** Convince yourself that

(i) $A \subseteq B$ iff $A \cup B = B$
(ii) $A \subseteq B$ iff $A \cap B = A$
(iii) $\{\varnothing\} \cap \varnothing = \varnothing$

**Example/Exercise 1.32** The union of empty sets is clearly an empty set. You may be wondering now: what about $\cap\varnothing$? This is much trickier. Can you see why?

**Definition 1.14** Let $A$ and $B$ be two sets. We say that $A$ and $B$ are disjoint, if $A \cap B = \varnothing$ (Figure 1.9).

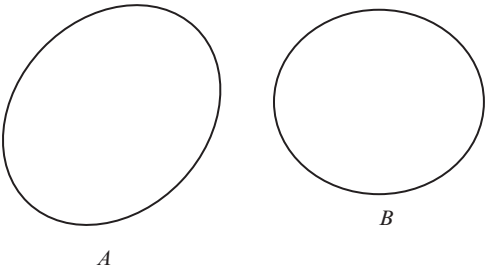



**Figure 1.9** $A \cap B = \varnothing$.

**Example 1.33** Consider the following:

Let $A_1 = \{0\}, A_2 = \{0, 1\}, A_3 = \{0, 1, 2\}, \ldots, A_{i+1} = \{0, 1, 2, \ldots, i\}, \ldots$. So we have an infinite collection of $A's$, such that for every $n \in \mathbf{N}^+$, $n \in A_{n+1}$.[26] Thus, $\mathbf{N}^+ = A_1 \cup A_2 \cup \cdots$ and $A_1 \cap A_2 \cap \cdots = 0$. ■

**Example 1.34** Consider a set $\mathbf{R}$. Let set $A$ be the interval $(-3, 5)$, and set $B$ the interval $(3, 8)$.

Find:

(i) $A \cap B$

(ii) $A \cup B$

**Solution** First, recall the definition of intervals on the set of real numbers $\mathbf{R}$:

An open interval

$$O = (a, b) = \{x | a < x < b\}$$

A closed interval

$$C = [a, b] = \{x | a \leq x \leq b\}$$

Of course, we can have a half-open–half-closed interval, such as

$$O_C = (a, b] = \{x | a < x \leq b\}$$

or

$$C_O = [a, b) = \{x | a \leq x < b\}$$

[26] In order to avoid confusion, when starting with zero in our collection of $A$'s, for the time being, we put $\mathbf{N} \cup \{0\} = \mathbf{N}^+$, which is also designated by $\mathbf{Z}^+$.

Now, observe that set

$$A = (-3, 5) = \{x | -3 < x < 5\}$$

and set

$$B = [3, 8) = \{x | 3 \leq x \leq 8\}$$

Hence,

(i) $A \cap B = [3, 5) = \{x | 3 \leq x < 5\}$
(ii) $A \cup B = (-3, 8] = \{x | -3 < x \leq 8\}$ ■

**Example/Exercise 1.35** Let the universal set be a set of all integers, that is, $\mathcal{U} = \mathbf{Z}$, and let $A = \{x \in \mathbf{Z} | x = 2n, n \in \mathbf{Z}\}$, and $B = \{y \in \mathbf{Z} | 2m + 1, m \in \mathbf{Z}\}$, then

$$A \cap B = \varnothing$$

Convince yourself that this is indeed so.

**Example/Exercise 1.36**[27] Consider the oldest mathematician among chess players and the oldest chess player among mathematicians. Could they be two different persons?

**Definition 1.15** We say that a collection $A_1, A_2, A_3, \ldots, A_n$ is a **partition** $P(A)$ (Figure 1.10) of a set $A$ iff

(i) $A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n = A$ and
(ii) $A_1 \cap A_2 \cap A_3 \cap \cdots A_n = \varnothing$

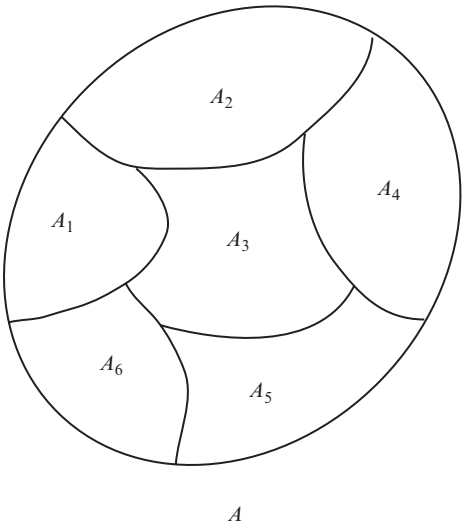



**Figure 1.10** Partition $P(A)$

[27] Shen, S., Vereshchagin, N. K., *Naïve Set Theory*, American Mathematical Society, 2002.

**Definition 1.16** Given two sets $A$ and $B$, we say that the **difference** of $A$ and $B$, denoted $A\backslash B$, and read "$A$ minus $B$," is the set of all elements $x$ from $\mathcal{U}$, such that $x$ is in $A$ and $x$ is not in $B$ (Figure 1.11). We write

$$A \setminus B = \{x \in \mathcal{U} | x \in A \ \& \ x \notin B\}$$

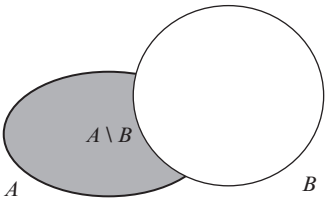



**Figure 1.11**

**Example 1.37** Let $A = \{a, b, c, d, e, f, g\}$ and $B = \{c, e, g, h, i, k\}$, then

$$A \setminus B = \{a, b, d, f\}$$ ■

**Example/Exercise 1.38** Prove the following:

(i) $A\backslash\varnothing = A$
(ii) $A\backslash A = \varnothing$
(iii) $A \cap (B \setminus A) = \varnothing$

**Definition 1.17** Let $A$ and $B$ be sets. The **symmetric difference** of $A$ and $B$, denoted $A\Delta B$ (Figure 1.12), is defined

$$A\Delta B = (A \setminus B) \cup (B \setminus A)$$

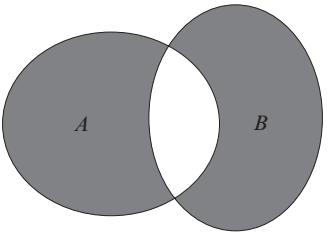



**Figure 1.12** $A \setminus B$

**Example/Exercise 1.39** Convince yourself that

(i) $A\Delta B = 0$ iff $A = B$
(ii) $A\Delta\varnothing = A$

**Example/Exercise 1.40** Show that

$$A \,\Delta\, B = (A \cup B) \setminus (A \cap B)$$

**Definition 1.18** Let $A$ be a subset of the universal set $\mathcal{U}$. We define the **complement** of $A$, denoted $A^c$, as the set of all elements $x$ from $\mathcal{U}$ (Figure 1.13), such that $x$ is not in $A$:

$$A^c = \{x \in \mathcal{U} | x \notin A \}$$

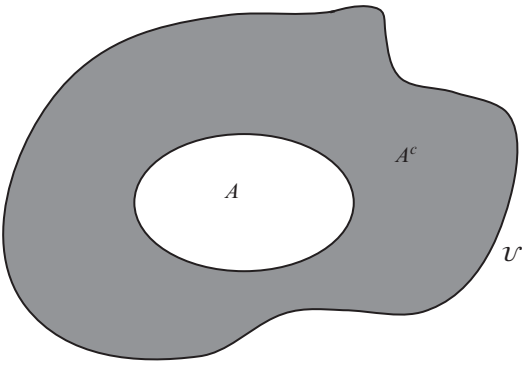



**Figure 1.13** $A^c$

**Example 1.41** Prove that $A \setminus B = A \cap B^c$. ■

***Proof*** The proof is easy. We need to show that $\forall x$ if $x \in A \setminus B$ then $x \in A \cap B^c$, and also that $\forall x$ if $x \in A \cap B^c$ then $x \in A \setminus B$.

So first, suppose we take any $x \in A \setminus B$. That means that $x \in A$ and $x \notin B$, which in turn implies $x \in B^c$. So, $x \in A$ and $x \in B^c$, and therefore $x \in A \cap B^c$.

Conversely, if $x \in A \cap B^c$ then $x \in A$ and $x \in B^c$, that is, $x \in A$ and $x \notin B$ and thus $x \in A \setminus B$. ■

**Example/Exercise 1.42** Let $A, B \subseteq \mathcal{U}$ be any two subsets of the universal set. Show that

$$A \subseteq B \text{ iff } B^c \subseteq A^c$$

**Example 1.43** Let $A = [0, 1)$, $B = (-1, 1)$, and $C = (-2, 1]$.
Find

(i) $A^c \cap B^c \cap C^c$
(ii) $(A \cap B) \cup C \cup B^c$

**Solution**

(i) The complements of $A, B,$ and $C$ are as follows:

$$A^c = ([0, 10))^c = (-\infty, 0) \cup [1, \infty)$$
$$B^c = ((-1, 1))^c = (-\infty, -1] \cup [1, \infty)$$
$$C^c = ((-2, 1])^c = (-\infty, -2] \cup (1, \infty)$$

Then

$$A^c \cap B^c \cap C^c = ((-\infty, 0) \cup [1, \infty)) \cap ((-\infty, -1] \cup [1, \infty)) \cap ((-\infty, -2] \cup (1, \infty))$$
$$= (-\infty, -2] \cup (1, \infty)$$

(ii)

$$(A \cap B) \cup C \cup B^c = ([0, 1) \cap (-1, 1)) \cup (-2, 1] \cup (-\infty, -1] \cup [1, \infty)$$
$$= [0, 1) \cup (-2, 1] \cup (-\infty, -1] \cup [1, \infty)$$
$$= (-\infty, -1] \cup [0, \infty)$$ ■

**Theorem 1.7**

(i) $A \cap \varnothing = \varnothing$
(ii) $A \cup \varnothing = A$
(iii) $A \cap A^c = \varnothing$
(iv) $A \cup A^c = \mathcal{U}$
(v) $\mathcal{U}^c = \varnothing$
(vi) $\varnothing^c = \mathcal{U}$

***Proof*** (i): Let $A$ be any set. Suppose $\cap \varnothing \neq \varnothing$, that is, suppose there exists an $x \in A \cap \varnothing$. By the definition of intersection, $x \in A$, and $x \in \varnothing$. But this is impossible since $\varnothing$ has no elements by definition. Thus,

$$A \cap \varnothing = \varnothing$$

Now you should try to prove parts (ii)–(vi) of the theorem. ■

**Example/Exercise 1.44** Consider three sets $A$, $B$, and $C$. Is it possible that

$$A \cap B \neq \varnothing, \quad A \cap C = \varnothing \quad \text{and} \quad (A \cap B) \setminus C = \varnothing?$$

**Theorem 1.8 (Set identities)** For all sets $A$, $B$ and $C$.

**1.8.1**

(i) $A \cap B = B \cap A$

(ii) $A \cup B = B \cup A$ (Commutative Laws for intersection and union)

**1.8.2**

(i) $A \cap A = A$

(ii) $A \cup A = A$ (Idempotent Laws)

**1.8.3**

(i) $A \cap (B \cap C) = (A \cap B) \cap C$

(ii) $A \cup (B \cup C) = (A \cup B) \cup C$ (Associative Laws for intersection and union)

**1.8.4**

(i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (Distributive Laws)

**1.8.5**

$A \cap \mathcal{U} = A$

**1.8.6**

$A \cup \mathcal{U} = \mathcal{U}$

**1.8.7**

(i) $A \cup (A \cap B) = A$

(ii) $A \cap (A \cup B) = A$ (Absorption Laws)

**1.8.8**

(i) $(A \cap B)^c = A^c \cup B^c$

(ii) $(A \cup B)^c = A^c \cap B^c$ (DeMorgan's Laws)

**Example/Exercise 1.45** Prove 1.8.1–1.8.8 of Theorem 1.8.

***Proof*** Remember, two sets $A$ and $B$ are equal iff $A \subseteq B$ and $B \subseteq A$. Thus, in each case, we need to show that any $x$, being an element of the set on the left-hand side (LHS) of our equation is also an element of the set on the right-hand side (RHS) of our equation, and vice versa. So,

**1.8.4 (ii):**

Suppose $x \in A \cap (B \cup C)$. By the definition of intersection that means that $x \in A$ and $x \in (B \cup C)$. That gives us two possible cases.

Case 1: $x \in A$ and $x \in B$, by the definition of union. Hence, $x \in A$ and $x \in B$ implies that $x \in A \cap B$, therefore,

$$x \in (A \cap B) \cup (A \cap C)$$

Case 2: $x \in A$ and $x \in C$, again by the definition of union. Hence, $x \in A$ and $x \in C$ implies that $x \in A \cap B$, therefore, $x \in (A \cap C) \cup (A \cap B)$. From Theorem 1.8.1 (ii), it follows that

$$x \in (A \cap B) \cup (A \cap C)$$

In both cases, $x \in (A \cap B) \cup (A \cap C)$.
Hence, we have proved that

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \qquad (*)$$

Suppose now that $x \in (A \cap B) \cup (A \cap C)$. By the definition of union that means that either

$$x \in (A \cap B) \quad \text{or} \quad x \in (A \cap C)$$

So, again, we have two possibilities.

Case 1: $x \in (A \cap B)$. By the definition of intersection, this implies that

$$x \in A \quad \text{and} \quad x \in B$$

Well, $x$ being an element of $B$, means that $x$ is also an element of $(B \cup C)$. We have that $x \in A$, and

$$x \in A \quad \text{and} \quad x \in (B \cup C)$$

Therefore, by the definition of intersection,

$$x \in A \cap (B \cup C)$$

Now consider
Case 2: $x \in (A \cap C)$. By the definition of intersection, this implies that

$$x \in A \quad \text{and} \quad x \in C$$

Since $x$ is an element of $C$, it also has to be an element of $(B \cup C)$. So, again, we have that

$$x \in A \text{ and } x \in (B \cup C)$$

Therefore, by the definition of intersection,

$$x \in A \cap (B \cup C)$$

In both cases, $x \in A \cap (B \cup C)$. Hence, we proved that

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C) \qquad (**)$$

Since both subset relations (*) and (**) have been proved, it follows by definition of set equality that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

as stated in Theorem 1.8.3 (ii).

Now you can prove Theorem 1.8.3 (i).

**Proof 1.8.8 (i)**

We need to prove that for every $x$

$$\text{if } x \in (A \cap B)^c \text{ then } x \in A^c \cup B^c$$

Suppose $x \in (A \cap B)^c$. By the definition of complement, $x \notin A \cap B$. But this implies that $x \notin A$ or $x \notin B$. Saying that $x \notin A$ means that $x \in A^c$. Similarly, if $x \notin B$, then $x \in B^c$. Hence, $x \in A^c$ or $x \in B^c$ and by the definition of union this implies that

$$x \in A^c \cup B^c$$

So, we have proved that

$$(A \cap B)^c \subseteq A^c \cup B^c \qquad (*)$$

Let's now consider the converse, that is, let's show that for every $x$

$$\text{if } x \in A^c \cup B^c \text{ then } x \in (A \cap B)^c$$

Suppose that $\in A^c \cup B^c$. By definition of union, it follows that $x \in A^c$ or $x \in B^c$. So we have to consider two cases.

Case 1: $x \in A^c$. Being an element of $A^c$ means that $x \notin A$, and therefore $x$ cannot be in $A \cap B$ either, that is

$$x \notin A \cap B$$

Well, since $x \notin A \cap B$, it is definitely true that

$$x \in (A \cap B)^c \qquad (**)$$

Case 2: $x \in B^c$ would lead us, by the similar arguments, to the same conclusion (**):

$$x \in (A \cap B)^c$$

Thus, we have also proved that

$$A^c \cup B^c \subseteq (A \cap B)^c$$

By the definition of equality of sets, (*) and (**) imply that $(A \cap B)^c = A^c \cup B^c$, as was to be shown. ■

Now you can prove Theorem 1.8.8(ii).

**Example 1.46 (Generalized distributive property)** Let $A_i \in \mathcal{U}$, $i \in \mathbf{N}$, and let $B \in \mathcal{U}$.[28] Show that

$$B \cup (\cap_{i=1}^{n} A_i) = \cap_{i=1}^{n} (B \cup A_i), \quad \forall n \in \mathbf{N}$$

**Solution** We will do the proof by the *Method of Mathematical Induction*:

First, we note that the statement is trivially true when $n = 1$. Theorem 1.8.4(b) assures us that the claim is true for $n = 2$. We will assume that it is also true for $n = k$. If we could prove that it is also true for $n = k + 1$, then the claim is true for any $n \in \mathbf{N}$. Consider

$$\begin{aligned} B \cup (\bigcap_{i=1}^{k+1} A_i) &= B \cup (\bigcap_{i=1}^{k} A_i \cap A_{k+1}) \\ &= (B \cup (\bigcap_{i=1}^{k} A_i) \cap A_{k+1}) \end{aligned}$$

(Since we assumed that the claim is valid for $n = k$)

$$\begin{aligned} &= \bigcap_{i=1}^{k} (B \cup A_i) \cap (B \cap A_{k+1}) \\ &= \bigcap_{i=1}^{k+1} (B \cup A_i) \end{aligned}$$

So, our proposition is true for $n = k + 1$ and thus,

$$B \cup (\bigcap_{i=1}^{n} A_i) = \bigcap_{i=1}^{n} (B \cup A_i) \quad \forall n \in \mathbf{N}$$ ■

[28] If you are unfamiliar with the "Proof by induction" method, you can skip this example until you have studied Chapter 4.

**Example/Exercise 1.47** Let $A_i \in \mathcal{U}$, $i \in \mathbf{N}$, and let $B \in \mathcal{U}$. Show that

$$B \cap (\bigcup_{i=1}^{n} A_i) = \bigcap_{i=1}^{n} (B \cap A_i), \quad \forall n \in \mathbf{N}$$

**Example 1.48** Let $A, B \subseteq \mathcal{U}$ be any two sets. Show that

$$(A \cap B) \cup (A \cap B^c) = A$$

**Solution**

$$\begin{aligned}(A \cap B) \cup (A \cap B^c) &= A \cap (B \cup B^c) \\ &= A \cap \mathcal{U} \\ &= A\end{aligned}$$

On the other hand,

$$\begin{aligned}A &= A \cap \mathcal{U} \\ &= A \cap (B \cup B^c) \\ &= (A \cap B) \cup (A \cap B^c)\end{aligned}$$

■

**Example/Exercise 1.49** Let $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ be the universal set, and let $A = \{1, 3, 5, 8\}$, $B = \{2, 3, 4, 5\}$, and $C = \{3, 4, 6, 7, 8\}$. Using these sets, convince yourself that Theorems 1.8.4 and 1.8.8 are indeed true.

**Example 1.50** Prove that the following statements are equivalent:

(i) $A \subseteq B$
(ii) $A \cap B = A$
(iii) $A \cup \mathrm{B} = B$

■

***Proof*** To prove that (i) implies (ii), let's assume that $A \subseteq B$. We need to establish that $A \cap B \subseteq A$ and that $A \subseteq A \cap B$. But, since $A \cap B \subseteq A$ for all $A$ and $B$, it is sufficient to prove that $A \subseteq A \cap B$. So, if $x \in A$, it follows from (i) that $x \in B$ and therefore $x \in A \cap B$. Hence, $A \subseteq A \cap B$.

To prove that (ii) implies (iii), let's assume that $A \cap B = A$ holds. Then,

$$\begin{aligned} A \cup B &= (A \cap B) \cup B = (A \cup B) \cap (B \cup B) \\ &= (A \cup B) \cap B = B \end{aligned}$$

Finally, to prove that (iii) implies (i), we assume that $A \cup B = B$ holds. Then, since $A \subseteq A \cup B$ for all $A$ and $B$, it follows that $A \subseteq B$. ■

**Example 1.51** Let $\mathcal{U} = \mathbf{R}$, $A = [0, 1)$, $B = (-1, 1)$ and $C = (-2, 1]$.[29] Determine

$$(A \cap B) \cup (A^c \cap C^c)$$

**Solution**

If $A = [0, 1)$, then $A^c = (-\infty, 0) \cup [1, \infty)$.
If $B = (-1, 1)$, then $B^c = (-\infty, -1] \cup [1, \infty)$.
If $C = (-2, 1]$, then $C^c = (-\infty, -2] \cup (1, \infty)$.
So, we have

$$\begin{aligned} (A \cap B) \cup (A^c \cap C^c) &= ([0, 1) \cap (-1, 1)) \cup (((-\infty, 0) \\ &\quad \cup [1, \infty)) \cap ((-\infty, -2] \cup (1, \infty))) \\ &= ([0, 1) \cap (-1, 1)) \cup ((-\infty, -2) \cup (1, \infty)) \\ &= [0, 1) \cup (-\infty, -2] \cup (1, \infty) \\ &= (-\infty, -2] \cup [0, 1) \cup (1, \infty) \end{aligned}$$

■

**Example 1.52 (Generalized DeMorgan's Law)** Prove that for all $n \in \mathbf{N}$, if $A_1, A_2, A_3, \ldots, A_n$ are sets, then

$$(\bigcup_{i=1}^{n} A_i)^c = \bigcap_{i=1}^{n} (A_i)^c$$

■

***Proof*[30]** The formula is obviously true for $n = 1$. (Why?) Suppose it is also true for $n = k$, that is, suppose

$$(\bigcup_{i=1}^{k} A_i)^c = \bigcap_{i}^{k+1} (A_i)^c$$

[29] We assume here that the reader is at least vaguely familiar with the properties of real numbers and she/he won't mind that we have not yet precisely defined the set **R.**

[30] Here, again, if you are not familiar with mathematical induction, you may skip this proof until you have learned it in later chapters.

We have to prove that it is also valid for $k+1$, that is

$$(\bigcup_{i=1}^{k+1} A_i)^c = \bigcap_{i}^{k+1} (A_i)^c$$

which would imply that our formula is valid for all $n$.

Recalling the properties of union and DeMorgan's law for two sets, we get

$$\begin{aligned}(\bigcup_{i=1}^{k+1} A_i)^c &= (\bigcup_{i=1}^{k} A_i \cup A_n)^c \\ &= (\bigcup_{i=1}^{k} A_i)^c \cap (A_n)^c \\ &= (\bigcup_{i=1}^{k} (A_i)^c) \cap (A_n) \\ &= \bigcup_{i=1}^{k+1} (A_i)^c\end{aligned}$$

Since the formula holds for $k+1$, it holds for every $n \in \mathbf{N}$. ■

In a similar way, you can work out

**Example/Exercise 1.53** Prove that for all $n \in \mathbf{N}$, if $A_1, A_2, A_3, \ldots, A_n$ are sets, then

$$(\bigcap_{i=1}^{n} A_i)^c = \bigcup_{i=1}^{n} (A_i)^c$$

**Example 1.54** Let $A, B, C \in \mathcal{U}$ be any three sets. Prove that

$$(A \cup B) \backslash C = (A \backslash C) \cup (B \backslash C)$$

**Solution**

$$\begin{aligned}(A \cup B) \setminus C &= (A \cup B) \cap C^c \\ &= C^c \cap (A \cup B) \\ &= (C^c \cap A) \cup (C^c \cap B) \\ &= (A \cap C^c) \cup (B \cap C^c) \\ &= (A \setminus C) \cup (B \setminus C)\end{aligned}$$

On the other hand, we could have said:

$$\begin{aligned}(A \setminus C) \cup (B \setminus C) &= (A \cap C^c) \cup (B \cap C^c) \\ &= (A \cup B) \cap C^c \\ &= (A \cup B) \setminus C\end{aligned}$$

Thus, we have our proof. ■

**Example 1.55** Let $A,\ B,\ C \in \mathcal{U}$ be any three sets. Prove that

$$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$$

**Solution**

$$\begin{aligned}C \setminus (A \cap B) &= C \cap (A \cap B)^c \\ &= C \cap (A^c \cup B^c) \\ &= (C \cap A^c) \cup (C \cap B^c) \\ &= (C \setminus A) \cup (C \setminus B)\end{aligned}$$

Similarly,

$$\begin{aligned}(C \setminus A) \cup (C \setminus B) &= (C \cap A^c) \cup (C \cap B^c) \\ &= C \cap (A^c \cup B^c) \\ &= C \cap (A \cap B)^c \\ &= C \setminus (A \cap B)\end{aligned}$$

which completes our proof. ■

**Example 1.56** Show that for any two sets $A$ and $B$

$$A^c \setminus B^c = B \setminus A$$

**Solution**

$$\begin{aligned}A^c \setminus B^c &= A^c \cap (B^c)^c \\ &= B \cap A^c = B \setminus A\end{aligned}$$

■

**Example/Exercise 1.57** Prove that for any sets $A, B, C \in \mathcal{U}$

$$A \setminus B = A \setminus (A \cap B)$$

**Example/Exercise 1.58** Show that for any sets $A_i$ and $C$, the following is true.

(i) $C \setminus (\underset{i=1}{\overset{n}{\cup}} A_i) = \underset{i=1}{\overset{n}{\cap}} (C \setminus A_i)$

(ii) $C \setminus (\underset{i=1}{\overset{n}{\cap}} A_i) = \underset{i=1}{\overset{n}{\cup}} (C \setminus A_i)$

**Theorem 1.9** Let $A, B \subseteq \mathcal{U}$ be any two sets. Then,

(i) $A \subseteq B$ iff $\mathcal{U} \setminus B \subseteq \mathcal{U} \setminus A$

(ii) $A \subseteq B$ iff $A \cap (\mathcal{U} \setminus B) = \varnothing$

***Proof***

(i) First, we prove that $A \subseteq B$ implies that $\forall x \in \mathcal{U} \setminus B$, $x \in \mathcal{U} \setminus A$. Let's see:
Suppose $x \in \mathcal{U} \setminus B$ then $x \notin B$. On the other hand, since $A \subseteq B$ if $y \in A$, then $y \in B$ too, which implies that for any $y \notin B$, $y \notin A$. Thus, $x \notin B$ implies that $x \notin A$ and therefore $x \in U \setminus A$. Hence, $\mathcal{U} \setminus B \subseteq \mathcal{U} \setminus A$.
Suppose $\mathcal{U} \setminus B \subseteq \mathcal{U} \setminus A$. We need to prove that it implies $A \subseteq B$. Well, if $x \in \mathcal{U} \setminus B$ then $x \in \mathcal{U} \setminus A$, which furthermore implies that *if* $x \notin B$ then $x \notin A$, and since $\mathcal{U} \setminus B \subseteq \mathcal{U} \setminus A$, it follows that $A \subseteq B$ as claimed.

(ii) First, we prove that $A \subseteq B$ implies $A \cap (\mathcal{U} \setminus B) = \varnothing$:
Suppose $A \subseteq B$, then for any $x \in A$ is true that $x \in B$. Therefore, $x \notin \mathcal{U} \setminus B$, and thus
$A \cap (\mathcal{U} \setminus B) = \varnothing$.
Next, let $A \cap (\mathcal{U} \setminus B) = \varnothing$. We need to prove that it implies that $A \subseteq B$. Consider

$$\begin{aligned} A \cap (\mathcal{U} \setminus B) &= A \cap (\mathcal{U} \cap B^c) \\ &= (A \cap \mathcal{U}) \cap B^c \\ &= (A \cap B^c) \\ &= A \setminus B \\ &= \varnothing \end{aligned}$$

Thus, $A \subseteq B$, as claimed. ■

## 1.5 THE POWER SET

**Definition 1.19 (Power set)** Given a set $X$, the set of all subsets of the set $X$, is called the **power set of** $X$, that is

$$\mathcal{P}(X) = \{A | A \subseteq X\}$$

The existence of a power set is postulated by

**Axiom 9** For any set $X$, there is a set consisting of all the subsets of $X$.

It is easy to convince yourself that the following theorem is true.

**Theorem 1.10** For any set $X$, $\varnothing,\ X \in \mathcal{P}(X)$.

**Example 1.59** Let $X = \{a, b, c\}$, then $\mathcal{P}(X) = \{\ \varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Note that the empty set and the set itself are considered members of this set of sets. ■

**Example 1.60**

(i) What is the power set of the empty set?

(ii) What is the power set of $\{\varnothing\}$?

**Solution**

(i) Since $\varnothing$ is a subset of any set, set $\varnothing$ has only one subset, namely itself. Therefore,

$$\mathcal{P}(\varnothing) = \{\varnothing\}$$

(ii) By the definition of the power set, the set $\{\varnothing\}$ has exactly two subsets: $\varnothing$, and the set $\{\varnothing\}$ itself, that is

$$\mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$$

■

**Example 1.61** Let $S_{n+1} = S_n \cup \mathcal{P}(S_n)$, with $S_0 = \varnothing$. Then, we can recursively construct the sequence of sets as follows:

$$\begin{aligned}
S_0 &= \varnothing \\
S_1 &= S_0 \cup \mathcal{P}(S_0) = \varnothing \cup \mathcal{P}(\varnothing) = \varnothing \cup \{\varnothing\} = \{\varnothing\} \\
S_2 &= S_1 \cup \mathcal{P}(S_1) = \{\varnothing\} \cup \mathcal{P}(\{\varnothing\}) \\
&= \{\varnothing\} \cup \{\varnothing, \{\varnothing\}\} = \{\varnothing, \{\varnothing\}\} \\
S_3 &= S_2 \cup \mathcal{P}(S_2) = \{\varnothing, \{\varnothing\}\} \cup \mathcal{P}(\{\varnothing, \{\varnothing\}\}) \\
&= \{\varnothing, \{\varnothing\}\} \cup \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\} \\
&= \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}
\end{aligned}$$

and so on. ■

**Theorem 1.11** Let $A$ and $B$ be any two sets. If $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

***Proof*** We have to show that $\forall X \in \mathcal{P}(A), X \in \mathcal{P}(B)$.

First note that if $A \subseteq B$, then every subset of $A$ is also a subset of $B$. Suppose that $X \in \mathcal{P}(A)$. Now recall that, by the definition of power set, $X$ being an element of $\mathcal{P}(A)$, has to be a subset of $A$. But $A \subseteq B$, so $X \subseteq B$ too. It follows immediately that $X \in \mathcal{P}(B)$, which was to be shown. Thus,

$$\mathcal{P}(A) \subseteq \mathcal{P}(B)$$ ■

The next question we may ask is: Given a set $X$ with $n$ elements, how do we find the number of subsets of $X$? The following theorem answers this question.

**Theorem 1.12** Let $X$ be any set such that $|X| = n$, $n \in \mathbf{N}$. Then, $|\mathcal{P}(X)| = 2^{|X|} = 2^n$.

For the proof, we need the following lemma.

**Lemma 1.1** Let $X$ be any set, and let $x_0 \in X$ be *any* element of $X$, then there are as many subsets of $X$ that contain $x_0$ as there are subsets of $X$ that do not contain $x_0$.

We reason as follows: suppose we take a set $X_n = \{x_1, x_2, x_3, \ldots, x_n\}$ and $X_{n-1} = \{x_1, x_2, x_3, \ldots, x_{n-1}\}$, that is, a set with one, say $x_0$, fewer elements than $X_n$. Evidently, $X_{n-1} \subseteq X_n$. Then, we argue, if we collect all the subsets of $X_{n-1}$ together with those same subsets, where each one of them is adjoined with $x_0 \in X_n$, we will get twice as many subsets of $X_n$ than of $X_{n-1}$. Formally, and more precisely, the proof of the lemma goes as follows:

***Proof of Lemma*** Let's express the set $X$ as a union of two subsets $A = \cup_i A_i$ and $B = \cup_j B_j$, that is, the union of collections of subsets $A_i$ and $B_j$.

$$\begin{aligned} X &= A \cup B \\ &= (\cup_i A_i) \cup (\cup_j B_j) \end{aligned}$$

such that $x_0 \in A_i$, $\forall\, i$, and $x_0 \notin B_j$, $\forall j$. In other words, every $A_i$ is a subset of $X$, and every $B_j$ is a subset of $X \setminus \{x_0\}$.

Observe that the number of subsets in collection $A$ is the same as the number of subsets in collection $B$. Indeed, every $B_j$ subsets of $X$ that do not contain $x_0$ can be matched up with $B_j \cup \{x_0\} = A_j$. Thus, there are as many subsets of $X$ that contain $x_0$ as there are those that do not. ■

Now, we proceed with the proof of Theorem 1.12.

***Proof*** [31] First note that Examples 1.59 and 1.60 in particular are in accord with the theorem. We need to prove that the theorem holds for any set $X$.

Consider the statement of the theorem when $n = 0$. We ask if a set with zero elements, that is, the empty set, has $2^0 = 1$ subset? The answer is yes, as we have shown in Example 1.60. So our theorem is true in the case $n = 0$. Let's assume that it is also true for $n = k$, that is, we assume that any set with $k$ elements has $2^k$ subsets. If we could show that the theorem is also true for $n = k + 1$, then it is true for any $n$.

Let $X$ be a set with $k + 1$ elements, and let $x_0 \in X$. From the previous lemma, we have learned that there is an equal number of subsets of $X$ that contain $x_0$, and those that do not. What does that mean? Well – and this is the crux of the matter – that tells us there are twice as many subsets of $X$ as there are subsets of $X \setminus \{x_0\}$. But $|X \setminus \{x_0\}| = k$, that is, $X \setminus \{x_0\}$ has $k$ elements by our assumption, hence the number of subsets of $X \setminus \{x_0\} = 2^k$, that is

$$|\mathcal{P}(X \setminus \{x_0\})| = 2^k$$

as our inductive hypothesis required.

It follows that the number of subsets of $X$ equals twice the number of subsets of $X \setminus \{x_0\}$, that is

$$|\mathcal{P}(X)| = 2 \cdot 2^k = 2^{2k+1}$$

as was to be shown.

In other words, the important conclusion is

$$|\mathcal{P}(X)| = 2^{|X|}$$ ■

At this point, it may be intuitively clear to everyone that the power set of any finite set, regardless of its size, is again a finite set. For infinite sets, of course, power sets are infinite.

## 1.6 THE CARTESIAN PRODUCT

**Definition 1.20** Let $n \in \mathbf{N}$, and let $x_1, x_2, \ldots, x_n$ be a collection of $n$, not necessarily distinct, elements. We say that $(x_1, x_2, \ldots, x_n)$ is an **ordered *n*-tuple** of $n$ elements, in which we distinguish the first, the second, and so on elements.

**Definition 1.21** Two ordered $n$-tuples $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ are said to be **equal** iff

$$x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n$$

[31] If you are not familiar with the technique of mathematical induction, you can skip this proof in the first reading. After mathematical induction is introduced in the following chapters, you can come back to the proof.

**Definition 1.22 (Cartesian product)** Let $A$ and $B$ be two sets. The **Cartesian product** of $A$ and $B$, denoted $A \times B$, is the set

$$A \times B = \{(a, b) |\ a \in A, b \in B\}$$

Given $n$ sets $A_1, A_2, \ldots, A_n$, then the $n$-fold Cartesian product of $A_1, A_2, \ldots, A_n$ is

$$\begin{aligned} A_1 \times A_2 \times \cdots \times A_n &= \prod_i^n A_i \\ &= \{(a_1, a_2, \ldots, a_n) | a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\} \end{aligned}$$

**Example 1.62** Let $A = \{a, b, c\}$ and $B = \{1, 2, 3, \}$ then

$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1), (c, 2), (c, 3)\}$$

■

**Theorem 1.13** Let $A_1, A_2, \ldots, A_n$ be sets, where $n \in \mathbf{N}$, and $n \geq 2$, then the Cartesian product $A_1 \times A_2 \times \cdots \times A_n$ is a set defined recursively by

$$A_1 \times A_2 \times \cdots \times A_n = A_1 \times (A_2 \times A_3 \cdots \times A_n)$$

**Example/Exercise 1.63** Convince yourself that

$$A \times B \neq B \times A$$

**Example/Exercise 1.64** Prove that $A \times \varnothing = \varnothing \times A = \varnothing$.

From the aforementioned discussion, we conclude that if $A$ and $B$ are (finite) sets, and if one of them is empty, then the Cartesian product $A \times B$ is empty. In other words, if neither $A$ nor $B$ is empty, then there is $a \in A$ and $b \in B$ so that $(a, b) \in A \times B$. The rather difficult question is : Can we generalize this to infinite sets, that is, can we say that *the Cartesian product of a nonempty family of nonempty sets is nonempty*?

**Example/Exercise 1.65** Suppose that $A \neq \varnothing$, and that $B \neq \varnothing$. Show that

$$A \times B = B \times A, \quad \text{iff } A = B$$

**Theorem 1.14** If $A, B,$ and $C$ are sets, then

(i) $(A \cup B) \times C = (A \times C) \cup (B \times C)$

(ii) $(A \cap B) \times C = (A \times C) \cap (B \times C)$
(iii) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$

**Definition 1.23** If $A = B$, then we write $A \times A = A^2$.

**Example 1.66** $\mathbf{R} \times \mathbf{R} = \mathbf{R}^2$ is our familiar 2-dimensional Euclidean plane. ■

## 1.7 THE SETS N, Z, AND Q

The sets of numbers **N**, **Z**, and **Q** have been mentioned several times already, but now we want to address some more interesting things about them.

The set of **natural numbers** is a collection

$$\mathbf{N} = \{1, 2, 3, \ldots\}$$

As was mentioned before, one will often find that some authors, especially those working in mathematical logic and computer science, prefer to include "0" (zero) in the set **N**, which is mostly for convenience. Consider this:

Suppose we came up with numerals such as this:

$$\mathit{I}, \mathit{II}, \mathit{III}, \mathit{IIII}, \ldots$$

Such a sequence can be considered a counterpart of natural numbers $1, 2, 3, 4, \ldots$ constructed with only one object "$\mathit{I}$." On the other hand, if we wanted to begin with zero, construction of our sequence would require two objects "**0**" and "$\mathit{I}$" and we would have

$$\mathit{0}, \mathit{0I}, \mathit{0II}, \mathit{0III}, \ldots$$

representing $0, 1, 2, 3, \ldots$. So, it is debatable whether it is advantageous to consider zero as a natural number. I hope the reader won't find this confusing, since it will be evident from the very context of every argument what is meant by the set **N**.

Also, you will often hear that the set **N** is called the set of **counting numbers**, or even the set of **nonnegative integers.** However, **natural numbers** is the name most commonly used, and it is historically the most appropriate one.

More importantly, note that whether you are expressing the set of natural numbers with zero or as $\mathbf{N} = \{1, 2, 3, \ldots\}$, the amount of information contained in this notation is astounding. Namely, just a few elements of this set, that is, "1," "2," "3," with the ellipsis " … " following them, suffice to "completely describe" the whole (infinite) set. In other words, our mind is able to grasp the enormous amount of information contained in **N** by recognizing just a few "examples" and that very significant "dot, dot, dot." We feel that we know exactly what kind of

numbers we are talking about when discussing the set **N**. But – what is a (natural) number? Well, assuming that we know what we mean by the terms "number," "1," and "successor," we can formally define a set of natural numbers by using axioms due to the Italian mathematician Giuseppe Peano.[32]

P1.: 1 is a natural number, that is, $1 \in \mathbf{N}$ (i.e., $\mathbf{N} \neq \emptyset$).[33]

P2.: $\forall\, n \in \mathbf{N},\ \exists\, n' = S(n) \in \mathbf{N}$, called the successor of $n$.

P3.: $n' \neq 1$, that is, there exists no number whose successor is 1.

P4.: If $n' = m'$ then $n = m$, that is, there is no number or there is exactly one number whose successor is the given number.

More generally, we can state Peano's axioms, and this time including "zero," as follows:

Let $X$ be a set such that:

(P1′): There is a special element $0_X \in X$.

(P2′): There is a function $S : X \to X$ such that the following holds: For every $x, y \in X$, if $x' = S(x) = S(y) = y'$then $x = y$.

(P3′): For every $x \in X$, $0_X \neq S(x)$.

(P4′): For every $A \subseteq X$, if $0_X \in A$ and $S(x) \in A$ whenever $x \in A$, then $A = X$.

If we take $X$ to be the set **N** with $0_X = 0$, that is, $X = \mathbf{N} = \{\, 0, 1, 2, 3, \ldots \}$ and defining the function $S$ by $n \mapsto n + 1$, we see that **N** satisfies axioms $P1' - P4'$.

**Theorem 1.15** The set **N** with a special element 0 and the successor function $S$ defined by $n \mapsto n + 1$ satisfies Peano's axioms.

**Definition 1.24 (Russell's hereditary principle)** A property is said to be "hereditary" in the natural number series if, whenever it belongs to a number $n$ it also belongs to $n + 1$. Similarly, a set is said to be "hereditary" if, whenever $n$ is an element of a set, so is $n + 1$.[34]

Speaking of sets in everyday parlance, we usually think of them as a collection of objects, whatever the "objects" are. In mathematics, however, we can equally well speak (and we often do) of "pure sets" – sets whose members are other pure sets, like the empty set itself. Can we use those to construct other familiar sets?

At this point, you may recall Axioms 0–6 and revisit our discussion on pages 19 and 20, and in particular Example 1.13, where we listed a sequence of sets:

[32] Giuseppe Peano (1858–1932).

[33] One can equally well take zero to be the element of **N** and start with it as the first natural number.

[34] Bertrand Russell, *Introduction to Mathematical Philosophy.*

$\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\{\varnothing\}, \{\{\varnothing\}\}\}, \ldots$. One way to construct natural numbers could be as follows:

$$\begin{aligned}
\mathbf{0} &= \varnothing = \{\} \\
\mathbf{1} &= \{0\} = \{\{\}\} \\
\mathbf{2} &= \{0, 1\} = \{0, \{0\}\} = \{\{\}, \{\{\}\}\} \\
\mathbf{3} &= \{0, 1, 2\} = \{0, \{0\}, \{0, \{0\}\}\} = \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\} \\
&\vdots \qquad\qquad\qquad\qquad \vdots \\
\mathbf{n} &= \{0, 1, 2, \ldots, n-2, n-1\} = \{0, 1, 2, \ldots, n-2\} \cup \{n-1\} \\
&= (n-1) \cup \{n-1\}
\end{aligned}$$

On the other hand, with the empty set $\varnothing = \{\ \}$ and a successor function[35] defined by

$$S(x) = \{x\}$$

we can have

$$\begin{aligned}
\mathbf{0} &= \varnothing = \{\} \\
\mathbf{1} &= S(0) = \{\varnothing\} = \{\{\}\} \\
\mathbf{2} &= S(1) = \{1\} = \{\{\{\}\}\} \\
\mathbf{3} &= S(2) = \{2\} = \{\{\{\{\}\}\}\}
\end{aligned}$$

and so on.

We can say that each natural number $n$ is equal to the set of the natural number preceding it, $1, 2, 3, \ldots, n-1$.

Alternatively, defining zero as

$$\mathbf{0} = \{\{\}\}$$

and the successor of $x$ as

$$S(x) = x \cup \{x\}$$

we have

$$\begin{aligned}
S(\varnothing) &= \varnothing \cup \{\varnothing\} \\
S(S(\varnothing)) &= S(\varnothing) \cup \{S(\varnothing)\} \\
&= \varnothing \cup \{\varnothing\} \cup \{\varnothing \cup \{\varnothing\}\}
\end{aligned}$$

[35]Here, for the sake of simplicity, we will designate a generic set by a lowercase $x$.

$$S(S(S(\varnothing)) = S(\varnothing) \cup \{S(\varnothing)\} \cup \{S(\varnothing) \cup \{S(\varnothing)\}\}$$
$$= \varnothing \cup \{\varnothing\} \cup \{\varnothing \cup \{\varnothing\}\} \cup \{\varnothing \cup \{\varnothing\} \cup \{\varnothing \cup \{\varnothing\}\}\}$$

and so on (cf. Example 1.61).

Thus, our newly designed natural numbers look like this:

$$\mathbf{0} = \{\{\}\}$$
$$\mathbf{1} = \{\{\}, \mathbf{0}\} = \{\{\}, \{\{\}\}\}$$
$$\mathbf{2} = \{\{\}, \mathbf{0}, \mathbf{1}\}$$

and so on. (In those examples, I purposely wrote natural numbers bold-faced to emphasize their "set-theoretical nature.")

Now, let me show you two things that can cause you some headache.

First, suppose we ask: Is it true that $S(x)$ has one element more than the set $x$? (One would expect that this is indeed true. After all, that's exactly how we constructed $S(x)$.) Well, let's see. Since $S(x) = x \cup \{x\}$, certainly $x \subseteq S(x)$. Now, $S(x)$ obviously contains $x$, which is also an element of $\{x\}$. But –and now comes the caveat – in order for this element (i.e., $\{x\}$) to be an *extra* element, we need $x \notin x$ (?!). On the other hand, if $x \in x$ then $\{x\}$ is a subset of $x$, and then $x \cup \{x\} = x$.

Second, as you might have anticipated, the three different ways (defined earlier) of identifying natural numbers with pure sets are not the only ones – there are infinitely many. What one would expect though is that they are all equivalent. Well, let's see. Consider only two versions:

(i)

$$\mathbf{0} = \varnothing$$
$$\mathbf{1} = \{\varnothing\}$$
$$\mathbf{2} = \{\{\varnothing\}\}$$
$$\mathbf{3} = \{\{\{\varnothing\}\}\}$$
$$\vdots$$

and

(ii)

$$\mathbf{0} = \varnothing$$
$$\mathbf{1} = \{\varnothing\}$$
$$\mathbf{2} = \{\varnothing, \{\varnothing\}\}$$
$$\mathbf{3} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$$
$$\vdots$$

Obviously, the 3 from (i) and the 3 from (ii) are not the same. From the set-theoretic standpoint $\{\{\{\varnothing\}\}\} \neq \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$. So, the question "What is a number?" is not as trivial as some might have thought.

Let's introduce another concept, which will prove to be very useful later.

**Definition 1.25** We say that a set $I$ is *inductive* if $\varnothing \in I$, and if for all $x \in I$ the successor $S(x) \in I$.

Do inductive sets exist? We will assume that there exists at least one inductive set.

**Theorem 1.16** If two sets $I$ and $J$ are the inductive sets, then $I \cap J$ is also inductive.

***Proof*** Following Definition 1.24, we need to show that

(i) $\varnothing \in I \cap J$, and
(ii) whenever $x \in I \cap J$, then $S(x) \in I \cap J$ too

For (i): Since both $I$ and $J$ are inductive, $\varnothing \in I$ and $\varnothing \in$ J, thus $\varnothing \in I \cap J$.
For (ii): If $x \in I \cap J$, then $x \in I$ and $x \in J$. But since $I$ and $J$ are inductive, $S(x) \in I$ and $S(x) \in J$. Hence, $S(x) \in I \cap J$. ■

As a simple exercise, you can now prove.

**Theorem 1.17** The set **N** is inductive.

In more general terms, we state

**Principle of Induction:**

Let $X$ be some set with $0_X \in X$ such that for all properties $P$, if $0_X$ has property $P$, and the successor function $S(x)$ has the same property $P$ whenever $x \in X$ has it, then every element of $X$ has property $P$.

This becomes "obvious" if we take $X = \mathbf{N}$ and $0_X = 0$. We will have to say more about the principle of induction later but for now let's illustrate it with

**Theorem 1.18** Let $X$ be the set that satisfies Peano's axioms. Then, for every $x \in X$ different from $0_X$ there exists $y \in X$ such that $x = S(y)$.

***Proof*** Let $A = \{x \in X | x = 0_X \text{ or } x = S(y), y \in X\}$.

By definition, $0_X \in A$. On the other hand, if $x$ is an element of $A$ then, again by definition, there has to be a $y \in X$, such that $x = S(y) \in A$ and therefore $S(x) = S(S(y)) \in A$. Thus, $A = X$. In other words, for every $x \neq 0_X$ there exists $y \in X$, such that $x = S(y)$.

We continue by "describing" a set of **integers** as a collection

$$\mathbf{Z} = \{ \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \}$$

where, as in the case of natural numbers, a few elements of the set, together with "$\ldots$," capture much of the relevant information about the set **Z**. (The symbol **Z**, which Cantor used to denote integers, comes from the German word *die Zahl = a number, Zahlen = to number*.)

At this point, we want to list the rules of arithmetic, the "**axioms of the set Z**," which are generally well known but rarely justified in introductory textbooks. Also, these rules, as well as many of the "everybody-knows-it" facts, point to some more advanced algebraic structures that will be studied later.

Consider the set **Z** with two operations defined on it: addition "+," and multiplication "·," so that from now on we will be working with the structure $(\mathbf{Z}; +, \cdot)$. Hence our **rules of arithmetic** are as follows:

1. $a + b \in \mathbf{Z}, \ \forall\, a, b \in \mathbf{Z}$
2. $a \cdot b \in \mathbf{Z}, \ \forall\, a, b \in \mathbf{Z}$
3. $a + (b + c) = (a + b) + c, \ \forall\, a, b, c \in \mathbf{Z}$
4. $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \ \forall\, a, b, c \in \mathbf{Z}$
5. $a + b = b + a, \ \forall\, a, b \in \mathbf{Z}$
6. $a \cdot b = b \cdot a, \ \forall\, a, b \in \mathbf{Z}$
7. $a \cdot (b + c) = a \cdot b + a \cdot c, \ \forall\, a, b, c \in \mathbf{Z}$
8. $\exists\, 0 \in \mathbf{Z}$, s.t. $0 + a = a + 0 = a, \forall\, a \in \mathbf{Z}$
9. $\exists\, 1 \in \mathbf{Z}$, s.t. $1 \cdot a = a \cdot 1 = a, \ \forall\, a \in \mathbf{Z}$
10. $\exists\, (-a) \in \mathbf{Z}$, s.t. $a + (-a) = (-a) + a = 0, \ \forall\, a \in \mathbf{Z}$ ■

**Example 1.67** Prove that (i) the additive and (ii) the multiplicative identities are unique. ■

***Proof*** (i) Suppose there are two additive identity, 0 and $0'$, then according to rule (7)

$$0 + 0' = 0' \quad \text{since 0 is an additive identity. But}$$
$$0 + 0' = 0 \quad \text{since } 0' \text{ is an additive identity too. Therefore}$$
$$0 = 0 + 0' = 0'$$

Now you should be able to prove part (ii). ■

**Example 1.68** Prove that

$$a \cdot 0 = 0, \quad \forall a \in \mathbf{Z}$$ ■

***Proof***

$$a \cdot 0 = a \cdot (b + (-b)) = a \cdot b - a \cdot b = 0$$ ■

**Example/Exercise 1.69** Show that if $a \in \mathbf{Z}$, then

$$(-1)\, a = -a$$

**Example/Exercise 1.70** Show that if $a,\ b \in \mathbf{Z}$, then

(i) $(-a)b = a(-b) = -ab$
(ii) $(-a)(-b) = ab$

**Example/Exercise 1.71** Show that $\forall a, b, c \in \mathbf{Z}$, and $a \neq 0$, if $ab = bc$, then

$$a = c$$

**Example/Exercise 1.72** Show that if $a, b \in \mathbf{Z}$, and $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

Here is another property of the set $\mathbf{Z}$ by the name of the

**Trichotomy Law**

$\forall a, b \in \mathbf{Z}$, only one of the following holds

(i) $a < b$
(ii) $a = b$
(iii) $a > b$

**Example 1.73** Prove that for any $a \in \mathbf{Z}$, $a > 0$ iff $-a < 0$. ■

***Proof*** Suppose $a > 0$, then

$$a\ + (-a) > 0 + (-a) > (-a)$$

which implies

$$0 > (-a)$$ ■

**Example/Exercise 1.74** Prove that for any $a, b \in \mathbf{Z}$, such that $a > 0$ and $b < 0$,

$$a \cdot b < 0$$

**Example 1.75** Prove that for any $a, b \in \mathbf{Z}$, such that $a < 0$ and $b < 0$,

$$a \cdot b > 0$$ ■

***Proof*** Suppose $a < 0$ and $b < 0$, then $-a > 0$ and $-b > 0$. Hence

$$(-a) \cdot (-b) = a \cdot b > 0$$ ■

**Example 1.76** Let $a, b \in \mathbf{Z}$, and $a > 0, b > 0$. Prove that $a < b$ iff $a^2 < b^2$. ■

***Proof*** Suppose $a > 0$ and $b > 0$, and, furthermore, suppose that $a < b$, then, since $a < b$,

$$a^2 < a \cdot b < b^2$$

as was to be shown.

Now suppose that $a^2 < b^2$. Then,

$$a \cdot a < a \cdot b < b \cdot b$$

Therefore, $a < b$, as claimed. ■

**Example/Exercise 1.77** Let $a, b \in \mathbf{Z}$, and let $a < 0$ and $b < 0$. Show that $a < b$ iff $b^2 < a^2$.

**Theorem 1.19** There are no integers between 0 and 1.

***Proof*** Suppose there is a set

$$A = \{a \in \mathbf{Z} | 0 < a < 1\}$$

Suppose, furthermore, that $A \neq \emptyset$. Then there is a least element $a_0 \in A$. Now, $a_0$ being an element of $A$ means that $0 < a_0 < 1$, which implies that $0 < a_0^2 < a_0$. But then it follows that $a_0^2 \in A$, and therefore $a_0$ is not the least element of $A$. Hence $A = \emptyset$, that is, there are no elements between 0 and 1 in **Z**. ■

So far, we haven't discussed the numbers of the form $a/b$, where $a, b \in \mathbf{Z}$ and $b \neq 0$. Those are ostensibly fully "legitimate" numbers and we have to include them in our family of numbers.

In order to describe those numbers, called **rational numbers Q**, we cannot proceed in the same way as before, that is, we cannot give a few examples that would be sufficient to encapsulate all properties of the set **Q**. We need to refer to set theory. So we define the set of all rational numbers **Q** as follows.

**Definition 1.26** We say that the set

$$\mathbf{Q} = \left\{ x \,\middle|\, x = \frac{p}{q}\,,\ \ p, q \in \mathbf{Z},\ \ q \neq 0 \right\}$$

is the set of rational numbers. In other words, we say a number $x$ is rational if and only if $x = p/q$ for some integers $p$ and $q$, with $q \neq 0$. In addition, to make things simpler, occasionally we request that $p$ and $q$ be relatively prime, that is, that there is no number that divides $p$ and $q$ at the same time (except, of course the number 1). By doing this, we are simply collecting all the numbers expressible as a quotient of two integers reduced to simplest form.

Observe that, based on everything we have discussed so far,

$$\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q}$$

which makes the following theorem obvious.

**Theorem 1.20** Every integer is a rational number.

***Proof*** It's easy – you should do it! ■

**Theorem 1.21** The sum of two rational numbers is rational.

***Proof*** Suppose $x, y \in \mathbf{Q}$. Then, by Definition 1.26, we know that $x = a/b$ and $y = c/d$ for some $a, b, c, d \in \mathbf{Z}$, with $b \neq 0, d \neq 0$. Then,

$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}$$

$ad + cb$ is the sum of two integers, therefore an integer, say, $p$, and $bd$ as the product of two integers is also an integer, say, $q$. So we have a quotient of two integers $p/q$, with $q \neq 0$. Hence, $x + y$ is a rational number. ■

**Theorem 1.22** The set $\mathbf{Q}$ is *dense*, that is, between any two rational numbers there is at least another one, that is

$$\forall a, b \in \mathbf{Q}, \quad (a < b), \exists\, c \in \mathbf{Q}, \text{ such that } a < c < b$$

Thus, there are infinitely many.

***Proof*** If $a, b \in \mathbf{Q}$, then $a = m/n$ and $b = p/q$. Consider

$$c = \frac{a + b}{2} = \frac{mq + mp}{2nq}$$

$c$, itself a rational number, is obviously an arithmetic mean of two rational numbers $a$ and $b$, that is

$$a < c < b$$

as was to be shown. ■

I want to show you some less obvious, and rather intriguing, properties of sets **N**, **Z**, and **Q.** First, recall that

(i) Set **N** has a least element but not a greatest.
(ii) Set **Z** has neither a least nor a greatest element.
(iii) Both sets **N** and **Z** are infinite.

Also, $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q}$, and since **N** and **Z** are infinite sets, **Q** has to be infinite too.

But how "big" are the infinities of **N** and **Z** and **Q**? In other words, if $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q}$, how do we compare those "three infinities?" Recall, in Definition 1.8, we said that two sets $A$ and $B$ are equivalent if and only if their cardinal numbers are the same, that is, they have the same number of elements. We need to examine the "number" of elements in infinite sets.

We will follow Cantor and call the cardinal number of **N**, $\aleph_0$ (aleph zero), that is, we say

$$|\mathbf{N}| = \aleph_0$$

Now, what about $|\mathbf{Z}|$ and $|\mathbf{Q}|$, and what about $\aleph_0$ itself? To address those questions, and some others pertaining to set **R**, we need to introduce briefly one of the most important concepts in the whole of mathematics – the concept of a function. We will devote much more time to functions later (see Chapter 4), but for now we will just state two (equivalent) definitions.

**Definition 1.27** Given two sets $X$ and $Y$, we say that a **function $f$ from set $X$ to set $Y$** is a map that assigns to every element of $X$ a unique element of $Y$ (Figure 1.14). We write this as follows:

$$f : X \to Y$$

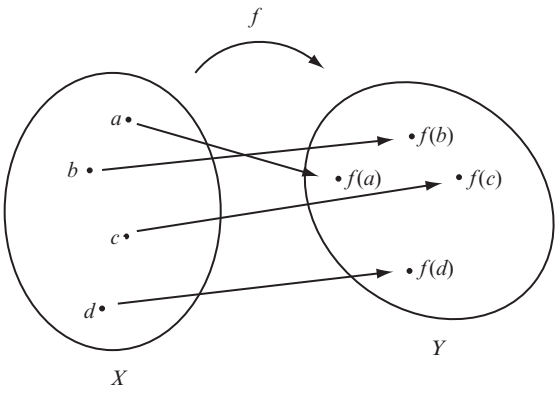



**Figure 1.14** Function $f : X \to Y$.

Set $X$ is called the **domain** of $f$ and $Y$ the **codomain** of $f$.[36]

[36]Some finesses in the definitions of domain, codomain, and range will be addressed in Chapter 4.

Sometimes, it is convenient to simply write

$$X \xrightarrow{f} Y$$

If there is no need to explicitly name the function, we abbreviate the notation by writing

$$x \mapsto f(x)$$

For example, if $x \in \mathbf{R}$, $x \mapsto x^2$ would indicate the function $f : \mathbf{R} \to \mathbf{R}$ that maps every real number to its square (Figure 1.15).

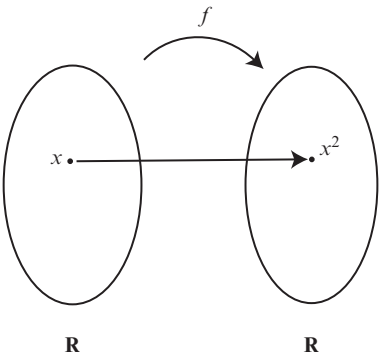



**Figure 1.15** Function $x \mapsto x^2$

**Definition 1.28** A function $f$ from set $X$ into set $Y$, is a set of all ordered pairs $(x, y)$, where for all $x \in X$ there exists a unique $y \in Y$, such that $(x, y) \in f$, that is

$$f = \{(x, y) | x \in X, y \in Y\}$$

$f(x) \in Y$ is said to be an image of $x \in X$. We say that set $X$ is the **domain** of $f$, set $Y$ is the **codomain**, and the set of all images of elements of $X$ is the **range** of $f$.

**Definition 1.29** Given a function $f : X \to Y$, and $A \subseteq X$, we say that the set

$$f[A] = \{f(x) | x \in A\}$$

is the *image* of $A$ under action of $f$.

Consequently, if $B \subseteq Y$ we call

$$f^{-1}[B] = \{x \in X | f(x) \in B\}$$

the *preimage* of $B$ under action of $f$.

**Definition 1.30** Two functions are said to be *equal* if and only if they have the same domain and assign the same value to every member of their common

domain. Symbolically,

$$f = g \leftrightarrow (\forall x \in X, \quad f(x) = g(x))$$

**Definition 1.31** The function $f : X \to Y$ is said to be **one-to-one**, (**1 − 1**, or an **injection**) if and only if

$$\forall x_1, x_2 \in X, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2$$

or equivalently

$$\forall\, x_1,\ x_2 \in X, \text{ if } x_1 \neq x_2 \text{ then } f(x_1) \neq f(x_2)$$

Often injections are designated with the special arrow "$\rightarrowtail$" (Figure 1.16), so for an injection we write

$$f : X \rightarrowtail Y$$

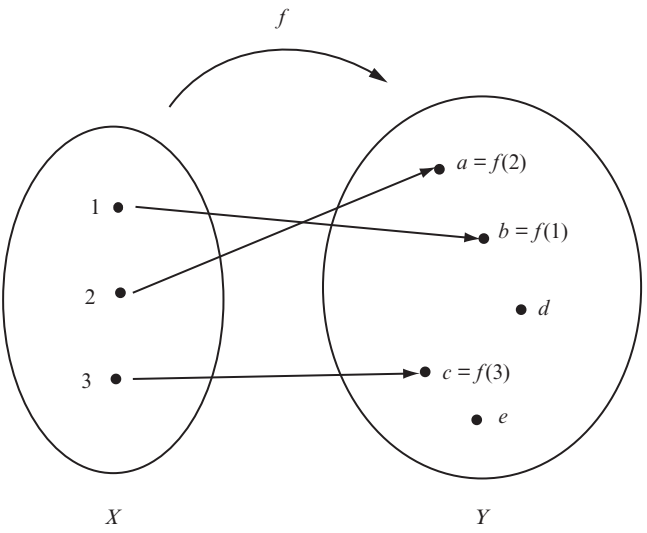



**Figure 1.16** One-to-one function

**Example/Exercise 1.78**[37] Let $f : X \rightarrowtail Y$ be an injection, and let $A, B \subseteq X$. Show that

(i) $f[A \cap B] = f[A] \cap f[B]$
(ii) $f[A \cup B] = f[A] \cup f[B]$

[37] For this example and the others involving functions, you may want to consult Chapter 4.

**Definition 1.32** We say that a function $f : X \to Y$ is **onto** (or a **surjection**, Figure 1.17) iff

$$\forall y \in Y, \exists\, x \in X, \text{ such that } f(x) = y$$

(Sometimes, we use "$\twoheadrightarrow$" to indicate surjection.)

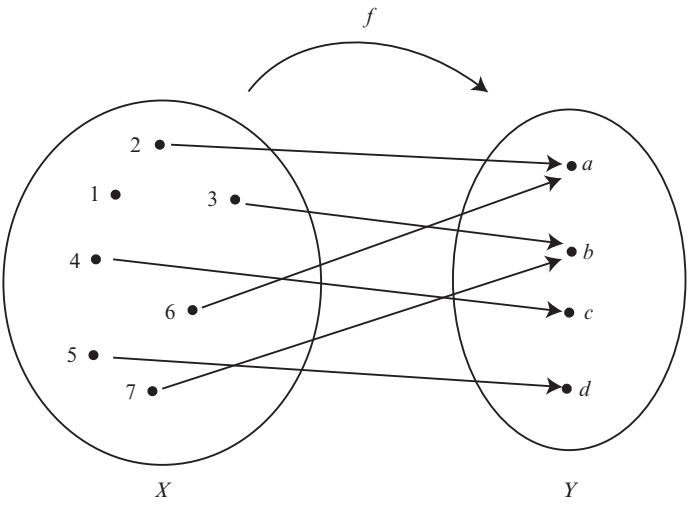



**Figure 1.17** Surjection

**Definition 1.33** A function $f : X \to Y$, that is both *one-to-one and onto*, we call a **bijection** or a **one-to-one correspondence** (Figure 1.18) between sets $X$ and $Y$ (sometimes, we use "$\rightarrowtail$" to indicate bijection).

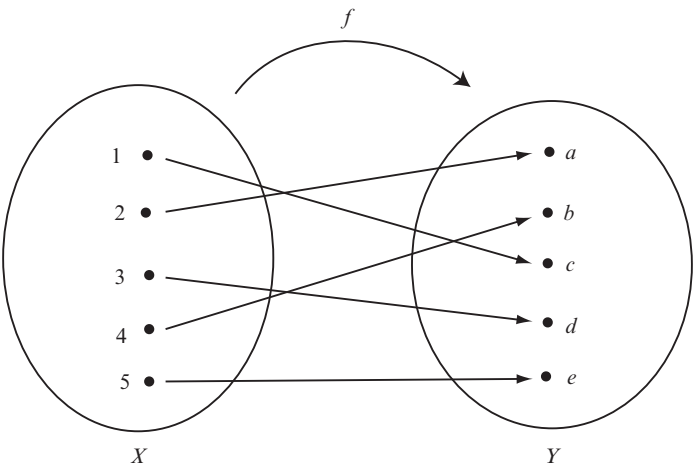



**Figure 1.18** Bijection (one-to-one correspondence)

**Example 1.79** Now we can restate Definition 1.6 and say: The cardinal number of a finite set $A$ is a natural number $n$ if there exists a bijection between $A$ and the set $\{x \in \mathbf{N} \mid 1 \leq x \leq n\}$, that is

$$f : A \rightarrowtail\!\!\!\!\!\rightarrow \{x \in \mathbf{N} \mid 1 \leq x \leq n\}$$ ■

Similarly, the concept of the equivalence of sets can be restated more precisely:

**Definition 1.34** Given two sets $X$ and $Y$, we say that they have the *same cardinality* and we write $|X| = |Y|$, iff there is a one-to-one correspondence between $X$ and $Y$, that is, there exists a function $f : X \to Y$, which is one-to-one and onto. Recall, in Definition 1.10, we call sets with the same cardinality *equivalent* and we write $X \sim Y$.

**Definition 1.35** We say that set $X$ has more elements than set $Y$, if there exists a function $f : X \to Y$ which is onto, but no function $g : X \to Y$ which is one-to-one.

**Theorem 1.23** If $X$ and $Y$ are any two sets, such that there exist one-to-one mappings $X \xrightarrow{f} Y$ and $Y \xrightarrow{g} X$, then $|X| = |Y|$.

**Definition 1.36** Let $f : X \to Y$ be a bijection. We say that

$$f^{-1} : Y \to X$$

is the **inverse function** of $f$, if the following is true:

$$f^{-1}(y) = x \quad \text{iff} \quad f(x) = y$$

**Definition 1.37** We say that $h = g \circ f : X \to Z$ is a **composition** of functions $f$ and $g$, that is

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

if

$$h(x) = g(f(x))$$

**Theorem 1.24** Let $f : X \to Y$ and $g : Y \to Z$ be two bijections. Then, $g \circ f$ is also a bijection.

***Proof*** See Chapter 4. ■

**Definition 1.38**

A set $A$ is said to be **finite** iff there is a bijection from a set $S = \{1, 2, 3, \ldots, n\}$ to $A$ (see Example 1.79).

A set $A$ is said to be infinite if there is no such bijection.

**Example 1.80** Prove that if two **finite** sets $X$ and $Y$ have the same number of elements, that is $|X| = |Y| = n$, then there exists a function $h : X \to Y$, which is one-to-one and onto.

**Solution** According to Definition 1.38, a set $A$ is said to be finite if there exists $n \in \mathbf{N}$, such that, given a set $S = \{1, 2, 3, \ldots, n\}$, there exists some function

$$f : S \to A$$

which is one-to-one and onto. Accordingly, for our sets $X$ and $Y$, there exist functions

$$f : S \to X \text{ and } g : S \to Y$$

both one-to-one and onto. Since $f$ is a bijection, by Definition 1.34, it follows that $f^{-1} : X \to S$ is a bijection too. Hence,

$$g \circ f^{-1} : X \to Y$$

is a bijection too. If we take $h = g \circ f^{-1}$ we have our proof. ■

The proofs of the following two, very important, theorems we leave for Chapter 4.

**Theorem 1.25 (Schröder–Bernstein)** If $A$ and $B$ are any two sets, and if there exist injections $f : A \to B$ and $g : B \to A$, then there exists a bijection between $A$ and $B$, and thus $|A| = |B|$.[38]

**Theorem 1.26** If $A$ and $B$ are any two sets, then exactly one of the following is true:

(i) $|A| = |B|$
(ii) $|A| < |B|$
(iii) $|A| > |B|$

[38] Ernst Schröder (1841–1902), German mathematician. Felix Bernstein (1878–1956), German mathematician.

**Theorem 1.27** Let $A, B$ and $C$ be any three finite sets. Then,

(i) $|A \cup B| = |A| + |B| - |A \cap B|$

(ii) $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

(iii) $|A \times B| = |A| \cdot |B|$

***Proof***

(i) Note that

$$|A \cup B| = |A \setminus B| + |A \cap B| + |B \setminus A| \tag{1.5}$$

On the other hand, observe that

$$|A| = |A \setminus B| + |A \cap B| \tag{1.6}$$

and

$$|B| = |B \setminus A| + |A \cap B| \tag{1.7}$$

Combining (1.5)–(1.7), we get the desired result.

(ii) For this proof, we will use (i) and the following identities:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C) \text{ and } (A \cap B) \cap (B \cap C) = A \cap B \cap C$$

So we have

$$\begin{aligned} |A \cup B \cup C| &= |A \cup B| + |C| - |(A \cap C) \cup (B \cap C)| \\ &= |A| + |B| - |A \cap B| + |C| - |A \cap C| \\ &\quad - |B \cap C| + |A \cap B \cap C| \\ &= |A| + |B| + |C| - |A \cap B| - |A \cap C| + |A \cap B \cap C| \end{aligned}$$

(iii) From the definition of the Cartesian product of two finite sets $A$ and $B$, for any $(a, b) \in A \times B$, there are $|A|$ possibilities for $a$, and $|B|$ possibilities for $b$, and therefore $|A \times B| = |A| \cdot |B|$. ■

**Theorem 1.28** If $A$ is a *finite* set with cardinality $k$, and $x \notin A$, then $|A \cup \{x\}| = k + 1$.

***Proof*** First note, that if $A = \varnothing$ then $|A| = |\varnothing| = 0$, therefore $|A \cup \{x\}| = 1 = 0 + 1$.

If $A \neq \varnothing$ then $A \sim \mathbf{N}_k$, where $\mathbf{N}_k = \{1, 2, \ldots, k\}$. It follows that

$$A \cup \{x\} \sim \mathbf{N}_k \cup \{k+1\} = N_{k+1}. \text{ Thus } |A \cup \{x\}| = k+1$$ ■

Things are quite different for infinite sets, as the following example illustrates.

**Example 1.81** With $\mathbf{N} = \{1, 2, 3, \ldots\}$ show that $|\mathbf{N} \cup \{0\}| = \aleph_0$

**Solution** Consider a function $f : (\mathbf{N} \cup \{0\}) \to \mathbf{N}$ defined by

$$f(x) = x + 1$$

It is easy to see that $f$ is a bijection.

Consequently, $|\mathbf{N} \cup \{0\}| = \aleph_0$. ■

The next theorem is almost trivial now. However, for its proof we need to invoke the technique of mathematical induction (see Chapter 3).[39]

**Theorem 1.29** For every $k \in \mathbf{N}$, every subset $A$ of $\mathbf{N}_k$ is finite.

***Proof*** Let $k \in \mathbf{N}$ be any natural number and let $A \subseteq \mathbf{N}_k$. If $k = 1$ then $A = \varnothing$ or $A = \mathbf{N}_k$ and thus $A$ is finite. Suppose that all the subsets of $\mathbf{N}_k$ are finite for some number $k$. Now, let $A \subseteq \mathbf{N}_{k+1}$, then $A \setminus \{k+1\} \subseteq \mathbf{N}_k$ which, by our induction hypothesis, is finite. Thus, $A$ is finite. Suppose not. Then, we could write

$$A = (A \setminus \{k+1\}) \cup \{k+1\}$$

which is finite by the previous theorem. We conclude that for every $k \in \mathbf{N}$, every subset of $\mathbf{N}_k$ is finite. ■

**Definition 1.39** We say that $A$ is *less than* or *equinumerous* with $B$, if there is a one-to-one function $f : A \to B$, and we write $A \preccurlyeq B$.

**Definition 1.40** A set $A$ is *less than or equal* to $B$ in "size" if it is equinumerous with at least one subset of $B$, that is

$$|A| \leq |B| \leftrightarrow (\exists C)(C \subseteq B \ \& \ |A| = |C|)$$

**Theorem 1.30** For any sets $A$ and $B$ if $A \subseteq B$, then $A \preccurlyeq B$.

[39] You can skip this proof until you have read Section 3.4.

***Proof*** Let $C \subseteq B$ be a set, such that $|A| = |C|$. Then, there has to be a bijection $f : A \to C$, which means that $f$ is an injection from $A$ to $B$. On the other hand, if there exists an injection $f : A \to B$, then the image $f[A]$ is a subset of $B$, that is, $f[A] \subseteq B$. However, $|A| = |f[A]|$, and thus, $A \preccurlyeq B$. ■

Now we return to our sets **N**, **Z**, and **Q**.

**Definition 1.41** A set is called **countably infinite** or **denumerable** (sometimes, just **countable**)[40] iff it has the same cardinality as the set of natural numbers **N**. If that is not the case, we say that a set is **uncountable**.

**Example 1.82** Let $\mathbf{N}_{\text{even}}$ be the set of all even natural numbers

$$\mathbf{N}_{\text{even}} = \{2, 4, 6, 8, \ldots\}$$ ■

Obviously, $\mathbf{N}_{\text{even}} \subseteq \mathbf{N}$, so what is the cardinal number of $\mathbf{N}_{\text{even}}$? In order to make the answer rather obvious let's take $\mathbf{N} = \{1, 2, 3, \ldots\}$ and then establish a one-to-one correspondence between **N** and $\mathbf{N}_{\text{even}}$ in the following way:

$$\begin{aligned} \mathbf{N} &= \{1, 2, 3, 4, \ldots\} \\ &\quad \updownarrow \updownarrow \updownarrow \updownarrow \cdots \\ \mathbf{N}_{\text{even}} &= \{2, 4, 6, 8, \ldots\} \end{aligned}$$

that is, we have obtained the following correspondence: $1 \leftrightarrow 2, 2 \leftrightarrow 4, 3 \leftrightarrow 6, 4 \leftrightarrow 8$, and so on.

In other words, we are considering a function $f : \mathbf{N} \to \mathbf{N}_{\text{even}}$ defined by

$$f(n) = 2n, \quad \forall n \in \mathbf{N}$$

Obviously, the described function is one-to-one and onto, therefore,

$$|\mathbf{N}| = |\mathbf{N}_{\text{even}}|$$

We came to the surprising and unexpected conclusion that, regardless of the fact that $\mathbf{N}_{\text{even}}$ is a proper subset of **N**, indeed just a "half" of **N**, they still have the same cardinality, that is, they are equivalent.

This shocking result, discovered by Cantor, disputed one of Euclid's famous axioms that seemed so "self-evident" for centuries: "*The whole is greater than its part.*" Euclid also stated "[*t*]*hings that coincide with one another are equal to*

[40] Sometimes, it is said that a set is *countable*, if it is either finite or denumerable.

*one another*." Obviously, "things" had to be reconsidered.

Reminding yourself of Definition 1.39, you may now try

**Example/Exercise 1.83** Decide whether the following statements are true:

(i) $2\mathbf{Z} \preccurlyeq \mathbf{Z}$
(ii) $2\mathbf{Z} \sim \mathbf{Z}$

With the concept of equivalence, and Cantor's aforementioned discovery, we are now in a position to define an infinite set yet another way:

**Definition 1.42** A set $X$ is infinite if there exists at least one proper subset of $X$ with the same cardinality as $X$, that is, a set is infinite if it is equivalent to at least one of its proper subsets.

**Example/Exercise 1.84** Convince yourself that a set of all natural numbers and a set of all squares of natural numbers have the same cardinality.

**Theorem 1.31 (Cantor)** Let $X$ be any set. Then, $|X| < |\mathcal{P}(x)|$.

***Proof*** Let $f : X \to \mathcal{P}(X)$ be a function defined by $f(x) = \{x\}$, that is, to every $x \in X$ we associate a singleton $\{x\}$. It is easy to see that $f$ is an injection. Indeed, if $f(x_1) = f(x_2)$ that is, $\{x_1\} = \{x_2\}$, then $x_1 = x_2$. Suppose that there also exists a bijection $g : X \to \mathcal{P}(X)$. Define

$$Y = \{x \in X | x \notin g(x)\}$$

Since $g$ is a bijection, there exists a unique $x \in X$, such that $Y = g(x)$, and we ask: Is $x \in g(x)$ or not? Suppose $x \in g(x)$, then by definition of $Y$, $x \notin Y$; conversely, if $x \notin g(x)$ then $x \in Y$. But that contradicts our request that $Y = g(x)$. Thus the proof. Needless to say, the similarity with Russell's paradox is evident. You may want to compare this theorem with Theorem 1.12. ■

**Corollary** Set $\mathcal{P}(\mathbf{N})$ is uncountable.

**Example/Exercise 1.85** Convince yourself that

(i) $\aleph_0 + \aleph_0 = \aleph_0$
(ii) $2\aleph_0 = \aleph_0$

**Example 1.86** Show that **Z** is countable.

**Solution** As the definition of countability requires, we need to find a function $f : \mathbf{N} \to \mathbf{Z}$ that is one-to-one and onto. Let's rearrange the elements of the set **Z** this way:

$$\mathbf{Z} = \{0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots\}$$

The pattern is self-evident, and we are sure that all integers have been "collected." Now, as before, we establish a correspondence

$$\begin{array}{rccccccccc} \mathbf{N} = \{1, & 2, & 3, & 4, & 5, & 6, & 7, & \ldots\} \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots \\ \mathbf{Z} = \{0, & 1, -1, & 2, & -2, & 3, & -3, & & \ldots\} \end{array}$$

It is clear from the aforementioned scheme that no integer has been missed or counted twice in the process of matching it with a corresponding natural number. The "function" defined by the aforementioned pattern is obviously the function $f : \mathbf{N} \to \mathbf{Z}$ given by

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is an even natural number} \\ -\frac{n-1}{2} & \text{if } n \text{ is an odd natural number} \end{cases}$$

The function is one-to-one and onto, telling us that $|\mathbf{Z}| = |\mathbf{N}| = \aleph_0$. ■

**Example/Exercise 1.87** Find another rearrangement of the elements of **Z** and **N** to establish a bijection between these two sets and prove that $|\mathbf{Z}| = \aleph_0$

**Example/Exercise 1.88** Try to find another explicit formula for the function $f : \mathbf{N} \to \mathbf{Z}$ that would produce the result obtained in the previous example.

For the next exercise, we will need the following:

**Theorem 1.32** Given three sets $A, B$, and $C$, such that $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$.

***Proof*** Suppose that there exist two bijections

$$f : A \to B \quad \text{and} \quad g : B \to C$$

telling us that $|A| = |B|$ and $|B| = |C|$. Consider the composition of $f$ and $g$

$$g \circ f : A \to C$$

By Theorem 1.24, $g \circ f$ is a bijection too, thus $|A| = |C|$. ■

**Exercise 1.89** Suppose that $A \sim B$ and $C \sim D$. Show that $(A \times C) \sim (B \times D)$.

**Solution** Since $A \sim B$ and $C \sim D$, there exist respective bijections $f : A \to B$ and $g : C \to D$. Define the function $h : (A \times C) \to (B \times D)$ by

$$h(a, c) = (f(a), g(c)), \quad a \in A, \quad c \in C$$

As constructed above, $h$ is evidently a bijection, hence $(A \times C) \sim (B \times D)$.

**Example/Exercise 1.90** Show that $|2\mathbf{Z}| = \aleph_0$.

From all that has been said so far, it becomes evident why we define a set as infinite if it could be made equivalent to a proper subset of itself. And vice versa: a set is said to be finite, if it could not be made equivalent to at least one of its subsets.

A natural question one could ask at this point is: What about the cardinality of the set of rational numbers? Recall that $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q}$. It is conceivable, then, that $\mathbf{Q}$ is much "bigger" than $\mathbf{N}$. Also, remember we proved in Theorem 1.22 that the set $\mathbf{Q}$ is dense. We can rephrase this by saying that in the ordering of rational numbers in terms of size, there is no next-larger rational number to any given number. So, it is definitely nontrivial to ask about larger infinities. In other words, all the sets we discussed so far have been countably infinite, that is, all of them have been of the "size" of $\aleph_0$. Now, considering the density of set $\mathbf{Q}$, one could expect the "size" of $\mathbf{Q}$ to be much larger than $\aleph_0$. However, the next theorem points to a different conclusion.

**Theorem 1.33** The set of all positive rational numbers $\mathbf{Q}^+$ is countable.

***Proof*** We would like to construct a "reasonable" function from $\mathbf{N}$ to $\mathbf{Q}^+$, and, hopefully, make it a bijection. Consider the following diagram suggested by Cantor:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **1 / 1** | **1 / 2** | **1 / 3** | **1 / 4** | **1 / 5** | **1 / 6** | **1 / 7** | … |
| **2 / 1** | 2/2 | **2 / 3** | 2/4 | **2 / 5** | 2/6 | 2/7 | … |
| **3 / 1** | **3 / 2** | 3/3 | **3 / 4** | **3 / 5** | 3/6 | **3 / 7** | … |
| **4 / 1** | 4/2 | **4 / 3** | 4/4 | **4 / 5** | 4/6 | **4 / 7** | … |
| . | . | . | . | . | . | . | |
| . | . | . | . | . | . | . | |

If we reduce each fraction to its lowest form and remove any repetition (i.e., we keep only the bold-faced numbers), we indeed obtain the set of all positive

rational numbers $\mathbf{Q}^+$. We can now establish a one-to-one correspondence between the natural numbers and the positive rational numbers in the following way:

$$1 \leftrightarrow 1/1, \quad 2 \leftrightarrow 1/2, \quad 3 \leftrightarrow 2/1, \quad 4 \leftrightarrow 3/1, \quad 5 \leftrightarrow 1/3, \quad 6 \leftrightarrow 1/4,$$
$$7 \leftrightarrow 2/3, \quad 8 \leftrightarrow 3/2, \quad 9 \leftrightarrow 4/1, \quad 10 \leftrightarrow 5/1, \ \ldots$$

Note that all the elements of $\mathbf{Q}^+$ have been "accounted for" exactly once, and each one of them has been matched to one and only one natural number. Such a one-to-one correspondence is indeed well defined, and, consequently, we conclude that $|\mathbf{N}| = |\mathbf{Q}^+|$. ■

Now try to prove

**Theorem 1.34** The set of all rational numbers is countable, that is, $|\mathbf{Q}| = |\mathbf{N}|$.
Hint: Consider the fact that $|\mathbf{Q}^+| = |\mathbf{Q}^-|$, and that for any set $A$, $A \cup A = A$.

More generally, we have

**Theorem 1.35** Any subset of a countable set is countable.

***Proof*** Let $X$ be a set such that $|X| = |\mathbf{N}|$, that is, $X$ is countable. Let $Y \subseteq X$. $Y$ could be finite or infinite. If it is finite, there is nothing to prove – $Y$ is countable by definition. So, let $Y$ be an infinite set. We would like to find a one-to-one correspondence between **N** and $Y$, that is, we are looking for a function $f : N \to Y$, such that $f$ is one-to-one and onto.

Now, considering that $X$ is countable, we can arrange the elements of $X$ as a sequence

$$x_1, x_2, x_3, \ \ldots$$

Since $Y \subseteq X$, this sequence must contain all the elements of $Y$. We search among all the $x_i$'s for the elements of $Y$, and arrange them in the order of occurrence as

$$f(1), f(2), f(3), \ \ldots$$

In other words, $\forall\, x_i \in X$, $\exists\, f(i) \in Y$. Since all the elements $x_1, x_2, x_3, \ \ldots$ are distinct, the function $f$ is one-to-one. Now, since every $f(i)$ is found by sequentially searching through all of $x_1, x_2, x_3, \ \ldots$, and is constructed as an image of a natural number, $f$ is also onto. Therefore, $f$ is a bijection from **N** to $Y$, which proves that $Y$ is countable. ■

**Theorem 1.36** Let $A_0, A_1, A_2, \ \ldots$ be a sequence of countable sets. Then the union

$$A = \bigcup_{i=1}^{\infty} A_i = A_0 \cup A_1 \cup A_2 \cup \cdots$$

is also a countable set.

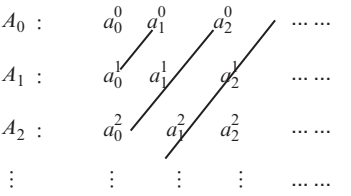
***Proof*** Assuming that every $A_i = \{a_0^i, a_1^i, a_2^i, \ldots, a_n^i, \ldots\} \neq \varnothing$, we can find an onto function

$$\pi^i : \mathbf{N} \to A_i$$

such that for every $i$

$$\pi^i(n) = a_n^i$$

Again, following Cantor, we can construct a table:




Collecting the elements on the diagonals, we obtain the elements of the union fully enumerated:

$$A = \{a_0^0, a_0^1, a_1^0, a_0^2, a_1^1, a_2^0, a_0^2, \ldots\}$$

and the one-to-one correspondence $\pi^i(n)$ between $A$ and $\mathbf{N}$ is evident:

$$\begin{array}{lccccccccc} A = \{ & a_0^0, & a_0^1, & a_1^0, & a_0^2, & a_1^1, & a_2^0, & \ldots \} \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \ldots \\ \mathbf{N} = \{ & 1, & 2, & 3, & 4, & 5, & 6, & \ldots \} \end{array}$$

■

**Corollary** The set of all finite subsets of a countable set is countable.

**Example 1.91** Let $A$ and $B$ be two countable sets. Show that $A \cup B$ is countable.

**Solution** Since $A$ and $B$ are countable, we can express them as

$$A = \{a_1, a_2, a_3, \ldots\} \quad \text{and} \quad B = \{b_1, b_2, b_3, \ldots\}$$

Let's now define a function $f : \mathbf{N} \to A \cup B$ by the following diagram:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & & \\ \downarrow & \downarrow & \downarrow & \downarrow & \ldots & \\ a_1 & b_1 & a_2 & b_2 & & \end{array}$$

Obviously, the function is one-to-one and onto, thus, $A \cup B$ is countable. ■

**Example 1.92** Another way to prove that a set of rational numbers is countable goes as follows: Let

$$A_i = \left\{ q \,\middle|\, q = \frac{z}{i},\ z \in \mathbf{Z},\ i \in \mathbf{N} \right\}$$

Since $A_i$ is obviously countable and $\mathbf{Q} = \cup_i^{\infty} A_i$, by Theorems 1.35 and 1.36, the set **Q** is countable too. ■

As a good exercise, you should now prove Theorems 1.37–1.39.

**Theorem 1.37** If $Y$ is a countable set, and if there exists an injection $f : X \to Y$, then $X$ is also countable.

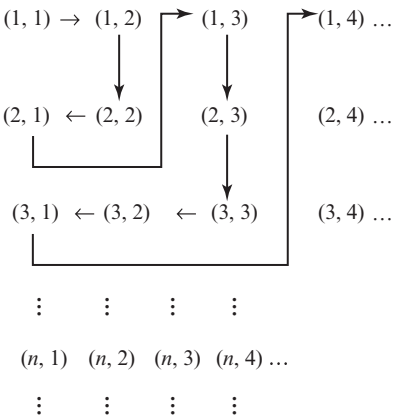
**Theorem 1.38** If $X$ is a countable set, and there exists a surjection $f : X \to Y$, then $Y$ is also countable.

**Theorem 1.39** Every two countably infinite sets are equivalent.

**Theorem 1.40** $\mathbf{N} \times \mathbf{N}$ is countable.

***Proof*** It suffices to show that $|\mathbf{N} \times \mathbf{N}| = |\mathbf{N}|$, that is, to construct a bijection $(\mathbf{N} \times \mathbf{N}) \to \mathbf{N}$.

One way to visualize it would be to count by following the arrows:



The other way to do it would be to arrange $\mathbf{N} \times \mathbf{N}$ as an infinite rectangular array of ordered pairs of natural numbers:

$$\begin{array}{cccccc}
(1,1) & (1,2) & (1,3) & (1,4) & \dots \\
(2,1) & (2,2) & (2,3) & (2,4) & \dots \\
(3,1) & (3,2) & (3,3) & (3,4) & \dots \\
\vdots & \vdots & \vdots & \vdots & \\
(n,1) & (n,2) & (n,3) & (n,4) & \dots \\
\vdots & \vdots & \vdots & \vdots &
\end{array}$$

Thus, we have constructed a countable set of countable sets, that is

$$\begin{array}{l}
A_1 = \{(1,1)\ (1,2)\ (1,3)\ (1,4)\ \dots\} \\
A_2 = \{(2,1)\ (2,2)\ \ (2,3)\ (2,4)\ \dots\} \\
A_3 = \{(3,1)\ (3,2)\ \ (3,3)\ (3,4)\ \dots\} \\
\qquad\qquad \vdots \\
A_n = \{(n,1)\ (n,2)\ \ (n,3)\ (n,4)\ \dots\} \\
\qquad\qquad \vdots
\end{array}$$

This is exactly the structure we have encountered in Theorem 1.36, so we conclude that $\mathbf{N} \times \mathbf{N}$ is a countable set.

Alternatively, we could have said: since $(n, m)$ from our aforementioned list is clearly the $m$th element of $A_n$, why not consider a function

$$f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$$

defined by $f(n, m) = 2^n\ 3^m \cdot f$ is obviously an injection, hence, by Theorem 1.37, we conclude again that $\mathbf{N} \times \mathbf{N}$ is countable. ■

Consequently, the following theorems hold:

**Theorem 1.41** If $A$ and $B$ are countable sets, then $A \times B$ is countable.

**Theorem 1.42** $\mathbf{Q} \times \mathbf{Q}$ is a countable set.

**Theorem 1.43** $\mathbf{N} \times \mathbf{N} \times \mathbf{N}$ is a countable set.

More generally,

**Theorem 1.44** The Cartesian product of a finite number of countable sets is countable.

## 1.8 THE SET R – REAL NUMBERS I

A natural question one may ask at this point is: Does there exist any "larger" set of numbers after the set **Q**? After all, we did say that $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q}$, and we did talk about how "big" and dense the set **Q** is. But again, how big is "big?" If a set is infinite, can one construct a set with greater cardinality? We start this section, predictably, with Cantor's answer:

Now that we have established the fact that, regardless of how "big" **Q** is (and, remember, still equinumerous to **N**), we can always find a bigger one. The inevitable question is whether **Q** is axiomatically rich enough to accommodate everything we want to do mathematically. The answer, of course, is no, it is not. As many a reader may well remember the classic example from high school algebra courses, the solutions of a simple quadratic equation $x^2 = 2, x_{1,2} = \pm\sqrt{2}$ cannot be found in **Q**, that is, $\sqrt{2}$ is not a rational number; it is irrational. So in order to adhere to the spirit of Plato[41] and elude his harsh judgment: *He is unworthy of the name of man who does not know that the diagonal of a square is incommensurable with its sides* – we prove the following, well-known

**Theorem 1.45** $\sqrt{2}$ is not a rational number.

***Proof*** First, recall Definition 1.26, where we defined rational numbers as

$$\mathbf{Q} = \left\{ x \;\middle|\; x = \frac{p}{q}, \quad p, q \in \mathbf{Z}, \quad q \neq 0 \right\}$$

Without loss of generality, let's take $p$ and $q$ to be *relatively prime*.

Suppose that, contrary to the statement of the theorem, $\sqrt{2}$ is a rational number, that is, suppose

$$\sqrt{2} \in \mathbf{Q}$$

Then, there exist $p, q \in \mathbf{Z}$ with $q \neq 0$, such that

$$\sqrt{2} = \frac{p}{q} \tag{1.8}$$

Squaring both sides of (1.8) we get

$$2 = \frac{p^2}{q^2} \tag{1.9}$$

Or, after multiplying both sides by $q^2$

$$2q^2 = p^2 \tag{1.10}$$

[41] Plato (427–347 BC).

Equation (1.10) implies that $p^2$ is an even integer, so $p$ has to be even too! (Why?) Let's express this fact by writing

$$p = 2k, \quad k \in \mathbf{Z} \tag{1.11}$$

Substituting (1.11) into (1.10), we get

$$2q^2 = 4k^2 \tag{1.12}$$

or

$$q^2 = 2k^2 \tag{1.12'}$$

which tells us that $q^2$ is even, and therefore $q$ is even too. As in the case of $p$, we express the fact that $q$ is an even integer by writing it as

$$q = 2l, \quad l \in \mathbf{Z} \tag{1.13}$$

Substituting (1.11) and (1.13) into (1.8) gives

$$\sqrt{2} = \frac{p}{q} = \frac{2k}{2l}$$

which contradicts our assumption that $p$ and $q$ are relatively prime. Hence, our assumption was wrong; therefore, the theorem is true. ■

**Example/Exercise 1.93** Show that $\sqrt{3} \notin \mathbf{Q}$

(Hint: Start, as usual, assuming that

$$\sqrt{3} = \frac{p}{q} \in \mathbf{Q}, \quad q, p \in \mathbf{Z}, \ \ q \neq 0$$

and from $3q^2 = p^2$, consider the cases when $q$ is an even number and when $q$ is an odd number.)

Evidently, in addition to the numbers that we have encountered so far (natural numbers, integers, and rational numbers), there exists another set of numbers called **irrational numbers** $\boldsymbol{I}$, that is, the numbers that cannot be found in any of the previously studied sets **N**, **Z,** and **Q**. The set that contains all of them we call the **set of real numbers R**. We have the following structure:

$$\begin{array}{ccccccc} & & & & \mathbf{I} & & \\ & & & & | & & \\ \mathbf{N} & \subseteq & \mathbf{Z} & \subseteq & \mathbf{Q} & \subseteq & \mathbf{R} \end{array}$$

or

$$\mathbf{Q} \cup \mathbf{I} = \mathbf{R}$$

An astute reader would now expect a formal definition of the set **R**, with all the axioms precisely laid down in order to fully understand all the intricacies of **R**. However, because of the complexities of such a formalism, some additional, more advanced concepts are needed for a full and rigorous definition of the structure. So, we will postpone the full formal definition for later and will now introduce a rather "heuristic" definition and some properties of **R**, which, we hope, will suffice for at least an intuitive appreciation of the richness and importance **R**.

We are about to venture deeper into the land of Cantor, "*a paradise from which no one shall drive us.*"

Without proof, we state

**Theorem 1.46** There is a one-to-one correspondence between the set **R** and the points on the number line.

**Theorem 1.47** The set **R** and the set of points in the open interval $(0, 1)$ are equivalent.

***Proof*** All we need to do is to find an appropriate bijection $f : (0, 1) \to \mathbf{R}$ and we have the proof. Any bijection $(0, 1) \to \mathbf{R}$ that is not defined at 0 and 1 will do. Let's try a function defined by

$$f(x) = \frac{1 - 2x}{x^2 - x} \qquad (*)$$

$f$ is certainly not defined at 0 and 1. Is it a bijection? Let's see. Take $x_1,\ x_2 \in (0,\ 1)$ and suppose that $f(x_1) = f(x_2)$, that is

$$\frac{1 - 2x_1}{x_1^2 - x_1} = \frac{1 - 2x_2}{x_2^2 - x_2}$$

Then,

$$(1 - 2x_1)(x_2^2 - x_2) = (1 - 2x_2)(x_1^2 - x_1)$$

or

$$(x_1 - x_2)(x_1 + x_2 - 2x_1x_2 - 1) = 0$$

If we could prove that $x_1 = x_2$, then our function is one-to-one. $x_1 = x_2$ if

$$x_1 + x_2 - 2x_1x_2 - 1 \neq 0$$

Suppose that is not the case, that is, suppose

$$x_1 + x_2 - 2x_1x_2 - 1 = 0$$

then, with little algebraic reshuffling, we get

$$-x_1 - x_2 + x_1x_2 + 1 = -x_1x_2$$

or

$$(x_1 - 1)(x_2 - 1) = -x_1x_2 \qquad (**)$$

Since $x_1,\ x_2 \in (0,\ 1)$, that is, $0 < x_1 < 1$ and $0 < x_2 < 1$, it would follow that the LHS of (**) implies

$$(x_1 - 1)(x_2 - 1) > 0$$

while the RHS implies

$$-x_1x_2 < 0$$

which, of course, is impossible. We conclude that $x_1 + x_2 - 2x_1x_2 - 1 \neq 0$ indeed. Therefore, $x_1 = x_2$ and our function $f$ is one-to-one. Next, we need to show that $f$ is also onto, that is, that for every $y \in \mathbf{R}$, there exists an $x \in (0,\ 1)$, such that $f(x) = y$. From $(*)$ it follows that one possible $x \in (0,\ 1)$ is

$$x = \frac{y - 2 + \sqrt{y^2 + 4}}{2y}$$

with $y \in \mathbf{R}, y \neq 0$.

Hence,

$$\begin{aligned} f(x) &= \frac{1 - 2x}{x^2 - x} \\ &= \frac{1 - 2\left(\frac{y-2+\sqrt{y^2+4}}{2y}\right)}{\left(\frac{y-2+\sqrt{y^2+4}}{2y}\right)^2 - \left(\frac{y-2+\sqrt{y^2+4}}{2y}\right)} \\ &= \frac{y(8 - 4\sqrt{y^2 + 4})}{8 - 4\sqrt{y^2 + 4}} = y \end{aligned}$$

Hence, our function is one-to-one and onto, that is, $f : (0, 1) \to \mathbf{R}$ is a bijection and therefore $|(0,\ 1)| = |\mathbf{R}|$. ■

**Example 1.94** If you find the aforementioned theorem too technical, or too complicated to be convincing, consider the statement: "There is the same number of points on a line segment 1 cm long as on one that is 1 km long." Here is the "proof":

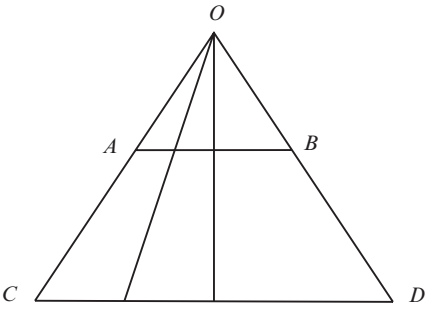



**Figure 1.19**

As you can see, to every point on segment $AB$ there corresponds one and only one point on segment $CD$, regardless of the difference in their lengths. So, a bijection between the points of segment $AB$ and segment $CD$ is evident. ■

If you are at least somewhat familiar with trigonometric functions, the following example is also a good "visual" proof of the equivalence of "short" and "long" segments.

**Example 1.95** The mapping $(\frac{-\pi}{2}, \frac{\pi}{2}) \mapsto \mathbf{R}$ defined by

$$f(x) = \tan x$$

is clearly a bijection (Figure 1.20).

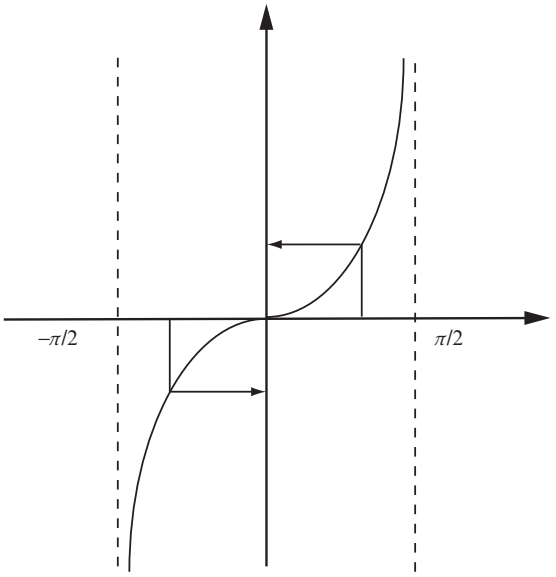



**Figure 1.20**

■

**Example/Exercise 1.96** Prove that $|[0, 1]| = |[0, \ 1)|$.

**Example/Exercise 1.97** Prove that $|(0, 1)| = |(a, \ b)|, \forall \ a, b \in \mathbf{R}$ (see Theorem 1.47).

**Theorem 1.48** The set $\mathbf{R}$ is *dense*, that is, between any two real numbers there is another one; therefore, there are infinitely many. You ought to recall that a similar statement has been made regarding rational numbers (cf. Theorem 1.22). Here, however, we are talking about an even "higher" density. Nevertheless, proof of this theorem should not be difficult for you.

**Theorem 1.49 (Cantor)** The set $\mathbf{R}$ is uncountable.

***Proof*** Consider a set of all real numbers between 0 and 1. Is this set countable or not? Suppose it is countable. In that case, these numbers have a decimal representation and we can list them all as follows:

$$\left.\begin{array}{l} 0.\, a_{11}a_{12}a_{13} \ \ldots \ a_{1n} \ \ldots \\ 0.\, a_{21}a_{22}a_{23} \ \ldots \ a_{2n} \ \ldots \\ 0.\, a_{31}a_{32}a_{33} \ \ldots \ a_{3n} \ \ldots \\ \qquad\vdots \\ 0.\, a_{n1}a_{n2}a_{n3} \ \ldots \ a_{nn} \ \ldots \\ \qquad\vdots \end{array}\right\} \qquad (*)$$

Note that every decimal digit in (*) has two indices; the first one indicating which member of the sequence it belongs to (i.e., which row in the aforementioned sequence), and the second indicating which decimal place the digit is in (e.g., let's say that $0.4758\ldots$ is the number in the third row, then $4 = a_{31}, 7 = a_{32}$, $5 = a_{33}, 8 = a_{34}$, and so on).

With a construction like this, we should be able to associate to every number in (*) one and only one element from $\mathbf{N}$, that is, we should be able to "count" them. For example,

$$\begin{array}{rl} 1 & \leftrightarrow \ 0.\, a_{11}a_{12}a_{13} \ \ldots \ a_{1n} \ \ldots \\ 2 & \leftrightarrow \ 0.\, a_{21}a_{22}a_{23} \ \ldots \ a_{2n} \ \ldots \\ 3 & \leftrightarrow \ 0.\, a_{31}a_{32}a_{33} \ \ldots \ a_{3n} \ \ldots \\ & \qquad\vdots \\ n & \leftrightarrow 0.\, a_{n1}a_{n2}a_{n3} \ \ldots \ a_{nn} \ \ldots \\ & \qquad\vdots \end{array}$$

Well, no. We cannot. Regardless of the construction of the sequence (*) of real numbers between 0 and 1, there are still numbers in this interval that are not contained in the list (*). Consider this: suppose we choose a decimal number

$$d = 0.\,\overline{a}_{11}\overline{a}_{22}\overline{a}_{33}\ \ldots$$

such that $\overline{a}_{ii} \neq a_{ii}$, that is, $\overline{a}_{11} \neq a_{11}$, $\overline{a}_{22} \neq a_{22}$, $\overline{a}_{33} \neq a_{33}$, and so on.

We can do this very easily. Say we first check $a_{11}$ in (*). If it is different from 1 we put $\overline{a}_{11} = 1$, but if it is equal to 1 we put $\overline{a}_{11} = 2$. Then we check $a_{22}$ and do the same: if $a_{22} \neq 1$, then we write $\overline{a}_{22} = 1$, and if $a_{22} = 1$, we write $\overline{a}_{22} = 2$. We continue this process for all $a_{ii}$ in our sequence (*). Of course, this is not the only way one can construct

$$d = 0.\,\overline{a}_{11}\overline{a}_{22}\overline{a}_{33}\ \ldots$$

In general, we can reason the following way: in the case that $a_{nn} = 0$, we have nine choices to make $\overline{a}_{nn}$ different. In the case that $a_{nn} \neq 0$, we still have eight choices for $\overline{a}_{nn}$. Hence, for every decimal digit, we have at least eight choices and, therefore, we have infinitely many choices for the number $d$. But whatever "technique" we use, note that the number $d$ cannot be found in our sequence (*), since it differs from the first number of (*) in the first decimal place. With the second number of (*), it differs in the second decimal place, and so on. We conclude that since the real number $d$ is different from all the numbers in our sequence (*), the sequence does not contain all the numbers between 0 and 1, contrary to our starting assumption. Hence, the set of numbers between 0 and 1 is uncountable. Since $(0, 1) \subseteq \mathbf{R}$, it follows that the set $\mathbf{R}$ is uncountable. ■

This proof is known as Cantor's diagonal argument. It turned out to be very important in mathematics and logic. There have been various versions of diagonal arguments, and the gist of it led to a number of very important results in mathematics. We have already encountered some of them in Section 1.7. You can find references to Cantor's argument over and over again in many discourses in mathematics, physics, computer science, philosophy, and so on. The next ingenious and witty example by Smullyan and Fitting[42] goes something like this:

**Example 1.98** Suppose there is a book with infinitely many pages: page 1, page 2, page 3, and so on. Obviously, the set of pages is countable. Furthermore, suppose that on each page there is a list, a set, of some natural numbers: on page 1 there is a set $N_1$, on page 2 there is a set $N_2$, on page 3 there is a set $N_3$, … on page $n$ there is a set $N_n$, and so on. The question is : Is every natural number listed in the book? The answer is no. There must be at least one set of natural

[42]R. M. Smullyan, M. Fitting, *Set Theory and the Continuum Problem,* Clarendon Press – Oxford, 1996.

numbers that is not listed in the book. In other words, there exists a set $N$, which is different from every one of the sets: $N_1, \ldots, N_n, \ldots$. Let's see why.

First consider the number 1 – either 1 belongs to set $N_1$ or it doesn't. We include it in $N$, **only if it does not** belong to $N_1$. Thus, whatever future decisions we make concerning the numbers $2, 3, \ldots, n, \ldots$, we know that $N \neq N_1$ because, **only one** of the two sets $N$ and $N_1$, contains 1 and the other doesn't. Next, we consider the number 2. We put it into $N$ only if it does not belong to $N_2$, and that makes $N \neq N_2$ (since one of them contains 2 and the other doesn't). We continue the process for every natural number $n$. This way, we constructed N such that for every $n$, $N \neq N_n$. What we have shown is that, given any countably infinite sequence $N_1, N_2, \ldots, N_n, \ldots$ of sets of natural numbers, there exists a set $N$ of natural numbers (namely, the set of all $n$ such that $n$ doesn't belong to $N_n$) such that $N$ is different from each of the sets $N_1, N_2, \ldots, N_n, \ldots$. This means that no countable set of sets of natural numbers contains every set of natural numbers, that is, the set of all sets of natural numbers is uncountable. ■

You may find the following two examples also engaging.

**Example 1.99** Let $r_1, r_2, r_3, \ldots$ be any sequence of real numbers, and let $[a_1, b_1], [a_2, b_2], [a_3, b_3], \ldots$ be a sequence of closed intervals where $a_i, b_i \in \mathbf{R}$, satisfying the following:

(i) $a_i < b_i, \quad \forall i$
(ii) $[a_i, b_i] \subseteq [a_j, b_j], \quad \forall i > j$
(iii) $r_i \notin [a_i, b_i]$

Because of (ii), $[a_1, b_1] \cap [a_2, b_2] \cap [a_3, b_3] \cap \cdots \neq \emptyset$. So suppose

$$r \in [a_1, b_1] \cap [a_2, b_2] \cap [a_3, b_3] \cap \cdots$$

Now, $r$ cannot be one of $r_1, r_2, r_3, \ldots$ because of (iii) and therefore

$$r \notin [a_1, b_1] \cap [a_2, b_2] \cap [a_3, b_3] \cap \cdots$$

Since the sequence $r_1, r_2, r_3, \ldots$ was arbitrarily chosen, it follows that no countable set of real numbers contains all real numbers. ■

**Example/Exercise 1.100** Give another example of a real number not in the list (*) on page 77, that is, construct another proof of the uncountability of real numbers.

**Example/Exercise 1.101** Prove that there are infinitely many possibilities to choose from along the original diagonal in (*) to construct another real number.

Although, generally, it is not easy to prove that a set is uncountable, fortunately, the following theorem is not difficult.

**Theorem 1.50** The set of all irrational numbers is uncountable.

***Proof*** Recall the set $\mathbf{R} \setminus \mathbf{Q} = \mathbf{I}$ is the set of irrational numbers.

Suppose now that the set $\mathbf{I}$ is countable. In that case, we could list all irrational numbers in a sequence $i_1, i_2, i_3, \ldots$. On the other hand, since rational numbers *are* countable, we can certainly list them as $q_1, q_2, q_3, \ldots$. Consequently, we could construct the following list:

$$i_1, q_1, i_2, q_2, i_3, q_3, \ldots \qquad (*)$$

Since $\mathbf{R} = \mathbf{Q} \cup \mathbf{I}$, the list (*) by construction should contain all real numbers and be countable. But that is impossible since $\mathbf{R}$ is uncountable. On the other hand, as we have established before, $\mathbf{Q}$ is countable. Hence, contrary to our supposition, the set $\mathbf{I}$ of all irrational numbers must be uncountable. ■

**Theorem 1.51** Let $A$ and $B$ be two sets such that $A \subseteq B$. If $A$ is uncountable, then $B$ is uncountable too.

***Proof*** Suppose not, that is, suppose $B$ is countable. $A$ being uncountable, and also a subset of the countable $B$, contradicts Theorem 1.35 thus $B$ has to be uncountable too. ■

**Example 1.102** If a set $A$ is uncountable, is it equivalent to $\mathbf{R}$?

**Solution** Of course not! Suppose we take $A = \mathcal{P}(\mathbf{R})$. $A$ is definitely uncountable, but at the same time $|\mathcal{P}(\mathbf{R})| > |\mathbf{R}|$. ■

**Theorem 1.52** Let $\mathcal{F} = \{f | f : \mathbf{N} \to \{0, 1\}\}$ be the set of all functions from $\mathbf{N}$ to $\{0, 1\}$. Then, $|\mathcal{F}| = |\mathcal{P}(N)|$

***Proof*** Let $\Phi : \mathcal{F} \to \mathcal{P}(\mathbf{N})$ be a function defined as follows:

$$\forall f \in \mathcal{F}, \Phi(f) = \{x \in \mathbf{N} \mid f(x) = 1\}$$

We would like to show that $\Phi$ is a bijection. So, let's take $f_1, f_2 \in \mathcal{F}$ such that $f_1 \neq f_2$. It follows that there exists $n \in \mathbf{N}$ such that $f_1(n) \neq f_2(n)$. Suppose $f_1, f_2$ are such that $f_1(n) = 1$ and $f_2(n) = 0$. Then,

$$n \in \{x \in \mathbf{N} \,|f_1(x) = 1\} = \Phi(f_1)$$

and similarly

$$n \notin \{x \in \mathbf{N} | f_2(x) = 1\} = \Phi(f_2)$$

Thus, $\Phi(f_1) \neq \Phi(f_2)$, that is, $\Phi$ is a one-to-one function. Is it onto? Well, consider a set $A \in \mathcal{P}(\mathbf{N})$. Then $A \subseteq \mathbf{N}$, and the characteristic function (see Chapter 4)

$$\chi_A : \mathbf{N} \to \{0, 1\}$$

is obviously an element of $\mathcal{F}$. Furthermore,

$$\Phi(\chi_A) = \{x \in \mathbf{N} \mid \chi_A(x) = 1\} = A$$

Thus, $\Phi$ is onto. Consequently, $|\mathcal{F}| = |\mathcal{P}(N)|$. ■

The following is also true.

**Theorem 1.53** A set $F = \{f | f : \mathbf{N} \to \mathbf{N}\}$ of all functions from $\mathbf{N}$ to $\mathbf{N}$ is uncountable.

*The mind of thee upon these lines of ours,*
*Till thou see through the nature of all things,*
*And how exists the interwoven frame*

*It has no bounds, no end, no limit,*
*And it matters not what part of the universe you are in;*
*Wherever you are, from the spot you take up,*
*It stretches to infinity in all directions. …*

*Titus Lucretius Carus*[43]

What is that thing which does not give itself, and which if it were to give itself would not exist? It is infinite!

*Leonardo da Vinci*[44]

## 1.9 A SHORT MUSING ON TRANSFINITE ARITHMETIC

### The Hilbert Hotel

*Let's imagine an Infinity Hotel, also (appropriately) known as the Hilbert Hotel, with infinitely many rooms (numbered 1, 2, 3, … and so on forever). As an infinite*

[43] Titus Lucretius Carus (ca. 99–55 BC), *De Rerum Natura.*
[44] Leonardo da Vinci (1452–1519), *Notebooks.*

*number of guests (mathematicians [sic!] attending a mathematics convention) occupy all rooms, the receptionist is convinced there are no vacancies and all latecomers should be turned away. "Not so," the manager exclaimed. When the next VIP arrives, move the person from room 1 to room 2, the person from room 2 to room 3, the person from room 3 to room 4, etc. This leaves room 1 vacant while everyone else is properly accommodated. In case more latecomers arrive the manager repeats the process. So infinitely many newcomers are accommodated. It turned out that infinitely many physicists came to the conference too, but the manager is not worried at all. He keeps guest from room 1 in room 1 but moves the guest from room 2 to room 4, the guest from room 3 to room 9, … , the guest from room n to room $n^2$ and so on forever. Obviously infinitely many rooms are now ready to accommodate all the physicists. And, as you might have anticipated, when in addition to all previous guests, infinitely many philosophers and infinitely many rock concert fans arrive, all of them are accommodated by similar methods. But this is not the end of the story. As is often in life, things turn unexpectedly odd. The Infinity Hotel became so profitable and soon enough infinitely many infinity hotels opened up: Hotel 1, Hotel 2, Hotel 3, … and so on forever. However, one day all the guests from those hotels, for some strange reason decided they wanted to move to the original Infinity Hotel. Our ingenious manager now has to accommodate infinitely many guests from each of infinitely many hotels. Here is what he does. Consider all prime numbers (there are infinitely many of them):* $2, 3, 5, 7, 11, 13, \ldots$, *and then do the following: put infinitely many guests from Hotel 1 into rooms 2, 4, 8, 16,* … $2, 4, 8, 16, \ldots$ (*i.e.*, $2^1, 2^2, 2^3, 2^4, \ldots$)*; those from Hotel* 2 *into rooms* $3, 9, 27, 81, \ldots$ (*i.e.*, $3^1, 3^2, 3^3, \ldots$ *etc.*); *those arriving from Hotel* 3 *into rooms* $5, 25, 125, 625, \ldots$ (*i.e.*, $5^1, 5^2, 5^3, \ldots$ *etc.*). *Continuing this process manager is sure that while accommodating all the guests from all the hotels no two persons will occupy the same room.*

At the beginning of Section 1.8, we asked: How big is "big." How do we determine whether one set is "larger" than the other? Let's think about this for a moment. We have already established that any infinite subset of a set of natural numbers is countable. Can we prove that any infinite set contains a countable subset? Let's see. Take any infinite set $X$. We can always pick a nonempty (infinite) countable subset $A \subseteq X$ the following way: remove one element, say, $a_1$ from $X$. Certainly, $X \setminus \{a_1\}$ is still an infinite set. Let's remove another element, $a_2$, which keeps $X \setminus \{a_1, a_2\}$ still infinite. We continue this process choosing $a_3, a_4, a_4, \ldots$ to be removed from $X$. Thus, we have extracted from $X$ a countable set $A = \{a_1, a_2, a_3, \ldots, a_n, \ldots\}$ and $X$ nevertheless remains to be an infinite set. As you might have anticipated by now, we could continue with these arguments further and, for instance, remove from $A$ the set of all elements with even indices, $B = \{a_2, a_4, a_6, \ldots\}$ and $A \setminus B$ remains countably infinite. We conclude that the cardinality of an infinite set does not change if we adjoin a countable set to it. And certainly cardinality of an uncountable set won't change if we extract a countable subset from it. It is reasonable to wonder how come that all infinities

are not the same? Also, recall that the sets we may want to study could have as elements whole families of countable or uncountable elements. The following few examples will make this more transparent.

**Example 1.103** Consider the following set $\mathcal{F} = \{\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}\}$. Observe that $\mathcal{F}$ is a finite (thus countable) family of sets. No matter that all of its elements are infinite sets themselves. ■

**Example 1.104** For each $i \in \mathbf{N}$, let's construct a family of sets $\mathbf{N}_i$, where each $\mathbf{N}_i$ is the set of all natural numbers divisible by $i$, that is, starting with $\mathbf{N}_1 = \mathbf{N}$ we have

$$\begin{aligned}
\mathbf{N}_2 &= \{2, 4, 6, \ldots, 2n, \ldots\} \\
\mathbf{N}_3 &= \{3, 6, 9, \ldots, 3n, \ldots\} \\
&\vdots \\
\mathbf{N}_i &= \{i, 2i, 3i, \ldots, ni, \ldots\} \\
&\vdots
\end{aligned}$$

Thus, we have obtained an infinite family of infinite countable sets

$$\mathcal{F} = \{\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3, \ldots, \mathbf{N}_i, \ldots\}$$ ■

Next is the example that we have encountered in a slightly different context earlier. Recall that the set $\boldsymbol{Q}^+$ is a countable set (Theorem 1.33), and this time let's look at Cantor's proof from the perspective of an infinite family of sets:

**Example 1.105** Define

$$\begin{aligned}
\mathbf{Q}_1^+ &= \left\{\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots\right\} \\
\mathbf{Q}_2^+ &= \left\{\frac{2}{1}, \frac{2}{2}, \frac{2}{3}, \ldots, \frac{2}{n}, \ldots\right\} \\
\mathbf{Q}_3^+ &= \left\{\frac{3}{1}, \frac{3}{2}, \frac{3}{3}, \ldots, \frac{3}{n}, \ldots\right\} \\
&\vdots \\
\mathbf{Q}_m^+ &= \left\{\frac{m}{1}, \frac{m}{2}, \frac{m}{3}, \ldots, \frac{m}{n}, \ldots\right\} \\
&\vdots
\end{aligned}$$

So we have obtained an infinite, countable family

$$\mathcal{F} = \{\mathbf{Q}_1^+, \mathbf{Q}_2^+, \mathbf{Q}_3^+, \ldots, \mathbf{Q}_m^+, \ldots\}$$

whose elements are exactly the rows in Cantor's diagram. ■

Thus, questions about the "nature" of infinities, and indeed, how many "infinities" there are, are inevitable.

Here is Cantor again:

**Definition 1.43 (Cantor)** A set $A$ is greater than a set $B$ if and only if $B$ is equivalent to some subset of $A$, but $A$ is not equivalent to any subset of $B$.

Cantor also showed that $\aleph_0$ is the smallest infinite cardinal number, and following Cantor we have shown that $\aleph > \aleph_0$. We have established the fact that there are at least two different sorts of infinite sets, two different "kinds" of infinities, that is, two different kinds of cardinal numbers. Let's remind ourselves what Cantor meant by the cardinal number of a set $X$:

> *… the general concept which by means of our active faculty of thought, arises from the aggregate X when we make abstraction of the nature of its various elements x and of the order in which they are given.*

Now we ask: Is there a cardinal number greater than $\aleph$? Cantor's answer is this: For any set $X$, there exist sets larger than $X$, in particular $\mathcal{P}(X)$. So, for instance $|\mathbf{N}| < |\mathcal{P}(\mathbf{N})|$, thus we are prompted to consider the following:

$$\begin{aligned} \aleph_0 &= |\mathbf{N}| \\ 2^{\aleph_0} &= |\mathcal{P}(\mathbf{N})| \\ 2^{2^{\aleph_0}} &= |\mathcal{P}(\mathcal{P}(\mathbf{N}))| \\ &\vdots \end{aligned}$$

Consequently, we can naturally proceed and construct a hierarchy of **transfinite** cardinals:

$$\aleph_0, 2^{\aleph_0}, 2^{2^{\aleph_0}}, 2^{2^{2^{\aleph_0}}}, \ldots \qquad (*)$$

Hence

**Theorem 1.54** There is an infinite sequence of infinite cardinals

$$\aleph_0 < \aleph_1 < \aleph_2 \cdots$$

where $\aleph_0 = |\mathbf{N}|$, $\aleph_1 = |\mathcal{P}(\mathbf{N})|$, $\aleph_2 = |\mathcal{P}(\mathcal{P}(\mathbf{N}))|$, and so on.

***Proof*** We have learned from Theorem 1.8.1 that $\aleph_0 < \aleph_1$. Next, consider $\aleph_2$. It is obviously a cardinal number of the power set of the set $\mathcal{P}(\mathbf{N})$. Thus, according to Theorem 1.31, $\aleph_1 < \aleph_2$. So, we have established that

$$\aleph_0 < \aleph_1 < \aleph_2 \cdots$$

There is no reason to stop at $\aleph_2$, so in general for any $n$ we have

$$\aleph_{n-1} < \aleph_n = |\mathcal{P}(\mathcal{P}(\mathcal{P}( \ldots \ (\mathcal{P}(\mathbf{N}))) \ \ldots)|$$

Hence, there is indeed a sequence of infinite cardinals

$$\aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_n < \cdots$$

which we recognize as our sequence (*). If you wish to "visualize" the aforementioned sequence, you may consider the following picture, but keep in mind, the line pictured is not a real line (Figure 1.21).

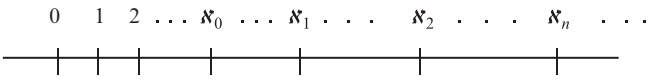



**Figure 1.21**

■

Where is the cardinal number of **R** in this sequence? It can be shown (cf. Theorem 1.12) that the cardinal number of the reals

$$|\mathbf{R}| = |\mathcal{P}(\mathbf{N})| = 2^{\aleph_0}$$

We conclude that the set of all real numbers **R** is equivalent to the set of all subsets of natural numbers $\mathcal{P}(\mathbf{N})$.

So, our sequence (*) is as expected

$$\aleph_0, \aleph_1, \aleph_2, \aleph_3, \ \ldots \qquad (**)$$

assuming that there is no cardinal number between $\aleph_0$ and $2^{\aleph_0}$, that is, no cardinal number greater than $\aleph_0$ and less than $2^{\aleph_0}$. Well, can we assume this? And why? Cantor said yes, $2^{\aleph_0} = \aleph_1 = c$,[45] that is, we take $|\mathbf{R}| = \aleph_1$. However, he was unsuccessful in proving it. This is what is known as the **Continuum Hypothesis (CH)**.

[45] Remember, we are assuming the Continuum Hypothesis, that is, $c = \aleph_1$

Let's have some fun and reflect on the issue some more. It is important to keep in mind that in the following lines, as in this whole section, we are just musing, and by no means do we expect to give the proof of the hypothesis, or anything even close to a definite answer. Some would suggest that the question of CH is subjective, and the whole issue has to do with how strong a Platonist you (the mathematician) are.

First, recall that the sets $\mathbf{N}$ and $\mathbf{Q}$ are countable and the set $\mathbf{R}$ is not. Also, remember $\mathbf{N} \subseteq \mathbf{Q} \subseteq \mathbf{R}$. Cantor conjectured that there is no set $X$ such that it has more elements than $\mathbf{N}$ and fewer elements than $\mathbf{R}$, that is

$$\nexists X \text{ s.t. } |\mathbf{N}| < X < |\mathbf{R}|$$

Remember (cf. Chapter 1.5), given a set $A$ such that $|A| = n$, then $|\mathcal{P}(A)| = 2^{|A|} = 2^n$. Hence, there are more elements in $\mathcal{P}(A)$ than in $A$. Consequently, for given $n = |A|$ there are $2^n - (n + 1)$ sets having the number of elements greater than $n$ and less than $2^n$. In general, for any sets $A$ and $B$ if

$$|B| \leq |A| \leq |\mathcal{P}(B)|$$

then either $A \sim B$ or $A \sim \mathcal{P}(B)$. Translating this to alephs, we get to the **generalized continuum hypothesis:**

$$2^{\aleph_n} = \aleph_{n+1}$$

Once we have "convinced" ourselves of this fact, it is natural to contemplate the extension of this to sets $\mathbf{N}$ and $\mathbf{R}$. Suppose there is a set $X$ with more elements than $\mathbf{N}$ and fewer than $\mathbf{R}$. Then $X$ should be such that

$$|\mathbf{N}| < |X| < 2^{|\mathbf{N}|}$$

Now, $2^{|\mathbf{N}|} > |\mathbf{N}|$ and (cf. Theorems 1.12, 1.31, and Definition 1.43) $2^{|\mathbf{N}|}$ is the number of elements of $\mathbf{R}$. Hence, $2^{|\mathbf{N}|}$ cannot be the cardinality of any set between $\mathbf{N}$ and $\mathbf{R}$. Everything said earlier is correct (except the last sentence – "Hence … " is kind of a stretch), but somehow your instinct might be telling you that something is still missing – our "proof" is not satisfying. No wonder many mathematicians have unsuccessfully struggled with the problem for years. In 1931, Kurt Gödel used the techniques of mathematical logic to show that Continuum Hypothesis could not be disproved on the basis of available axioms.[46] That, of course, does not mean that it could be proved either. In 1963, Paul Cohen took it one step further and showed that it was also impossible to prove the Continuum Hypothesis. All efforts were unfruitful, because the assumptions of set theory,

[46]Zermelo–Fraenkel axioms.

which Cantor and others used, were independent of the Hypothesis. Being aware of Gödel's work, Cohen concluded:

> *Set Theory with the assumption of the Continuum Hypothesis is consistent; Set Theory with the denial of Continuum Hypothesis is consistent.*

So, what are we to make of all this? Obviously, we are venturing into the territories beyond everyday experiences. In standard mathematics, saying that you *cannot* prove that $A = B$ but that you *can* prove that $A \neq B$ would sound pretty odd. Here, however, we are talking "the other" mathematics. Simply put, alephs are definitely different kinds of numbers (for lack of a better word), or at least "numbers" that many of us have never thought about before, and consequently every statement regarding them has to be pondered over with special care. Before we continue with our "regular" mathematics, I cannot resist the temptation of showing you something I find extremely fascinating. What follows is again mostly due to Cantor. The concepts that we will briefly touch upon are generally uncontroversial nowadays. However, although the logical consistency of the theory is indisputable, one might occasionally hear some dissonant voices regarding the existence and the "reality" of infinities. I'll let you make up your own mind.

> Alfred North Whitehead, however, would say: "*Our minds are finite, and yet even in the circumstances of finitude we are surrounded by possibilities that are infinite, and the purpose of life is to grasp as much as we can of that infinitude.*"

With this encouragement in mind, we may continue a bit further. Mathematics – any mathematics – is about thinking, wouldn't you agree? And thinking is "due" to our mind (whatever that may be). So, let's also agree, for starters at least, that admitting that mathematics (as well as science and philosophy) has its limitations does not imply that there are limitations of the universality of reason. (All right, I concede that this is a rather big assumption, but let's not dwell on it for the time being.) Accordingly, here are some new realms that our mind can explore.

Recall what Cantor meant by the cardinal number: the cardinal number of a set $X$ is what $X$ has in common with all the sets equivalent to $X$. We get cardinal number(s) by simply counting: $1, 2, 3, \ldots, \aleph_0$. In other words, the cardinal number indicates how many members there are in a given set. Nothing is said as to how they are *ordered.* That's why, you may recall, he denoted the cardinal number of a set $X$ as $\overline{\overline{X}}$.[47] It is worth repeating that the double bar indicates double abstraction, first from the nature of the elements and second from their order. Now, consider the sequence (**) on page 84. We start with 1 and then 2, and so

[47] This should not cause confusion with our notation $|X|$. See Definition 1.9.

on until we reach the first transfinite cardinal, the second transfinite cardinal, and so on. In other words, we have the sequence

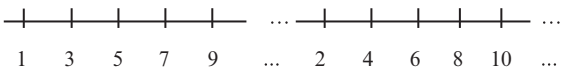
$$1,\ 2,\ 3,\ \ldots\ ,\ \aleph_0, \aleph_1, \aleph_2, \aleph_3,\ \ldots \qquad (***)$$

in which subscripts indicate the ordering by the size of transfinite cardinals.

We can lump them all in some set, the set of cardinals, but now we also distinguish which one is the first element, which one is the second, and so on. With such ordering, we obtained the set of *ordinal numbers.* What are those? Strictly speaking, every time when we count and use the expressions "first," "second," "third," and so on, we talk about ordering the elements in a set. Think about it this way: We can use natural numbers to count (and that's why some call them "counting numbers"), and so on to answer the question of "how many" of a certain object we have: one, two, three, and so on, and in this case, we call them *cardinals.* But if we want to answer the question "in which order" the objects are arranged, and so on, which object is first, second, third, and so on, we call them *ordinals.* Now comes the important part. Suppose we list the elements of the set **N** in the following way:

$$1, 3, 5, 7,\ \ldots\ , 2, 4, 6,\ \ldots$$

that is, we first list all odd natural numbers and then we list all even natural numbers. We could picture this as in Figure 1.22.

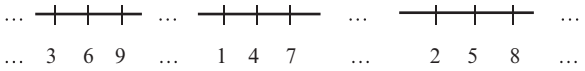



(1)

**Figure 1.22**

Suppose now that we want to enumerate them. How could we do that? As you already know, we would "exhaust" the whole of set **N** just to enumerate the odds, and we would still be left with infinity many evens (i.e., $\aleph_0$ of them) without any means of counting them. The same problem would arise if we wanted to first list all numbers, say, divisible by 3, and then those which leave remainder 1 after division by 3, and those that leave remainder 2 after division by 3, that is, $3, 6, 9,\ \ldots\ , 1, 4, 7,\ \ldots\ , 2, 5, 8,\ \ldots$

This would look something like in Figure 1.23.




(2)

**Figure 1.23**

Obviously, we need some other symbol to take care of this "problem." Cantor introduced the symbol $\omega$ to account for the problem of emerging *transfinites*. Let's superimpose a "picture" of $\{1, 2, 3, 4, 5, \ldots, n, \ldots\}$ on (1) in Figure 1.22:

The first transfinite ordinal $\omega$ corresponds to 2, $\omega + 1$ to 4, and so on. So, how many transfinite numbers are there? Let's look at (2) again, but this time taking into account the just acquired concept of the transfinite $\omega$. We get something like Figure 1.24.

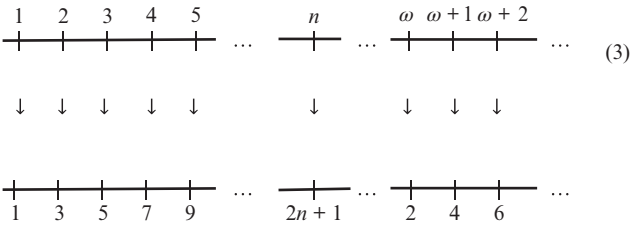



**Figure 1.24**

Yet another way to look at this.

Consider "Zeno-like" running on the real line such that every "step" (every number) is at half the distance of the previous one. That will look something like this:

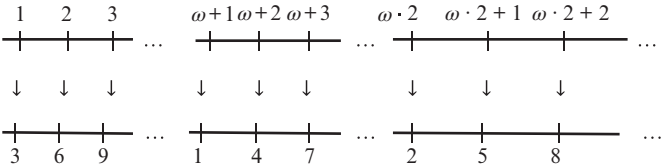



**Figure 1.25**

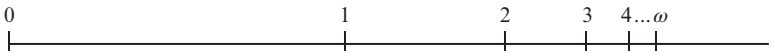



**Figure 1.26**

Now, "superimpose" a copy of Figure 1.25 onto each of the spaces between the points 0 and 1, 1 and 2, 2, and 3, and so on. That will look something like Figure 1.27.

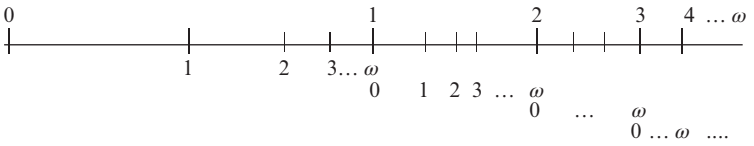



**Figure 1.27**

Repeating the process again we come to:

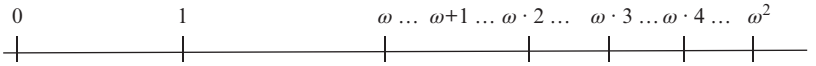



**Figure 1.28**

Doing it one more time gives: Figure 1.29

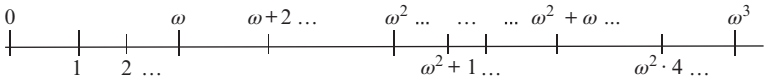



**Figure 1.29**

Repeating the process over and over again, we get the "final result" that would look something like Figure 1.30:

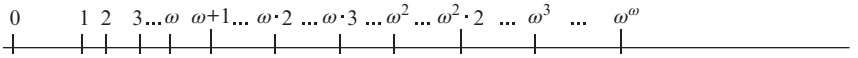



**Figure 1.30**

Of course, there is no reason to stop there, so the answer to the question of how many ordinal numbers there are is: There are infinitely many of them! Well, said Cantor, let's collect them "all," according to the following recipe: If $\alpha$ is an ordinal number, then we can always find the next ordinal $\alpha + 1$, and once we obtain a definite sequence of increasing ordinals, then we can find the last ordinal, called $\lim(\alpha)$, which is greater than all the $\alpha$'s. Thus, the following series of ordinals (which we tried to "visualize" earlier) is

$$1, 2, \ldots, \omega$$

$$\omega + 1,\ \omega + 2,\ \ldots$$
$$\omega \cdot 2,\ \omega \cdot 2 + 1,\ \omega \cdot 2 + 2,\ \ldots$$
$$\omega \cdot 3,\ \omega \cdot 3 + 1,\ \omega \cdot 2 + 2,\ \ldots$$
$$\vdots$$
$$\omega^2,\ \omega^2 + 1,\ \omega^2 + 2,\ \omega^2,\ \ldots$$
$$\omega^2 + \omega,\ \omega^2 + \ (\omega + \ 1),\ \omega^2 + (\omega + 2),\ \ldots$$
$$\vdots$$
$$\omega^3,\ \omega^3 + 1,\ \omega^3 + 2,\ \ldots$$
$$\vdots$$

An important note is in order. Unlike finite ordinals, the infinite ordinals demand a particular "order of operation," namely, commutativity no longer holds. Observe that $1 + \omega = \omega$, but $\omega + 1$ is the next "number" after $\omega$. In other words,

$$1 + \omega = \omega \neq \omega + 1$$

Similarly, $2 \cdot \omega = \omega$, but $\omega \cdot 2 = \omega + \omega$.

We continue this way until we reach

$$\omega^\omega,\ \omega^\omega + 1,\ \omega^\omega + 2,\ \ldots$$
$$\vdots$$

And on and on until we reach

$$\omega^{\omega^\omega},\ \omega^{\omega^\omega} + 1,\ \omega^{\omega^\omega} + 2,\ \ldots$$
$$\vdots$$

Continuing this way (and now it really gets complicated), we come to a new sequence

$$\varepsilon_0, \varepsilon_1, \varepsilon_2,\ \ldots$$

where $\varepsilon_0 = \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}$.

We can go on like this forever, right? Why not? Well, we "have been going" forever already while "counting" to $\omega$, so "going" to $\varepsilon_0$ means – what?

Do you see where "*this*" is going? Do you see where our mind is taking us? Do you feel the richness of the underlining theory? Talking about "big," really, really "big," infinitely big, infinitely, infinitely big. The Absolute???

*We know that the infinite exists without knowing its nature, just as we know that it is untrue that numbers are finite. Thus it is true that there is an infinite number, but we don't know what it is.*[48]

So Cantor said:

*The Absolute can only be acknowledged and admitted, never known, not even approximately.*

Before I offer you another paradox, let's sum up what we know about ordinals:

(i) There is a first ordinal.
(ii) For each ordinal, there is an immediate successor ordinal.
(iii) For each set of ordinals, there is an ordinal which is the first succeeding them all.

So, we get the familiar sequence (cf. Example 1.61)

$$\begin{aligned}
0 &= \varnothing \\
1 &= \{\varnothing\} \\
2 &= \{0,1\} = \{\varnothing, \{\varnothing\}\} \\
3 &= \{0,1,2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \\
&\vdots \\
\omega &= \{0,1,2,3,\ldots\} \\
&= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \ldots\} \\
\omega+1 &= \{0,1,2,3,\ldots,\omega\} \\
\omega+2 &= \{0,1,2,3,\ldots,\omega,\omega+1\} \\
&\vdots \\
&\vdots \\
\omega\cdot 2 &= \{0,1,2,3,\ldots,\omega,\omega+1,\ldots\} \\
\omega\cdot 2+1 &= \{0,1,2,3,\ldots,\omega,\omega+1,\ldots,\omega\cdot 2\} \\
&\vdots \\
&\vdots
\end{aligned}$$

Now consider

[48] Blaise Pascal, *Penseés.*

### The Burali-Forti[49] Paradox

Suppose we are tempted to form a set $\Omega$ of *all* (infinitely many) ordinals. Can we do that? After all, we have a set of all natural numbers, rational numbers, real numbers, and so on, so why not do the same with ordinals? Well, if the set $\Omega$ exists, then it is the set (of ordinals) like any other. But then, by condition (iii), there must be *another ordinal*, $\Omega + 1$, the first to succeed it, that is, the first to succeed all the members of $\Omega$. In other words, $\Omega < \Omega + 1$. But that contradicts the assumption that $\Omega$ contains *all* ordinals. We conclude: *The ordinal numbers do not form a set.*

In the same way by which we can always find more ordinals, we can always "find" more cardinals. Consider this sequence:

$$\aleph_0, \aleph_1, \aleph_2, \ \dots\ , \aleph_\omega, \aleph_{\omega+1}, \ \dots\ \aleph^{\omega^\omega}, \ \dots$$

As you might have anticipated by now, we do not stop here. A whole new universe of more and more complex structures opens up and the mathematics of transfinite turns out to be an exceptionally rich and philosophically exciting theory.

The assiduous reader may feel a little uneasy by now. After all the discussion of the transfinite, the author, with all of his fascination with alephs, so far has still not satisfactorily defined the very culprit of all of this – the real number(s). We will do that in a moment, but let's see briefly some of the remarkable features of ***arithmetic of transfinites***. We start with

**Theorem 1.55** Let $\aleph$ be any infinite cardinal then

(i) $0 + \aleph = \aleph$
(ii) $n + \aleph = \aleph, \ \ \forall n \in \mathbf{N}(n \text{ is finite})$

***Proof***

(i) Let $X$ be a set s.t. $|X| = \aleph$. We know that $0 = |\varnothing|$, thus we have

$$0 + \aleph = |\varnothing \cup X| = |X| = \aleph$$

(ii) Since $X$ is an infinite set, there exists a set $A = \{a_1, \ a_2, \ \dots\ , \ a_n\ \} \subseteq X$, then

$$n + \aleph = |A \cup X| = |X| = \aleph \qquad \blacksquare$$

[49] Cesare Burali-Forti (1861–1931), Italian mathematician.

**Example 1.106** Let $n$ be a finite cardinal number. Then

$$n + \aleph_0 = |\{1, 2, 3, \ldots, n\} \cup \{n+1, n+2, \ldots\}| = \aleph_0$$ ■

**Example 1.107** From Theorem 1.55, it follows that

$$\aleph_0 + 0 = \aleph_0 + 1 = \aleph_0 + 10^{10^{10^{10}}} \qquad (*)$$

You might immediately object that equation (*) cannot be true since, by elementary school algebra, (*) implies that $1 = 0$, which is obviously an absurdity. But remember, we are not doing ordinary algebra! Although the addition of transfinites is (well?) defined, interestingly enough, subtraction is not. Why not? Well, consider

$$\aleph_0 + 1 = \aleph_0$$

This one we can believe (we have proved even more: $\aleph_0 + \aleph_0 = \aleph_0$). Using ordinary algebra, we could go a step further and argue that

$$\begin{aligned} 1 + 0 &= 1 + \aleph_0 - \aleph_0 \\ &= (1 + \aleph_0) - \aleph_0 \\ &= \aleph_0 - \aleph_0 \\ &= 0 \end{aligned}$$

concluding that

$$1 = 0$$

which, of course, is nonsense. Therefore, we are forced to accept that $\aleph_0 - \aleph_0$ simply is not defined. ■

However, things are quite different for addition. Consider the following:

**Example 1.108**

$$\aleph_0 + \aleph_0 = |\{2, 4, 6, \ldots\} \cup \{1, 3, 5, \ldots\}| = |\{1, 2, 3, 4, 5, \ldots\}| = \aleph_0$$ ■

Actually, this can be generalized even further.

**Theorem 1.56** Let $\aleph_\alpha$ and $\aleph_\beta$ be two infinite cardinals such that $\aleph_\alpha < \aleph_\beta$. Then,

$$\aleph_\alpha + \aleph_\beta = \aleph_\beta$$

***Proof*** Let $A$ and $B$ be two sets s.t. $|A| = \aleph_\alpha$ and $|B| = \aleph_\beta$. If $\aleph_\alpha < \aleph_\beta$, then there exists a one-to-one function

$$f : A \to B$$

We need to show that $A$ and $f(A)$ are equivalent sets. Consider the function

$$g : A \to f(A)$$

defined by the same rule as $f$, except that it is restricted to map $A$ into $f(A) \subseteq B$. Since we choose $f$ as one-to-one, $g$ is also one-to-one by construction. Note that although $f$ may not be onto, we would like $g$ to be onto. To see that $g$ is onto, let's take some $y \in f(A)$. By definition of $f(A)$ there has to be an $x \in A$, such that

$$y = f(x) = g(x)$$

We conclude that $g$ is onto, and therefore a bijection. Thus $A$ and $f(A)$ are equivalent, that is, $|A| = |f(A)|$.

Since $f(A) \subseteq B, f(A) \cup B = B$, we get the following:

$$\begin{aligned} \aleph_\alpha + \aleph_\beta &= |f(A)| + |B| \\ &= |f(A) \cup B| \\ &= |B| \\ &= \aleph_\beta \end{aligned}$$

which was to be proved. ■

**Example 1.109**

$$\aleph_0 + 2^{\aleph_0} = \aleph_0 + \aleph_1 = \aleph_0 + c = c$$ ■

**Example 1.110** Let's examine the "sum" $c + c$ on the interval $[0, 1]$:

$$c + c = \left| \left[0, \frac{1}{2}\right] \cup \left(\frac{1}{2}, 1\right] \right| = c$$ ■

**Example 1.111**

$$\aleph + 2^{\aleph} = 2^{\aleph}$$

Since $\aleph_0$ is the first infinite cardinal, it follows that $\aleph_0 \leq \aleph$ for any other infinite cardinal. Hence, as a consequence of Theorem 1.56, $\aleph_0$ behaves as a neutral element with respect to addition of infinite cardinals, that is, it always holds that

$$\aleph + \aleph_0 = \aleph_0 + \aleph = \aleph$$

Since cardinals can be added, we conclude that

$$\aleph + \aleph + \cdots + \aleph = n \cdot \aleph = \aleph, \quad \forall\ \in \mathbf{N} \tag{*}$$

■

However, we also have

**Theorem 1.57** Let $\aleph$ be an infinite cardinal. Then,

$$0 \cdot \aleph = 0$$

***Proof*** In Example/Exercise 1.64, you were asked to prove that for any set $A$, $A \times \varnothing = \varnothing \times A = \varnothing$. If you haven't done it, let's do it now so we can use that to prove our theorem.

Suppose $A \times \varnothing \neq \varnothing$. Then, there exists an $n \in A \times \varnothing$ such that $n = (x, y)$, with $x \in A$ and $y \in \varnothing$. But this contradicts the fact that $\varnothing$ has no elements. Thus, our supposition was wrong and we conclude that

$$A \times \varnothing = \varnothing \times A = \varnothing$$

as claimed. Since we didn't specify $A$ to be any particular set, we take that our assertion also holds for any set; therefore, $\mathbf{N} \times \varnothing = \varnothing$ as well as $\mathbf{R} \times \varnothing = \varnothing$. Now the proof of the theorem follows immediately: Consider a set $A$ such that $|A| = \aleph$.

$$0 \cdot \aleph = |\varnothing \times A| = |\varnothing| = 0$$

■

So far so good. But now the next natural question arises: if we accept the statement (*) from Example 1.111, how far can we push the multiplication of alephs? In other words, what is $\aleph_0 \cdot \aleph_0$? Or, in general, $\aleph \cdot \aleph_0$?

Recalling our discussion of the Cartesian product from Chapter 1.6, you can easily convince yourself that if we are given $k$ finite sets $A_1, A_2, \ldots, A_k$ such that

$$A_1 = n_1, |A_2| = n_2, \ldots, |A_k| = n_k$$

then

$$|A_1 \times A_2 \times \ldots \times A_k| = n_1 \cdot n_2 \cdot \ldots \cdot n_k$$

Indeed, each element in $A_1 \times A_2 \times \ldots \times A_k$ is a $k$-tuple of the form $(a_1, a_2, \ldots, a_k)$, where $a_i \in A_i$. Thus, there are $n_1$ ways to choose the first element in a $k$-tuple, $n_2$ ways to choose the second one, and so on. Therefore,

there are $n_1 \cdot n_2 \cdot \ldots \cdot n_k$ elements in $A_1 \times A_2 \times \ldots \times A_k$. We extend this formalism to calculate the product of infinite cardinals by

**Definition 1.44** Let $A$ and $B$ be two sets such that $|A| = \aleph_\alpha$ and $|B| = \aleph_\beta$ are respective infinite cardinals. Then, we define

$$\aleph_\alpha \cdot \aleph_\beta = |A \times B|$$

**Example 1.112**

$$\begin{aligned} \aleph_0 \cdot \aleph_0 &= |\mathbf{N} \times \mathbf{N}| \\ &= |\mathbf{N}| \\ &= \aleph_0 \end{aligned}$$

Note that we utilize Theorem 1.37 in the second step. ■

This rule is valid for any other aleph, that is

$$\aleph \cdot \aleph = \aleph$$

Here is another good example:

**Theorem 1.58** $\mathbf{R} \sim \mathbf{R} \times \mathbf{R}$. That is to say $|\mathbf{R} \times \mathbf{R}| = |\mathbf{R}|$.

***Proof*** Consider a function

$$f : \mathbf{R} \to \mathbf{R} \times \mathbf{R}$$

defined by $f(x) = (x, 0), \ \forall x \in \mathbf{R}$. $f$ is clearly a one-to-one function. In order to complete the proof, we also need another one-to-one function

$$g : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$$

Since the cardinality of the interval $(0, 1)$ is the same as the cardinality of $\mathbf{R}$, rather than working with the whole $\mathbf{R}$ we prefer to work with

$$g : (0, 1) \times (0, 1) \to (0, 1)$$

defined by

$$g(0.\, a_1a_2a_3 \ \ldots\ , 0.\, b_1b_2b_3 \ \ldots) = 0.\, a_1b_1a_2b_2a_3b_3 \ \ldots$$

with the only restriction that the $a_i'$ s and $b_i's$ not be repeating nines. Thus, $g$ is a well-defined function and it is clearly one-to-one. The Schröder–Bernstein theorem immediately leads to the desired proof. ■

**Example/Exercise 1.113** Show that $\mathbf{R} \times \mathbf{R} \times \mathbf{R} \sim \mathbf{R}$.

**Theorem 1.59** Let $A$ and $B$ be two sets such that $|A| = \aleph_\alpha$ and $|B| = \aleph_\beta$ are respective infinite cardinals. Then,

$$\aleph_\alpha \cdot \aleph_\beta = \aleph_\beta \cdot \aleph_\alpha$$

***Proof*** Consider a function

$$f : A \times B \to B \times A$$

defined by

$$f(a, b) = (b, a)$$

The function $f$ is obviously a bijection. That implies

$$\aleph_\alpha \cdot \aleph_\beta = |A \times B| = |B \times A| = \aleph_\beta \cdot \aleph_\alpha$$

which was to be proved. ■

Without proof, we state

**Theorem 1.60** If $\aleph_\alpha$ and $\aleph_\beta$ are two infinite cardinals such that $\aleph_\alpha \leq \aleph_\beta$, then

$$\aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$$

that is, the larger of the two cardinals.

The following examples illustrate another "unusual" consequence of multiplication of alephs.

**Example 1.114**

$$\aleph \cdot \aleph = \aleph^2$$

but also

$$\aleph \cdot \aleph = \aleph$$

Thus,

$$\sqrt{\aleph} = \aleph$$ ■

A few more peculiar properties of infinite cardinals are listed without proof in the following theorem.

**Theorem 1.61** If $n \in \mathbf{N}$ is any finite cardinal, then

(i) $n^{\aleph_0} = \aleph_0^{\aleph_0} = \mathfrak{c}^{\aleph_0} = \mathfrak{c}$
(ii) $2^{\mathfrak{c}} = n^c = \aleph_0^{\mathfrak{c}} = \mathfrak{c}^{\mathfrak{c}}$

**Example 1.115**

(i) $c \cdot c = c^{50}$
(ii) $\aleph_0 \cdot c = c$
(iii) $\aleph_0 \cdot \aleph = \aleph$
(iv) $\aleph \cdot \aleph \cdot \aleph = \aleph$

■

**Example 1.116**

(i) $c^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \aleph_0} = 2^{\aleph_0} = c$
(ii) $c^c = (2^{\aleph_0})^c = 2^{\aleph_0 c} = 2^c = c$ ■

**Example/Exercise 1.117** Prove that $c^{\aleph_0} = c$.

It is very important to stress again that, regardless of the fact that we "know" how to multiply cardinals, the division is not defined. Our inherent intuition is worthless when dealing with alephs. Here is a simple example: Suppose we can divide cardinals. Then, it would be natural to infer the following:

$$\aleph_0 \cdot \frac{1}{\aleph_0} = 1$$

From expression (*) on page 95, it would in particular follow that $2\aleph_0 = \aleph_0$, so by ordinary algebra, we could write

$$2 \cdot \aleph_0 \frac{1}{\aleph_0} = \aleph_0 \cdot \frac{1}{\aleph_0}$$

which would entail

$$2 = 1$$

[50]Remember, we are assuming the Continuum Hypothesis, that is, $c = \aleph_1$

Obviously, we cannot accept something this absurd. Thus, our assumption of the possibility of division was wrong. We conclude that, the same as with subtraction, division is also not defined! Again, we realize that mathematics has a life of its own – we just have to discover the beautiful new world hidden under the surface.

Before concluding this section, I need to tell you about an axiom that may seem fairly obvious to you. Indeed, we have done much of our set theory tacitly assuming its validity. As a matter of fact, it has not been recognized by mathematicians for a long time. And even today, regardless of the many beautiful results one can prove with it, many mathematicians are rather skirmish about it. The discomfort that they feel is mostly due to its nonconstructive nature and some very unexpected and counterintuitive implications that follow. Let's devote a short subsection to the (in)famous Axiom of Choice.

### Axiom of Choice

In mathematics, there are arguably very few so "simple" and "self-evident" and still so controversial axioms as The Axiom of Choice (AC). As B. Russell said: *At first it seems obvious, but the more you think about it the stranger the deductions from this axiom seem to become; in the end you cease to understand what is meant by it.* Many crucial concepts in different branches of mathematics, as well as the (proofs of) theorems therein, are based on it. However, do note that I put "simple" and "self-evident" in quotation marks. Being "simple" and "self-evident" can be misleading indeed! For instance, on page 46, after introducing the Cartesian product, we asked whether one could extend the conclusion (evidently valid for finite sets) to infinite ones (see Example 1.64) as well. Similarly, when discussing the Continuum Hypothesis, we have encountered the sequence of alephs

$$\aleph_0, \aleph_1, \aleph_2, \aleph_3, \ \dots \ , \aleph_\omega, \ \dots$$

and we ask: Suppose an infinite set of infinite sets is given, *is it possible to choose one element from each set without giving a* ***rule of choice*** *in advance?*

It turns out that the issues involved are very profound and we will end this chapter with just a rudimentary exposition of the subject.

A very well-known and witty formulation of this question, which I like to call "*On Socks and Shoes,*" is due to (who else but) Bertrand Russell who said: Suppose there are infinitely many pairs of socks and shoes. To choose one sock from each pair of identical socks requires the Axiom of Choice, but for shoes the Axiom is not needed, it suffices to simply impose a rule "always chose the left shoe" and we are done. Once again, the phrase "*infinitely many*" is crucial, for with finite sets of socks we wouldn't have the problem. (Can you figure out why?) Let's start with a few simpler examples.

**Example 1.118** Consider a set $S = \{A, B, C\}$, where $A, B$, and $C$ are disjoint sets such that

$$A = \{a_1, a_2\}, B = \{b_1, b_2\}, \text{ and } C = \{c_1, c_2\}$$

Suppose we want to construct a set $\mathcal{A}$ by choosing for its elements one and only one element from each of the sets $A, B, C$. For instance, one possible "*choice set*" could be

$$\mathcal{A} = \{a_1, b_1, c_1\}$$

where the "*choice function*" was: "*take the 'first' element from each set*" (whatever "*the first*" means – in this case, obviously, an element with index 1). ■

However, how would you do

**Example/Exercise 1.119**

(i) If $\varnothing \in S$ what would be the choice set?
(ii) If $S = \varnothing$ what would be the choice set?

**Example 1.120** Let

$$S = \{A | A \subseteq \mathbf{N}, A \neq \varnothing\}$$

be a collection of all nonempty subsets of $\mathbf{N}$, then we can simply define the "choice function" by saying $f(A) =$ smallest member of $A$. ■

**Example 1.121** Let

$$S = \{I = [a, b] | a, b \in \mathbf{R}, d(a, b) < \infty\}$$

that is, a collection of all intervals of real numbers with finite length. Then, we can define $f(I)$ to be the midpoint of the interval $I$. ■

Now comes a problem: Consider Example 1.118, again assuming this time that the sets $A, B, C \in S$ are open intervals, that is

$$A = (a, b), B = (c, d) \quad \text{and} \quad C = (e, f); \quad a, b, c, d, e, f \in \mathbf{R}$$

How would you choose an element from each of the sets to construct the set $\mathcal{A}$? (Say, you first consider our familiar interval $(0, 1)$, how would you take the least element from it?) To make it even more intriguing, take the set $S$ to be the set of all nonempty subsets of $\mathbf{R}$. How would we find a suitable function $f$ to collect an element from all of those subsets? So we ask: If an infinite set of infinite sets is given, is it possible to choose one element from each set without giving the rule of choice in advance? Yes, it is possible, said Zermelo.[51] In 1904, he introduced the

[51] Ernst Zermelo (1871–1953), German mathematician.

**Axiom of Choice (AC)**

Let $S$ be a collection of mutually disjoint nonempty sets; then, there exists a set $\mathcal{A}$ consisting of exactly one member chosen from each set in the collection $S$. In other words, given any family of nonempty sets,

$$S = \{A_i | i \in I, I = \text{index set}\}$$

there exists a function – the choice function

$$f : I \to \underset{i \in I}{\cup} A_i$$

such that $f(i) = a_i \in A_i$.

Equivalently, we can approach AC as follows:

Let $S = \cup_{i \in I} A_i$ be a nonempty family of nonempty sets. Then, the Cartesian product $\prod_{i \in I} A_i$ of the sets $A_i$ is the set of all choice functions $f : I \to \cup_{i \in I} A_i$ where $f(i) = a_i \in A_i$, for all $i \in I$. In other words, for every $i \in I$, $f$ chooses a point $a_i$ from each set $A_i$.

Hence, we can restate the Axiom of Choice as follows: The Cartesian product of a nonempty family of nonempty sets is nonempty.

Note that the axiom only claims the existence of the choice function. It doesn't say anything about its construction.

As an example, let's prove

**Theorem 1.62** Every infinite set has a countably infinite subset.

***Proof*** Let $S$ be an infinite set. Consider a set $A_1 = S \backslash \{a_1\}$, where $a_1 \in S$. $A_1$ is certainly not empty since $S$ is not empty. Furthermore, $A_1$ is infinite, for if $A_1$ were finite $S$ would be finite too, contradicting our original assumption. Next, we can consider a set.

$A_2 = A_1 \backslash \{a_2\} = S \backslash \{a_1, a_2\}$, $a_2 \in S$. $A_2$ is also infinite, and in particular it contains an element $a_3$. Can we continue these arguments ad infinitum? Well, to continue with this argumentation we need AC, and we construct $A_i$ for any $1 \leq i \leq n, i \in \mathbf{N}$ according to the aforementioned prescription. We claim that $A_i$ is infinite. But then, there is $a_{n+1} \in A_n$, such that $A_{n+1} = A_n \backslash \{a_{n+1}\}$ is also infinite. Note that if $i < j$, then $a_i \in A_{i+1}$, but $a_j \notin A_{i+1}$. Now, if we let $B = \{a_i | i \in \mathbf{N}\}$, then $B$ is infinite and $|B| = |\mathbf{N}|$. ■

Going back to our list of cardinals, it is reasonable to ask: Can we form a set $C$ of all cardinal numbers? Well, let's try that. Suppose $C$ is a set of all cardinals. Then, for every $c \in C$, there exists a set $A_c$ such that $c = |A_c|$. Furthermore, let

$$A = \underset{c \in G}{\cup} A_c$$

Consider now $\mathcal{P}(A)$ and let $|\mathcal{P}(A)| = \alpha$. Then, since

$$|\mathcal{P}(A)| = \alpha$$

we have

$$|\mathcal{P}(A)| \leq |A|$$

On the other hand, by Cantor's theorem

$$|\mathcal{P}(A)| > |A|$$

so we have a contradiction. We see that, the same as with the ordinals, the axioms of set theory fail to accommodate the cardinals also.

Finally, without proof, we list three crucial theorems of mathematics:

**Theorem 1.63 (Zorn lemma)** Let $X$ be a nonempty partially ordered set, whose every linearly ordered subset has an upper bound in $X$. Then $X$ contains at least one maximal element.

**Theorem 1.64 (Zermelo's well-ordering theorem)** Every nonempty set $X$ can be well ordered.

**Theorem 1.65** The following are equivalent:

(i) Axiom of choice
(ii) Zorn lemma
(iii) Well-ordering theorem.

It might be appropriate to conclude this subsection with a quote you may philosophically disagree with but, nevertheless, you have to admit it is rather captivating:

> *… For me, and I suppose for most mathematicians, there is another reality, which I will call "mathematical reality" … I believe that mathematical reality lies outside us, that our function is to discover or observe it, and that the theorems which we prove, and which we describe grandiloquently as our "creations" are simply our notes of our observations.*[52]

## 1.10 THE SET R – REAL NUMBERS II

So far, we have dealt with real numbers more or less heuristically. We assumed their existence for a simple reason: set **Q** obviously was not sufficiently rich

[52]Hardy, G. H., *A Mathematician's Apology,* Cambridge University Press, 1967.

enough to accommodate everything we wanted to do mathematically. Also, as the reader is obviously aware of by now, the importance of set **R**, and therefore its proper definition, can hardly be overstated. We need to introduce a few more concepts in order to adequately address real numbers.

**Definition 1.45 (A ring)** A **ring** is a set $R$ with two binary operations on it: "+" and "·" called "addition" and "multiplication,"[53] respectively, such that

1. addition is commutative: $a + b = b + a, \quad \forall a, b \in R$;
2. addition is associative: $a + (b + c) = (a + b) + c, \quad \forall a, b, c \in R$;
3. addition has a neutral element with respect to addition: $\exists\, 0 \in X, \quad$ s.t. $a + 0 = 0 + a = a$,
4. addition has an inverse: $\forall a \in R, \exists(-a) \in R, \quad$ s.t. $a + (-a) = (-a) + a = 0$;
5. multiplication is associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad \forall a, b, c \in R$;
6. multiplication is distributive with respect to addition:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad \forall a, b, c \in R$$

**Definition 1.46 (A field)** A **field** $\Phi$ is a set with two binary operations on it, such that $\Phi$ ***is a commutative ring with the identity with respect to "multiplication,"*** that is, in addition to (1)–(6) from Definition 1.44, there are three more properties that have to be satisfied:

1. $a \cdot b = b \cdot a, \quad \forall a, b \in \Phi$
2. There exists a unique element $1 \in \Phi$, which we call the **identity** (sometimes unity) with respect to multiplication, s.t. $1 \cdot a = a \cdot 1 = a, \quad \forall a \in \Phi$, and
3. for every element $a \in \Phi$, there exists a **multiplicative inverse** $a^{-1} \in \Phi$, s.t.

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

**Example 1.122** The sets $Z$, $Q$, and $R$, with the usual addition and multiplication, are rings. $Q$ and $R$ are also fields. ■

**Example/Exercise 1.123** Convince yourself that the set **R** is a field.

**Example 1.124** The set $2\mathbf{Z}$ of even integers with the usual addition and multiplication is a ring. Note that it doesn't have an identity with respect to multiplication. ■

**Example 1.125** I hope that you are familiar with the concept of a polynomial of $n$ th degree in one variable, that is, a function of the form

[53] "Addition" and "Multiplication" are names that we conveniently associate with "+" and "·" These operations do not necessarily have to be our ordinary addition and multiplication.

$$f(x) = P_n(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

where $n, n-1, n-2, \ldots \in \mathbf{Z}^+$, that is, nonnegative integers,[54] and $a_n, a_{n-1}, \ldots a_0 \in R$. You can easily convince yourself that a set of all polynomials is a ring. On the other hand, a set of polynomials is not a field for obvious reasons: there is no multiplicative inverse that is also a polynomial. ■

**Example 1.126** If you are familiar with matrices, you can immediately recognize that the set of all square $(n \times n)$ – matrices form a noncommutative ring. ■

**Definition 1.47** We say that a field $\Phi$ is an **ordered field** if the following is satisfied:

1. If $a, b \in \Phi$, then one and only one of the following holds:

$$a < b, \quad a = b, \text{ or } a > b$$

2. If $a, b, c \in \Phi$, s.t. $a > b$, and $b > c$, then $a > c$
3. If $a, b, c \in \Phi$, and if $a > b$, then $a + c > b + c$.
4. If $a, b, c \in \Phi$ and if $a > b$, with $c > 0$, then $ac > bc$.

**Example 1.127** Prove that $a > 0$ iff $-a < 0$. ■

***Proof***

(i) If $a > 0$, then $a + (-a) > 0 + (-a) \Rightarrow 0 > -a$
(ii) If $-a < 0$, then $-a + a < 0 + a \Rightarrow 0 < a$ ■

**Example 1.128** Prove that if $a > 0$ and $b < 0$, then $a \cdot b < 0$. ■

***Proof*** Suppose $a > 0$ and $b < 0$. Then,

$$-b > 0$$

therefore,

$$a \cdot (-b) = -(a \cdot b) > 0$$

Hence,

$$a \cdot b < 0$$ ■

[54] $Z^+ = N \cup \{0\} = N^+$.

**Example/Exercise 1.129** Prove that if $a > 0$ and $b > 0$, then $a \cdot b > 0$.

**Example/Exercise 1.130** Prove that if $a \neq 0$, then $a^2 > 0$.

**Example/Exercise 1.131** Prove that if $a < 0$ and $b < 0$, then $a \cdot b > 0$.

Now, we are ready for some important definitions that will safely lead us to a better insight into real numbers.

**Definition 1.48** Let $\Phi$ be an ordered field, and let $A$ be a nonempty subset of $\Phi$. We say that $A$ is **bounded above**, if there exists an element $a \in \Phi$, such that $x \leq a, \ \ \forall x \in A$. We call $a$ an **upper bound** of $A$.

Similarly, we say that $A$ is **bounded below**, if there exists a $b \in \Phi$, such that $x \geq b, \ \ \forall x \in A$. We call $b$ a **lower bound** of $A$.

We say that $A$ is **bounded** if it is bounded above and below.

**Definition 1.49** Let $A$ be a nonempty subset of $\Phi$. We say that $a \in \Phi$ is the **least upper bound or a *supremum*** of $A$ iff $a$ is an upper bound of $A$, and for every other upper bound $x$ of $A$, $a \leq x$. We write $a = \sup A$.

**Definition 1.50** Let $A$ be a nonempty subset of $\Phi$. We say that $b \in \Phi$ is the **greatest lower bound or *infimum*** of $A$ iff $b$ is a lower bound of $A$, and for every other lower bound $x$ of $A$, $b \geq x$. We write $b = \inf A$.

**Definition 1.51** A field $\Phi$ is said to be **completely ordered** if the **completeness property** is satisfied, that is, if every nonempty bounded set $S \subseteq \Phi$ has a supremum in the field.

**Theorem 1.66** If a nonempty set $A$ has a supremum, then $\sup A$ is unique.

***Proof*** Suppose there are two elements $x_1$ and $x_2$, both supremums of a set $A$. By definition, both $x_1$ and $x_2$ are upper bounds of $A$, and since $x_1$ is a supremum, $x_1$ is less or equal to any other upper bound, in particular, $x_1 \leq x_2$. On the other hand, $x_2$, being a supremum, is less or equal to any other upper bound, in particular, $x_2 \leq x_1$. Hence $x_1 = x_2$. ■

Now you should be able to prove

**Theorem 1.67** If a nonempty set $A$ has an infimum, then $\inf A$ is unique.

Finally, we have

**Definition 1.52** The set of real numbers **R** is a completely ordered field.

As an additional exercise you may want to revisit Theorems 1.66 and 1.67 and simply replace the words "nonempty set $A$" by "nonempty subset $A$ of $R$."

Let's pause for a moment and reflect on all of this. Suppose we are familiar only with rational numbers and take a subset of all rational numbers such that $(p/q)^2 < 2$. This subset does not have a supremum, because if it did have a supremum, say $a$, we could eventually get $a^2 = 2$. But we have proved (see Theorem 1.45) that this is impossible. So, indeed, we want a set of numbers, call it $\mathbf{R}$, with a property that any nonempty subset $A \subseteq R$, which is bounded above, has a supremum. Well, said Dedekind,[55] suppose we knew only the infinite set $\mathbf{Q}$. Here is what we could do. Let's partition – *cut* – set $\mathbf{Q}$ into two subsets $L$ and $R$, such that (1) every element of $L$ is smaller than every element of $R$, and (2) $R$ has no least element. The idea being that every rational number is either an element of $L$ or an element of $R$. Thus, we have

$$L = \{x \in \mathbf{Q} | x < r\} \quad \text{and} \quad R = \{x \in \mathbf{Q} | x > r\}$$

For instance, our (in)famous $\sqrt{2}$ would be represented by the cut $[L, R]$ such that

$$L = \left\{ \frac{p}{q} \middle| \left(\frac{p}{q}\right)^2 < 2, \;\; p, q \in \mathbf{Z} \right\}$$

and

$$R = \left\{ \frac{p}{q} \middle| \left(\frac{p}{q}\right)^2 > 2, p, q \in \mathbf{Z} \right\}$$

It may be worth mentioning at this point that in 1872, when Dedekind introduced his "cut," topology did not exist. Today's treatment of the "Dedekind cut," as a topological space in open interval topology, had to wait for better times. Dedekind's idea still holds today: real numbers cannot be represented in terms of discrete mathematical objects. The only way to consistently represent arbitrary real numbers is by infinite sets. (Remember the statement of Cantorism at the beginning of this chapter: *Everything is a set*.)

We conclude this discussion with

**Definition 1.53** A real number is a pair $[R, L]$ of infinite sets.

For the sake of completeness, let's put together everything we have said about the field of real numbers and state it explicitly: Let $\mathbf{R}$ be a set with two binary operations on it, called **addition, "+,"** and **multiplication, "·."** These operations satisfy the following properties:

[55] Richard Dedekind (1831–1916).

1. $\forall a, b \in \mathbf{R},\ \ a + b = b + a \in \mathbf{R}$
2. $\forall a, b \in \mathbf{R},\ \ a \cdot b = b \cdot a \in \mathbf{R}$
3. $\forall a, b, c \in \mathbf{R},\ \ a + (b + c) = (a + b) + c$
4. $\forall a, b, c \in \mathbf{R},\ \ a \cdot (b \cdot c) = (a \cdot b) \cdot c$
5. $\forall a, b, c \in \mathbf{R},\ \ a \cdot (b + c) = a \cdot b + a \cdot c$
6. $\exists\, 0 \in \mathbf{R},$ s.t. $0 + a = a + 0 = a,\ \ \forall a \in \mathbf{R}$
7. $\exists\, 1 \in \mathbf{R},$ s.t. $1 \cdot a = a \cdot 1 = a,\ \ \forall a \in \mathbf{R}$
8. $\forall a \in \mathbf{R},\ \ \exists(-a) \in \mathbf{R},$ s.t. $a + (-a) = (-a) + a = 0$
9. $\forall a \in \mathbf{R},\ \ \exists a^{-1} \in \mathbf{R},$ s.t. $a \cdot a^{-1} = a^{-1} \cdot a = 1$

We call the field **R** the field of real numbers. Consequently, we have a theorem that summarizes the most important algebraic properties of the field **R**.

**Theorem 1.68** For any real numbers $a, b, c, d \in \mathbf{R}$, the following holds:

(i) *Cancellation Law for Addition*: If $a + b = a + c$, then $b = c$

(ii) *Possibility of Subtraction*: Given $a$ and $b$, there is exactly one $x$ such that

$$a + x = b$$

(iii) $a - b = a + (-b)$

(iv) $a \cdot (b - c) = a \cdot b - a \cdot c$

(v) $0 \cdot a = a \cdot 0 = 0$

(vi) *Cancellation Law for Multiplication*: If $ab = ac$ and $a \neq 0$, then $b = c$

(vii) If $b \neq 0$, then $a/b = ab^{-1}$

(viii) If $a \neq 0$, then $(a^{-1})^{-1} = a$

(ix) *Zero Product Property:* If $a \cdot b = 0$, then $a = 0$ or $b = 0$

(x) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

(xi) $(-a) \cdot (-b) = a \cdot b$

(xii) *Rule of addition of fractions:*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad b \neq 0,\ \ d \neq 0$$

(xiii) *Rule of multiplication of fractions:*

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}, \quad b \neq 0,\ \ d \neq 0$$

(xiv) *Rule of division of Fractions:*

$$\frac{a/b}{c/d} = \frac{a \cdot d}{b \cdot c}, \quad b \neq 0,\ c \neq 0,\ d \neq 0$$

(xv) *Trichotomy Law:* Given any two real numbers $a, b$, only one of the three relations holds:

$$a < b, b < a, \text{ or } a = b$$

(xvi) *Transitive Law*: If $a < b$ and $b < c$, then $a < c$

(xvii) If $a < b$, then $a + b < b + c$

(xviii) If $a < b$ and $c > 0$, then $ac < bc$

(xix) If $a \neq 0$, then $a^2 > 0$

We have already proved many of the statements in the aforementioned theorem in a different context. The reader shouldn't have any problems proving the remaining parts.

**Definition 1.54** Suppose $a \in \mathbf{R}$, we define the **absolute value of** $a$ by

$$|a| = \begin{cases} a & \text{if} \quad a \geq 0 \\ -a & \text{if} \quad a < 0 \end{cases}$$

**Theorem 1.69**

(i) For any $a, b \in \mathbf{R}$, $|ab| = |a||b|$.

(ii) For any $a, b \in \mathbf{R}$, $|a + b| \leq |a| + |b|$ (*Triangle inequality*).

***Proof***

(i) Suppose $a > 0$ and $b > 0$. Then, by definition, $|a| = a$ and $|b| = b$. Thus, $|a||b| = ab$. On the other hand, $|ab| = ab$. We conclude that $|ab| = |a||b|$. If $a < 0$ and $b < 0$, then $|a| = -a$ and $|b| = -b$, so we again have

$$|ab| = ab = (-a)(-b) = |a||b|$$

(ii) Consider the following obvious inequalities:

$$-|a| \leq a \leq |a| \tag{1.14}$$

$$-|b| \leq b \leq |b| \tag{1.15}$$

Adding (1.14) and (1.15), we get

$$-(|a| + |b|) \leq a + b \leq |a| + |b|$$

which implies

$$|a + b| \leq |a| + |b|$$

■

**Example/Exercise 1.132** Prove that

$$\left|\frac{a}{b}\right| = \frac{|a|}{|b|}, \quad b \neq 0$$

## 1.11 SUPPLEMENTARY PROBLEMS

**1.** Given four sets $A = \{a, b, c, d\}, B = \{a, a, c, b, d, d\}, C = \{d, b, a, c, 0\}$, and $D = \{d, b, a, c\}$, determine which sets are equal.

**2.** Is $a = \{a\}$? Why? Why not?

**3.** Is $0 = \{\}$? Why? Why not?

**4.** Let $A = \{a, b, c\{a\}, \{\{a\}\}, \{a, d\}, d\}$
(i) Is $a \in A$?
(ii) Is $\{a\} \subseteq A$?
(iii) Is $\{\{a\}\} \in A$?
(iv) Is $\{\{a\}\} \subseteq A$?
(v) Is $\{a, b, c\} \subseteq A$?

**5.** Let $\mathcal{U} = \{a, b, c, d, e, f, g\}$ be a universal set, and let $A = \{b, c, d, f\}$, $B = \{a, b, c\}$, and $C = \{d, e, f, g\}$. Find
(i) $A \cap B$
(ii) $A \cup B$
(iii) $A \cap C$
(iv) $B \backslash A$
(v) $A \backslash (B \cap C)$

**6.** Let $A$ be a set. Show that
(i) $A \cup \varnothing = A$
(ii) $A \cap \varnothing = \varnothing$
(iii) $A \cup A = A$
(iv) $A \cap A = A$
(v) $A \backslash \varnothing = A$

**7.** Let the universal set be the set of all natural numbers, that is, let $\mathcal{U} = N$ and $A = \{x | x = 2n, n \in \mathbf{N}\}$, find
(i) $A \cap \mathbf{N}$
(ii) $A \cup \mathbf{N}$
(iii) $A^c$

**8.** Let the universal set $\mathcal{U}$ be the set of all real numbers $\mathbf{R}$, and let $A = \{x \in \mathbf{R} | 0 \leq x \leq 1\}$, and $B = \{x \in \mathbf{R} | -3 < x \leq 3\}$. **Find**

(i) $A \cup B$

(ii) $A \cap B$

(iii) $A^c$

(iv) $B^c$

(v) $(A \cap B)^c$

**9.** What is the cardinality of each of the following sets?

(i) $\{a\}$

(ii) $\{\{a\}\}$

(iii) $\{\varnothing\}$

(iv) $\{\varnothing, \{\varnothing\}\}$

(v) $\{a, \{\{\varnothing\}\}\}$

**10.** Show that for all sets $A, B,$ and $C$

(i) If $A \subseteq B$ and $A \subseteq C$ then $A \subseteq B \cap C$

(ii) If $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$

**11.** Show that if $A \subseteq B$, then $B = A \cup (B \backslash A)$.

**12.** Show that for all sets $A, B,$ and $C$

$$(A \cup B) \backslash C = (A \backslash C) \cup (B \backslash C)$$

**13.** Show that for any sets $A$ and $B$

$$A \backslash B = A \backslash (A \cap B)$$

**14.** Let $A \subseteq C$ and $B \subseteq C$. Prove the following assertions:

(i) $C \backslash (C \backslash A) = A$

(ii) $C \backslash (A \cap B) = (C \backslash A) \cup (C \backslash B)$

(iii) $C \backslash (A \cup B) = (C \backslash A) \cap (C \backslash B)$

**15.** Show that for all sets $A, B,$ and $C$

$$(A \backslash B) \backslash C = (A \backslash C) \backslash (B \backslash C)$$

**16.** Prove: $(A \cup B) \cap B^c = A$ iff $A \cap B = \varnothing$.

**17.** Let $A$ and $B$ be subsets of $X$. Prove that

$$(A \subseteq B) \Leftrightarrow [(x\backslash B) \subseteq (x\backslash A)]$$

**18.** Show that (i) and (ii) are logically equivalent:
(i) $A$ and $B$ are disjoint sets.
(ii) $A \subseteq \mathcal{U}\backslash B, \quad B \subseteq \mathcal{U}\backslash A$.

**19.** Show that for all $A \neq B \neq \emptyset, \quad A \times B \neq B \times A$.

**20.** Prove that for all sets $A, B, C,$ and $D$

$$(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$$

**21.** Suppose $A = \{a, b\}$ and $B = \{c, b\}$. Find
(i) $\mathcal{P}(A \cap B)$
(ii) $\mathcal{P}(A \cup B)$

**22.** Let $A, B \subseteq \mathcal{U}$. Show that

$$(A \cup B) \cap (A^c \cup B^c) = A \Delta B$$

**23.** Let $A, B \subseteq \mathcal{U}$. Show that
(i) $A \Delta B = (A \cup B)\backslash(A \cap B)$
(ii) $A \Delta (B \Delta C) = (A \Delta B) \Delta C$

**24.** Show that for all sets $A, B,$ and $C$
(i) $(A \cap B) \times C = (A \times C) \cap (B \times C)$
(ii) $(A \cup B) \times C = (A \times C) \cup (B \times C)$

**25.** Show that for all sets, $B$ and $C$

$$(A\backslash B) \times C = (A \times C)\backslash(B \times C)$$

**26.** Verify that Definition 1.23 is a good definition, that is, prove that if $X$ is an infinitely countable set, then it has a proper subset with the same cardinality.

**27.** Which of the following is true:
(i) $\mathbf{N} \subseteq \mathbf{Z}$
(ii) $\mathbf{Q} \subseteq \mathbf{Z}$

(iii) $\mathbf{R} \cap \mathbf{Q} = \mathbf{Q}$
(iv) $\mathbf{Z} \cup \mathbf{Q} = \mathbf{Q}$
(v) $\mathbf{Q} \cap \mathbf{Z} \cap \mathbf{N} = \mathbf{N}$

**28.** Prove that if $X \subseteq \mathbf{N}$, then $X$ is either countably infinite or finite.

**29.** Prove that if
(a) $X$ is countable and $Y \subseteq X$ is finite, then $X \backslash Y$ is countable.
(b) $X$ is uncountable and $Y \subseteq X$ is countable, then $X \backslash Y$ is uncountable.

**30.** Prove that $A = [0, 1]$ and $B = [0, 2]$ have the same number of elements.

**31.** Prove that $A = (0, 1)$ and $B = (0, 2)$ have the same number of elements.

**32.** Determine the cardinality of the following sets:
(i) $\mathbf{N} \cap [1, \pi]$
(ii) $\mathbf{N} \cup [1, \pi]$

**33.** Determine the cardinality of the following sets:
(i) $\mathbf{Q}^3$
(ii) $\mathbf{Q}^{\mathbf{R}}$

**34.** Define $\mathbf{N}^k = \underbrace{\mathbf{N} \cdot \mathbf{N} \cdot \cdots \cdot \mathbf{N}}_{k \text{ times}}$. Prove that $\mathbf{N}^3 \sim \mathbf{N}$ that is $|\mathbf{N}^3| = |\mathbf{N}|$

**35.** Let $S_n$ be the set of all subsets of $\mathbf{N}$ whose size is $n$. Prove that $S_n$ is countable for all $n \in \mathbf{N}$.

**36.** Show that $Q \cap [0, 1]$ is countable.

**37.** Show that $(\mathbf{R} \backslash \mathbf{Q}) \sim \mathbf{R}$.

**38.** Show that for all $n = \mathbf{N}$, $|\mathbf{R}^n| = c$.

**39.** Determine the cardinality of the following sets:
(i) $\mathcal{P}(\mathbf{Z}) \times \mathcal{P}(\mathbf{Z})$
(ii) $\mathcal{P}(\mathcal{P}(\mathbf{Z}))$

**40.** Prove that if $A \neq \varnothing$ is a finite set and if $B = \{f | f : \mathbf{N} \to A\}$, then $B$ is uncountable. (Hint: recall Cantor's proof for the uncountability of the set $(0, 1)$.)

**41.** Let $(A \to B) = \{f | f : A \to B\}$
Show that if $|A_1| = |A_2|$ and $|B_1| = |B_2|$, then

$$|(A_1 \to B_1)| = |(A_2 \to B_2)|$$

**42.** Prove that the countable union of sets of cardinality $\mathbf{c} = 2^{\aleph_0}$ (continuum) again has cardinality $\mathbf{c}$.

**43.** Here is Cantor's Paradox: Consider the set of all sets. The set of all its subsets, according to Cantor's own theorem, has a cardinal number larger than the cardinal number of the original set. Yet our original set by definition includes **all** sets. Thus, we constructed a set larger than the set of all sets. Can you resolve this paradox?

**44.** Here again is Russell's famous paradox: Let $S$ be the set that contains a set $X$. If the set $X$ doesn't belong to itself, so $S = \{X | X \notin X\}$,
Show that

(i) the assumption that $S$ is a member of $S$ leads to a contradiction;

(ii) the assumption that $S$ is not a member of $S$ leads to a contradiction too.

**45.** Explain why there are no "holes" in **R.**