My Mathematics Notes

Analysis I

Phædrus

Logic, Set, $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$

By A Student from the Australian National University, Canberra • Updated: November 25, 2017

Preface

- This note aims to build a relative rigorous system of mathematics. Therefore, in order to avoid circularity, any concept will not be used unless have been defined. However, sometimes those ideas will be used as an example to introduce some definitions intuitively.

Aims of this Note

- Define the natural numbers
- Define the decimal system
- Learn a skill: proving complicated properties from simpler ones.
- Learn a skill: using mathematical induction to prove statements.
- Prove rules of algebra from more primitive, fundamental properties of the number system.
- Avoid circularity[1]
- Realize that even though a statement may be ‘obvious’, it may not be easy to prove.

[1] Using an advanced fact to prove a more elementary fact, and then use the elementary fact to prove the advanced fact.

Several Useful Notes

Axiom

An **axiom** is a statment that is taken to be true, to serve as a premise or starting point for further reasoning and arguments.

Lemma, Proposition, Theorem & Corollary

From a logical point, there is no difference between a lemma, proposition, theorem or corollary — they are all claims waiting to be proved. However, we use these term to suggest different level of importance and difficulty:

- A **lemma** is an easily proved claim which is helpful for proving other propositions and theorems, but is usually not particular interesting in its own right.
- A **proposition** is a statement which is interesting in its own right.
- A **theorem** is a more important statement than a proposition which says something definitive on the subject, and often takes more effort to prove than a proposition or lemma.
- A **corollary** is a quick consequence of a proposition ot theorem that was proven recently. is a quick consequence of a proposition ot theorem that was proven recently.

Symbols Used in This Note

Throughout this note, we apply the following symbols for particular usage:

- ☡
  We use **Bourbaki Dangerous Bend Symbol** to highlight all the conterexamples in this note. In few rare cases, this sign is also used when something must be understand extremely carefully.
- □
  We use **Halmos** to denote the end of a proof.

Contents

Chapter 1

The Basics of Mathematical Logic

1.1 Mathematical statements

Under Construction.

1.2 Implication

Under Construction.

1.3 The structure of proofs

Under Construction.

1.4 Variables and quantifiers

Under Construction.

1.5 Nested quantifiers

Under Construction.

1.6 Some example of proofs and quantifiers

Under Construction.

1.7 Equality

Equality is the most important relation linking two objects, so it is worth talking about it. Equality is a relation linking two objects x, y of the same type T. Given two such objects x, y, the statement $x = y$ may or may not be true; it depends on the value of x and y and also on how equality is defined for the class of objects under consideration.

For example, we can say that $12 = 2$ if we define that numbers are considered equal when their remainders are equal of value modulo 10.

However, no matter how equality are defined, for the purposes of logic we require that equality obeys the following four axioms of equality.

- (Reflexive Axiom) Given any object x, we have $x = x$.
- (Symmetry Axiom) Given any two objects x and y of the same type, if $x = y$, then $y = x$.

- (Transitive Axiom) Given any three objects x, y, z of the same type, if $x = y$ and $y = z$, then $x = z$
- (Substitution Axiom) Given any two objects x and y of the same type, if $x = y$, then $f(x) = f(y)$ for all functions of operations f. Similarly, for any property $P(x)$ depending on x, if $x = y$, then $P(x)$ and $P(y)$ are equivalent statement.

We now give some examples on Substitution Axiom.

Example 1.7.1 Let x and y be real numbers. If $x = y$, then $2x = 2y$, and $\sin(x) = \sin(y)$. Furthermore, $x + z = y + z$ for any real number z.

Example 1.7.2 Let n and m be integers. If n is odd and $n = m$, then m must also be odd. If we have a third integer k, and we know that $n > k$ and $n = m$, then we also know that $m > k$

Example 1.7.3 Let x, y, z be real numbers. If we know that $x = \sin(y)$ and $y = z^2$, then we have $\sin(y) = \sin(z^2)$, and hence we have $x = sin(z^2)$.

Example 1.7.4 Let a, b, c, d be four real numbers and $a = b$, $c = d$. We have $a + d = b + c$.

So if one day we decided to modify the concept of equality so that $12 = 2$, we have to make sure that $f(12) = f(2)$ for any function and operation f. For instance, $2 + 5 = 12 + 5$ where $f(x) = x + 5$.

Chapter 2

Set Theory

Before talking about sets, it worth answering a question why almost every book on mathematics begins with set theory. Modern mathematics is a subject that can be processed by 'hypothetical computers' which can prove any known propositions from the axioms and definitions. However, 'hypothetical computers' are not like human who are sensitive and intuitional; each step of this machine only depends on the primitive condition. For example, if we want this computer to do calculations, at least we hould first teach it what are numbers and operations. Similarly, every time when we are trying to define some new concept, we always define it based on the definitions we already have. Then how should we define the first conecpt in mathematics—sets? Well, before defining sets we know nothing. Therefore, set is the only one concept that cannot be defined in mathematics in a *satisfied* way. But there is still a thing we can do; we can introduce everal axioms to restrict the concept of set. This process is called the axiomatization of sets.

2.1 Fundamentals

Just as what we did to the natural numbers, in this section we set out some axioms for sets. We first give some informal description of what a set should be.

Definition 2.1.1 (Informal) We define a set A to be any unordered collection of objects, e.g., $\{3, 8, 5, 2\}$ is a set. If x is an object, we say that x is an element of A or $x \in A$ if x lies in the collection; otherwise we say that $x \notin A$. For instance, $3 \in \{1, 2, 3, 4, 5\}$ but $7 \notin \{1, 2, 3, 4, 5\}$.

This definition is intuitive enough, but it doesn't answer a number of questions, such as which collections of objects are considered to be sets, which sets are equal to other sets, and how one defines operations on sets. Also, we have no axioms telling us what sets do, or what their elements do.
We first clarify one point: we consider sets themselves to be type of object.

Axiom 2.1 (Sets are objects) If A is a set, then A also an object. In particular, given two sets A and B, it is meaningful to ask whether A is also an element of B.

Example 2.1.1 (Informal) The set $\{3, \{3, 4\}, 4\}$ is a set of three distinct elements, one of which happens to be a set of two elements.

Remark 2.1.1 There is a special case of set theory, called 'pure set theory', in which *all* objects are sets; for instance the numbers 0 might be identified with the empty set $\emptyset = \{\}$, the number 1 might be identified with $\{0\} = \{\{\}\}$, the number 2 might be idntified with $\{0, 1\} = \{\{\}, \{\{\}\}\}$, and so forth.
From a logical view, 'pure set theory' is a much simpler theory because we only need to deal with set and not objects; however, from a conceptical point of view it is often easier to deal with impure set theories in which some objects are not considered as sets. However, two types of theories are more or less equivalent for the purpose of doing mathematics, ad so we shall take an agnostic position as to whether all objects are sets or not.

So what we have known is that among all the objects we studied in mathematics, some of them happens to be sets; and if x is an object and A is a set, then either $x \in A$ is true of $x \in A$ is false. (If A is not a set, we leave the statement $x \in A$ undefined. For example, $3 \in 4$ is meaningless.)
Now we are going to define the equality of sets.

Definition 2.1.2 (Equality of sets) Two sets A and B are considered equal, $A = B$, iff every element of A is an element of B and vice versa. In another way, $A = B$ iff every element x of A belongs also to B, and vice versa.

Well, ince we have defined the equality, we have to verify the first three axiom for it now and the substitution axiom every time we defined a new operation to the sets.

Verify (Equality of sets is well-defined) A, B and C are both sets, then:

- (Reflexive) $A = A$.
- (Symmetric) If $A = B$ then $B = A$.
- (Transitive) If $A = B$ and $B = C$ then $A = C$.

Proof.

- $(\forall x \in A \iff x \in A) \implies A = A$
- $(A = B) \implies \forall x(x \in A \iff x \in B) \implies \forall x(x \in B \iff x \in A) \implies (B = A)$
- $(A = B) \vee (B = C) \implies \forall x[(x \in A \iff x \in B) \vee (x \in B \iff x \in C)]$
  $\implies \forall x(x \in A \iff x \in C) \implies A = C$ □

Since we have defined the notion of $\in$, therefore we have to verify its substitution axiom.

Verify If $x \in A$ and $A = B$, then $x \in B$.

Proof. $(x \in A) \wedge \forall x(x \in A \iff x \in B) \implies x \in B$ □

Then we have a good news that if an operation can bedefined only with the operation $\in$, we will not have to verify its substitution axiom.
Also, we should note carefully that we should not use the term 'the first element' or the 'last element' in a well-defined manner, because this would not respect the axiom of substitution since $\{1, 2, 3, 4\} = \{4, 3, 2, 1\}$.
Now we try to point out which object are sets and which are not. We plan to do this in the following way. We first define the empty set, and then we build more sets out of the empty set by various operation.
We begin by postulating the existence of the empty set.

Axiom 2.2 (Empty set) There exist a set $\emptyset$, known as empty set, which contains no element, *i.e.,* for every object x we have $x \notin \emptyset$.

The empty set is also dented as $\{\}$. Note that there is only one empty set:

Proposition 2.1.1 (Empty set is unique) If $\emptyset$ and $\emptyset'$ are both empty set, then $\emptyset = \emptyset'$.

Proof. Suppose for ths sake of contradiction that $\emptyset \neq \emptyset'$, then:
$\emptyset \neq \emptyset' \implies \exists x[(x \in \emptyset \wedge x \notin \emptyset) \vee (x \notin \emptyset \wedge x \in \emptyset)] \implies \exists x(x \in \emptyset \vee x \in \emptyset')$, a contradiction since $\forall x(x \notin \emptyset \wedge x \notin \emptyset')$.
Therefore, $\emptyset = \emptyset'$. □

If a set is not equal to empty set, we call it non-empty. Then we have the following statement, which is simple but worth stating.

Lemma 2.1.1 (Single choice) Let A be a non-empty set. Then there exists an object x such that $x \in A$.

Proof. Suppose for the sake of contradiction that $\forall x(x \notin A)$, then:
$\forall x(x \notin A) \implies A = \emptyset$, a contradiction since $A \neq \emptyset$. Therefore, $A \neq \emptyset \implies \exists x(x \in A)$ □

Remark 2.1.2 The above lemma shows that given any non-empty set A we are llowed to 'choose' an element x of A which demonstrates this non-emptyness. Later on we will show that given any finite number of non-empty sets, say $A_1, ..., A_n$, it is possible to choose one element $x_1, ..., x_n$ from each set $A_1, ..., A_n$: this is known as 'finite choice' However, in order to choose element form an infinite number of sets, we need an additional axiom, the axiom of choice, which we will discuss later.

Remark 2.1.3 Note that $\emptyset$ is not the same thing as the number 0; one is a set and the other is a number. However, it is true that the cardinality of the empty set is 0, which will be discussed later.

Now we have finished defining the empty set; we now going to introduce another axiom as the preparation of enriching the class of sets available.

Axiom 2.3 (Singleton sets and pair sets) If a is an object, then there exists a set $\{a\}$ whoe only element is a, *i.e.,* for every object y we have $y \in \{a\}$ iff $y = a$; we refer to $\{a\}$ as the singleton set whose element is a. Furthermore, if a and b are both objects, then there exists a set $\{a, b\}$ whose only elements are a and b; *i.e.,* for every object y, we have $y \in \{a, b\}$ iff $y = a$ or $y = b$; we refer this set as the pair set formed by a and b.

Lemma 2.1.2

- There is only one singleton set for each object a.
- Given any two objects a and b, there is only one pair set formed by a and b.
- $\{a, b\} = \{b, a\}$.
- $\{a, a\} = \{a\}$.

Proof.

- Suppose A and B are both singleton sets for a, then:
  $\forall x[(x \in A \iff x = a) \land (x \in B \iff x = a)] \implies \forall x(x \in A \iff x \in B) \implies A = B$
- Suppose A and B are both pair sets of a and b, then:
  $\forall x[(x \in A \iff x = a \lor x = b) \land (x \in B \iff x = a \lor x = b)] \implies \forall x(x \in A \iff x \in B)$
  $\implies A = B$
- $\forall x[(x \in \{a, b\} \iff x = a \lor x = b) \land (x \in \{b, a\} \iff x = b \lor x = a)]$
  $\implies \forall x(x \in \{a, b\} \iff x \in \{b, a\}) \implies \{a, b\} = \{b, a\}$
- $\forall x[(x \in \{a, a\} \iff x = a \lor x = a) \land (x \in \{a\} \iff x = a)]$
  $\implies \forall x(x \in \{a, a\} \iff x \in \{a\}) \implies \{a, a\} = \{a\}$ □

Thus, the singleton set axiom is in fact redundant, being a consequence of the pair set axiom. Conversely, the pair set axiom below (see Lemma 2.1.4). One may wonder why we don't go further and create triplet axioms, quadruplet axioms, etc.; however, there will be no need for this once we introduce the pairwise union axiom below.

Example 2.1.2 Since $\emptyset$ is a set and hence an object, so is singleton set $\{\emptyset\}$, *i.e.,* the set whose only element is $\emptyset$, is a set (and is not the same set as $\emptyset$). Similarly, the singleton set $\{\{\emptyset\}\}$ and the pair set $\{\emptyset, \{\emptyset\}\}$ are also sets. These three sets are not equal to each other.

Proof.

- $\{\emptyset\} \neq \emptyset$
  $\emptyset \in \{\emptyset\} \implies \exists x \in \{\emptyset\} \implies \{\emptyset\} \neq \emptyset$
- $\{\emptyset\} \neq \{\{\emptyset\}\}$
  $(x \in \{\emptyset\} \iff x = \emptyset) \land (x \in \{\{\emptyset\}\} \iff x = \{\emptyset\}) \land (\emptyset \neq \{\emptyset\})$
  $\implies \emptyset \in \{\emptyset\} \land \emptyset \notin \{\{\emptyset\}\}$
  $\implies \exists x(x \in \{\emptyset\} \land x \notin \{\{\emptyset\}\})$
  $\implies \{\emptyset\} \neq \{\{\emptyset\}\}$
- $\{\emptyset\} \neq \{\emptyset, \{\emptyset\}\}$
  $(x \in \{\emptyset\} \iff x = \emptyset) \land (x \in \{\emptyset, \{\emptyset\}\} \iff x = \emptyset \lor x = \{\emptyset\}) \land (\emptyset \neq \{\emptyset\})$
  $\implies (\{\emptyset\} \notin \{\emptyset\}) \land (\{\emptyset\} \in \{\emptyset, \{\emptyset\}\})$
  $\implies \exists x(x \notin \{\emptyset\} \land x \in \{\emptyset, \{\emptyset\}\})$
  $\implies \{\emptyset\} \neq \{\emptyset, \{\emptyset\}\}$

- $\{\{\emptyset\}\} \neq \{\emptyset, \{\emptyset\}\}$
  $(x \in \{\{\emptyset\}\} \iff x = \{\emptyset\}) \wedge (x \in \{\emptyset, \{\emptyset\}\} \iff x = \emptyset \vee x = \{\emptyset\}) \wedge (\emptyset \neq \{\emptyset\})$
  $\implies (\emptyset \notin \{\{\emptyset\}\}) \wedge (\emptyset \in \{\emptyset, \{\emptyset\}\})$
  $\implies \exists x(x \notin \{\{\emptyset\}\} \wedge x \in \{\emptyset, \{\emptyset\}\})$
  $\implies \{\{\emptyset\}\} \neq \{\emptyset, \{\emptyset\}\}$ □

As the above example shown, we can now create quite a few sets; however, the sets we make are still fairly small (each set that we can make consists of no more than two elements, so far). The next axiom allows us to build somewhat larger sets than before.

Axiom 2.4 (Pairwise union) Given two sets A, B, there exists a set $A \cup B$ of A and B, whose elements consists of all the elements which belong to A or B or both. In other words, for any object x,

$$x \in A \cup B \iff (x \in A \text{ or } x \in B)$$

Example 2.1.3 The set $\{1, 2\} \cup \{2, 3\}$ consists of those elements which either lie on $\{1, 2\}$ or in $\{2, 3\}$ or in both, or in other words the elements of this set are simply 1, 2, and 3. Because of this, we denote this set as $\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\}$.

Remark 2.1.4 Lemma 2.1.3 If A, B, A' are sets, and A is equal to A', then

- $A \cup B = A' \cup B$
- $B \cup A = B \cup A'$

Proof.

- $\forall x[(x \in A \cup B \iff x \in A \vee x \in B) \wedge (x \in A \iff x \in A')]$
  $\implies \forall x(x \in A \cup B \iff x \in A' \vee x \in B)$
  $\implies \forall x(x \in A \cup B \iff x \in A' \cup B)$
  $\implies A \cup B = A' \cup B$
- $\forall x[(x \in B \cup A \iff x \in B \vee x \in A) \wedge (x \in A \iff x \in A')]$
  $\implies \forall x(x \in B \cup A \iff x \in B \vee x \in A')$
  $\implies \forall x(x \in A \cup B \iff x \in B \cup A')$
  $\implies B \cup A = B \cup A'$ □

Thus the operation of union obeys the axiom of substitution, and is well-defined on sets.

We now give some basic properties of unions.

Lemma 2.1.4 If a and b are objects, then $\{a, b\} = \{a\} \cup \{b\}$. If A, B, C are sets, then the union operation is commutative (*i.e.,* $A \cup B = B \cup A$) and assiociative (*i.e.,* $(A \cup B) \cup C = A \cup (B \cup C)$). Also, we have $A \cup A = A \cup \emptyset = \emptyset \cup A = A$.

Proof.

- $\{a, b\} = \{a\} \cup \{b\}$
  $\forall x[x \in \{a, b\} \iff (x = a \vee x = b) \iff (x \in \{a\} \vee x \in \{b\})]$
  $\implies \forall x[x \in \{a, b\} \iff x \in \{a\} \cup \{b\}]$
  $\implies \{a, b\} = \{a\} \cup \{b\}$
- $A \cup B = B \cup A$
  $\forall x(x \in A \cup B \iff x \in A \vee x \in B)$
  $\implies \forall x(x \in A \cup B \iff x \in B \vee x \in A)$
  $\implies \forall x(x \in A \cup B \iff x \in B \cup A)$
  $\implies A \cup B = B \cup A$
- $(A \cup B) \cup C = A \cup (B \cup C)$ $\forall x[x \in (A \cup B) \cup C \iff x \in A \cup B \vee x \in C]$
  $\implies \forall x[x \in (A \cup B) \cup C \iff x \in A \vee x \in B \vee x \in C]$
  $\implies \forall x[x \in (A \cup B) \cup C \iff x \in A \vee x \in B \cup C]$
  $\implies \forall x[x \in (A \cup B) \cup C \iff x \in A \cup (B \cup C)]$
  $\implies (A \cup B) \cup C = A \cup (B \cup C)$

- $A \cup A = A \cup \emptyset = \emptyset \cup A = A$
  $\forall x(x \in A \cup A \iff x \in A \vee x \in A) \implies \forall x(x \in A \cup A \iff x \in A) \implies A \cup A = A$
  $\forall x(x \in A \cup \emptyset \iff x \in A \vee x \in \emptyset) \implies \forall x(x \in A \cup \emptyset \iff x \in A) \implies A \cup \emptyset = A$
  $A \cup \emptyset = \emptyset \cup A$
  Therefore, $A \cup A = A \cup \emptyset = \emptyset \cup A = A$ □

Because of this lemma we do not have to use parenthee to denote multiple unions, thus for instance we can write $A \cup B \cup C$ insted of $(A \cup B) \cup C$ or $A \cup (B \cup C)$. Similarly for union of four sets $A \cup B \cup C \cup D$, etc.

Remark 2.1.5 While the operation of union has something to do with addition, the two operationa are not identical. For instance $\{2\} \cup \{3\} = \{2, 3\}$ and $2 + 3 = 5$, whereas $\{2\} + \{3\}$ is meaningless (addition pertains to numbers, not sets) and $2 \cup 3$ is also meaningless (union pertains to sets, not numbers).

This axiom allows us to dfined triplet sets, quadruplet sets, and so forth:
If a, b, c are three objects, we define $\{a, b, c\} := \{a\} \cup \{b\} \cup \{c\}$
If a, b, c, d are four objects, we define $\{a, b, c, d\} := \{a\} \cup \{b\} \cup \{c\} \cup \{d\}$ and so forth.
On the other hand, we are not yet in a posisiton to define sets consisting of n objects for any given natural number n; this would require iterating the above construction n times, but the concept of n-fold iteration has not yet been rigorously defined. For similar reasons, we cannot yet define sets consisting of infinitely many objects, because that would require iterating the axiom of pairwise union infinitely often, and it is not clear at this stage that one can do this rigorously. Later on, we will introduce other axioms of set theory which allow one to construct arbitarily large, and even infinite, sets.
Clearly, some sets seem to be larger than others. One way to formalize this concept is through the notion of a subset.

Definition 2.1.3 (Subsets) Let A, B be sets. We say that A is subset of B, denoted $A \subseteq B$, iff every element of A is also an element of B, *i.e.,*

$$\forall x \in A \implies x \in B.$$

We say that A is a proper subset of B, denoted $A \subsetneq B$, if $A \subseteq B$ and $A \neq B$.

Remark 2.1.6 Because these definitions involve only the notions of equality and the '$\in$' relation, both of which already obey the axiom of substitution. Thus, $A \subseteq B \wedge A = A' \implies A' \subseteq B$.

Lemma 2.1.5

- $A \subseteq A$
- $\emptyset \subseteq A$

Proof.

- $(\forall x \in A \implies x \in A) \iff A \subseteq A$
- $\forall x \in \emptyset \implies (\forall x \notin A \implies x \notin \emptyset) \iff \emptyset \subseteq A$ □

Proposition 2.1.2 (Sets are partically ordered by set inclusion) Let A, B, C be sets.

- $(A \subseteq B) \wedge (B \subseteq C) \implies A \subseteq C$
- $(A \subseteq B) \wedge (B \subseteq A) \implies A = B$
- $(A \subsetneq B) \wedge (B \subsetneq C) \implies A \subsetneq C$

Proof.

- $(A \subseteq B) \wedge (B \subseteq C) \iff \forall[(x \in A \implies x \in B) \wedge (x \in B \implies x \in C)]$
  $\implies \forall x(x \in A \implies x \in C) \iff A \subseteq C$
- $(A \subseteq B) \wedge (B \subseteq A) \iff \forall[(x \in A \implies x \in B) \wedge (x \in B \implies x \in A)]$
  $\implies \forall x(x \in A \iff x \in B) \iff A = B$

- $(A \subsetneq B) \wedge (B \subsetneq C) \implies (A \subseteq B) \wedge (B \subseteq C) \wedge A \neq B$
  $\implies A \subseteq C \wedge \exists x(x \in B \wedge x \notin A) \wedge \forall x(x \in B \implies x \in C)$
  $\implies A \subseteq C \wedge \exists x(x \in C \wedge x \notin A) \implies A \subseteq C \wedge A \neq C$
  $\implies A \subsetneq C$ □

Remark 2.1.7 There is one important difference between the subset realtion $\subsetneq$ and the les than relation $<$. Given any two distinct natural numbers m, n, we know that one of them is smaller than the other; however, given two distinct sets, it is not in general true that one of them is a subset of the other. This is why we say that sets are only partically ordered, whereas the natural numbers are totally ordered.

Remark 2.1.8 We should note the difference between the subset relation $\subseteq$ and the element relation $\in$. It is important to distinguish sets from their elements, as they have different properties.
For example, it is possible to have an infinite set consisting of finite numbers like $\mathbb{N}$ which has infinity many numbers, but each number is finite; we can also have a finite set consisting of infinite objects as $\{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$, which has four elements, all of which are infinite.

We now give an axiom which easily allows us to create subsets out of larger sets.

Axiom 2.5 (Axiom of specification/Axiom of seperation) Let A be a set, and for each $x \in A$, let $P(x)$ be a property pertaining to x (*i.e.,* $P(x)$ is either a true statement or a false statement). Then there exists a set, called $\{x \in A : P(x) \text{ is true}\}$ (or simply $\{x \in A : P(x)\}$ for short), whose elements are precisely the elements x in A for which $P(x)$ is true. In other words, for any object y,

$$y \in \{x \in A : P(x)\} \iff [y \in A \wedge P(x) \text{ is true}]$$

Lemma 2.1.6

- $\{x \in A : P(x)\} \subseteq A$
- $A = A' \implies \{x \in A : P(x)\} = \{x \in A' : P(x)\}$

Proof.

- $\forall y\{y \in \{x \in A \mid P(x)\} \iff [y \in A \wedge P(y)] \implies y \in A\} \iff \{x \in A : P(x)\} \subseteq A$
- $A = A' \iff \forall y(y \in A \iff y \in A') \implies \forall y\{[y \in A \wedge P(y)] \iff [y \in A' \wedge P(y)]\}$
  $\implies \forall y[y \in \{x \in A : P(x)\} \iff y \in \{x \in A' : P(x)\}]$
  $\implies \{x \in A : P(x)\} = \{x \in A' : P(x)\}$ □

We sometimes write $\{x \in A \mid P(x)\}$ insted of $\{x \in A : P(x)\}$; this is useful when we are using the colon ':' to denote something else, for example to denote the range and domain of a function $f : X \to Y$.
We can use this axiom of specification to define some further operation on sets, namely intersections and difference sets.

Definition 2.1.4 (Intersections) The intersection $S_1 \cap S_2$ fo two sets is defined to be the set

$$S_1 \cap S_2 := \{x \in S_1 \mid x \in S_2\}.$$

In other words, $S_1 \cap S_2$ consists of all the elements which belong to both S_1 and S_2. Thus, for all object x,

$$x \in S_1 \cap S_2 \iff x \in S_1 \wedge x \in S_2.$$

Remark 2.1.9 Since this concept is defined in terms of more primitive operations which have already been proved well-defined, it obeys the Axiom of Substitution. *Similar remarks apply to future definitions in this chapter and will usually not be mentioned explicitly again.*

Remark 2.1.10 By the way, we should be careful with the English word 'and': rather confusingly, it can mean either union, intersection or addition:

- (Union) The set of boys nd girls

- (Intersection) The set of people who are single and male
- (Addition) 2 and 3 is 5

This can certainly be confusing. To solve this problem, we use mathematical logic symbols which always have precise and unambiguous meanings. However, we still must look very carefully at the context in order to work out what an English word means.

Two sets are said to be disjoint if $A \cap B = \emptyset$. Note that this is not the same concept as being distinct, $A \neq B$. For example, $\{1, 2, 3\}$ and $\{2, 3, 4\}$ are distinct but not disjoint. Meanwhile, $\emptyset$ and $\emptyset$ are disjoint but not distinct.

Definition 2.1.5 (Difference sets) Given two sets A and B, we define the set $A - B$ or $A \backslash B$ to be the set A with any elements of B removed:

$$A \backslash B := \{x \in A \mid x \notin B\}.$$

In many cases B will be a subset of A, but not necessarily.

We no give some basic properties of unions, intersections, and difference sets.

Proposition 2.1.3 (Sets from a boolean algebra) Let A, B, C be sets, and let X be a set containing A, B, C as subsets.

(*a*) (Minimal element) $A \cup \emptyset = A$; $A \cap \emptyset = \emptyset$.

(*b*) (Maximal element) $A \cup X = X$; $A \cap X = A$.

(*c*) (Identity) $A \cup A = A$; $A \cap A = A$.

(*d*) (Commutativity) $A \cup B = B \cup A$; $A \cap B = B \cap A$.

(*e*) (Associativity) $(A \cup B) \cup C = A \cup (B \cup C)$; $(A \cap B) \cap C = A \cap (B \cap C)$.

(*f*) (Distributivity) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(*g*) (Absorbtion) $A \cap (A \cup B) = A$;$A \cup (A \cap B) = A$

(*h*) (Partition) $A \cup (X \backslash A) = X$; $A \cap (X \backslash A) = \emptyset$.

(*i*) (De Morgan law) $X \backslash (A \cup B) = (X \backslash A) \cap (X \backslash B)$; $X \backslash (A \cap B) = (X \backslash A) \cup (X \backslash B)$

Remark 2.1.11 The de Morgan laws are named after the logicin Augustus De Morgan $(1861 - 1871)$, who identified them as one of the basic laws of set theory.

Proof.

(*a*) $A \cup \emptyset = A$ (Proved)
$\forall x[x \notin \emptyset \iff x \notin \emptyset \vee x \notin A \iff \neg(x \in \emptyset \wedge x \in A) \iff \neg x \in \emptyset \cap A \iff x \notin \emptyset \cap A]$
$\implies A \cap \emptyset = \emptyset$

(*b*) $\forall x[(x \in A \cup X \iff x \in A \vee x \in X) \wedge (x \in A \implies x \in X)]$
$\implies \forall x(x \in A \cup X \iff x \in X)$
$\implies A \cup X = X$
$\forall x[(x \in A \cap X \iff x \in A \wedge x \in X) \wedge (x \in A \implies x \in X)]$
$\implies \forall x(x \in A \cap X \iff x \in A)$
$\implies A \cap X = A$

(*c*) $A \cup B = B \cup A$ (Proved)
$\forall x(x \in A \iff x \in A \wedge x \in A) \implies \forall x(x \in A \iff x \in A \cap A) \implies A \cap A = A$

(*d*) $A \cup B = B \cup A$ (Proved)
$\forall x(x \in A \cap B \iff x \in A \wedge x \in B \iff x \in B \wedge x \in A \iff x \in B \cap A)$
$\implies A \cap B = B \cap A$

(*e*) $(A\cup B)\cup C = A\cup(B\cup C)$ (Proved)
$\forall x[x\in(A\cap B)\cap C \iff x\in A\cap B\wedge x\in C \iff (x\in A\wedge x\in B)\wedge x\in C$
$\iff x\in A\wedge(x\in B\wedge x\in C) \iff x\in A\wedge x\in B\cap C \iff x\in A\cap(B\cap C)]$
$\implies (A\cap B)\cap C = A\cap(B\cap C)$

(*f*) $\forall x[x\in A\cap(B\cup C) \iff x\in A\wedge x\in B\cup C \iff x\in A\wedge(x\in B\vee x\in C)$
$\iff (x\in A\wedge x\in B)\vee(x\in A\wedge x\in C) \iff x\in A\cap B\vee x\in A\cap C$
$\iff x\in(A\cap B)\cup(A\cap C)]$
$\implies A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$
$\forall x[x\in A\cup(B\cap C) \iff x\in A\vee x\in B\cap C \iff x\in A\vee(x\in B\wedge x\in C)$
$\iff (x\in A\vee x\in B)\wedge(x\in A\vee x\in C) \iff x\in A\cup B\vee x\in A\cup C$
$\iff x\in(A\cup B)\cap(A\cup C)]$
$\implies A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$

(*g*) $\forall x[x\in A\cap B \iff x\in A\wedge x\in B \implies x\in A] \implies A\cap B\subseteq A \overset{(b)}{\Longrightarrow} A\cup(A\cap B) = A$
$A\cap(A\cup B) \xlongequal{(c)} (A\cup A)\cap(A\cup B) \xlongequal{(f)} A\cup(A\cap B) = A$

(*h*) $\forall x[x\in A\cup(X\backslash A) \iff x\in A\vee x\in X\backslash A \iff (x\in A\vee x\in X)\wedge(x\in A\vee x\notin A)$
$\iff x\in A\cup X = X]$
$\implies A\cup(X\backslash A) = X$
$\forall x[x\in A\cap(X\backslash A) \iff x\in A\wedge x\in X\backslash A \iff x\in A\wedge x\in X\wedge x\notin A$
$\iff x\in\emptyset\wedge x\in X \iff x\in\emptyset\cap X = \emptyset]$
$\implies A\cap(X\backslash A) = \emptyset$

(*i*) $\forall x[x\in x\backslash(A\cup B) \iff x\in X\wedge x\notin A\cup B \iff x\in X\wedge(x\notin A\wedge x\notin B)$
$\iff (x\in X\wedge x\notin A)\wedge(x\in X\wedge x\notin B) \iff x\in X\backslash A\wedge x\in X\backslash B$
$\iff x\in(X\backslash A)\cap(X\backslash B)]$
$\implies X\backslash(A\cup B) = (X\backslash A)\cap(X\backslash B)$
$\forall x[x\in X\backslash(A\cap B) \iff x\in X\wedge x\notin A\cap B \iff x\in X\wedge(x\notin A\vee x\notin B)$
$\iff (x\in X\wedge x\notin A)\vee(x\in X\wedge x\notin B) \iff x\in X\backslash A\vee x\in X\backslash B$
$\iff x\in(X\backslash A)\cup(X\backslash B)]$
$\implies X\backslash(A\cap B) = (X\backslash A)\cup(X\backslash B)$ □

Remark 2.1.12 We can observe a certain symmetry in the above laws between $\cup$ and $\cap$, and between X and $\emptyset$. This is an example of duality — two distinct properties or objects being dual to each other. In this case, the duality is manifested by the complementation relation $A\mapsto X\backslash A$; the de Morgan laws assert that this relation converts unions into intersections and vice versa. Also, it interchanges X and $\emptyset$. The above laws are collectively known as the laws of Boolean algebra, after the mathematician George Boole (1815-1864), and are also applicable to a number of other objects other than sets; it plays a particularly important rôle in logic.

We also have several lemmae about sets.

Lemma 2.1.7 Let A, B, C and X be sets.

(*a*) $A\subseteq B \iff A\cup B = B \iff A\cap B = A$

(*b*) $A\cap B\subseteq A$ and $A\cap B\subseteq B$

(*c*) $C\subseteq A\wedge C\subseteq B \iff C\subseteq A\cap B$

(*d*) $A\subseteq A\cup B$ and $B\subseteq A\cup B$

(*e*) $A\subseteq C\wedge B\subseteq C \iff A\cup B\subseteq C$

(*f*) $A\cup B = X\wedge A\cap B = \emptyset \implies A = X\backslash B\wedge B = X\backslash A$

(*g*) $\begin{cases} (A\backslash B)\cap(B\backslash A) = \emptyset \\ (A\cap B)\cap(A\backslash B) = \emptyset \\ (A\cap B)\cap(B\backslash A) = \emptyset \end{cases}$ and $(A\backslash B)\cup(A\cap B)\cup(B\backslash A) = A\cup B$

Proof.

(*a*) $A \cup B = B \iff \forall x[x \in A \cup B \iff x \in B] \iff \forall x[x \in A \cup B \implies x \in B \land x \in A \cup B \impliedby x \in B]$
$\iff \forall x[x \in A \cup B \implies x \in B] \implies \forall x[(x \in A \lor x \in B) \implies x \in B]$
$\iff \forall x[x \in A \implies x \in B \land x \in B \implies x \in B] \iff \forall x[x \in A \implies x \in B]$
$\iff A \subseteq B$
$A \cap B = A \iff \forall x[x \in A \cap B \iff x \in A] \iff \forall x[x \in A \cap B \implies x \in A \land x \in A \cap B \impliedby x \in A]$
$\iff \forall x[x \in A \implies x \in A \cap B] \implies \forall x[x \in A \implies (x \in A \land x \in B)]$
$\iff \forall x[x \in A \implies x \in A \land x \in A \implies x \in B] \iff \forall x[x \in A \implies x \in B]$
$\iff A \subseteq B$
Therefore, $A \subseteq B \iff A \cup B = B \iff A \cap B = A$.

(*b*) $\forall x[x \in A \cap B \iff x \in A \land x \in B \implies x \in A] \implies A \cap B \subseteq A$
$\forall x[x \in A \cap B \iff x \in A \land x \in B \implies x \in B] \implies A \cap B \subseteq B$

(*c*) $C \subseteq A \land C \subseteq B \iff \forall x[x \in C \implies x \in A \land x \in C \implies x \in B]$
$\iff \forall x[x \in C \implies (x \in A \land x \in B)] \iff \forall x[x \in C \implies x \in A \cap B]$
$\iff C \subseteq A \cap B$

(*d*) $\forall x[x \in A \implies x \in A \lor x \in B] \iff \forall x[x \in A \implies x \in A \cup B] \implies A \subseteq A \cup B$
$\forall x[x \in B \implies x \in A \lor x \in B] \iff \forall x[x \in B \implies x \in A \cup B] \implies B \subseteq A \cup B$

(*e*) $A \subseteq C \land B \subseteq C \iff \forall x[x \in A \implies x \in C \land x \in B \implies x \in C]$
$\iff \forall x[(x \in A \lor x \in B) \implies x \in C] \iff \forall x[x \in A \cup B \implies x \in C]$
$\iff A \cup B \subseteq C$

(*f*) $A \cup B = X \implies \forall x[x \in X \iff (x \in A \lor x \in B)]$
$A \cap B = \emptyset \implies \forall x[(x \in A \implies x \notin B) \land (x \in B \implies x \notin A)]$
$\forall x[x \in X \backslash B \iff x \in X \land x \notin B \iff (x \in A \lor x \in B) \lor x \notin B$
$\iff (x \in A \land x \notin B) \lor (x \in B \land x \notin B) \iff x \in A \lor x \notin B \iff x \in A]$
$\implies X \backslash B = A$
$\forall x[x \in X \backslash A \iff x \in X \land x \notin A \iff (x \in A \lor x \in B) \lor x \notin A$
$\iff (x \in A \land x \notin A) \lor (x \in B \land x \notin A) \iff x \in B \lor x \notin A \iff x \in B]$
$\implies X \backslash A = B$

(*g*) Suppose for the sake of contradiction that $\begin{cases} (A \backslash B) \cap (B \backslash A) = C_1 \neq \emptyset \\ (A \cap B) \cap (A \backslash B) = C_2 \neq \emptyset \\ (A \cap B) \cap (B \backslash A) = C_3 \neq \emptyset \end{cases}$

Then:

- $\exists x \in (A \backslash B) \cap (B \backslash A) \iff \exists x[x \in A \land x \notin A \land x \in B \land x \notin B]$, a contradiction.
- $\exists x \in (A \cap B) \cap (A \backslash B) \iff \exists x[x \in A \land x \in B \land x \notin B]$, a contradiction.
- $\exists x \in (A \cap B) \cap (B \backslash A) \iff \exists x[x \in B \land x \in A \land x \notin A]$, a contradiction.

Therefore, $\begin{cases} (A \backslash B) \cap (B \backslash A) = \emptyset \\ (A \cap B) \cap (A \backslash B) = \emptyset \\ (A \cap B) \cap (B \backslash A) = \emptyset \end{cases}$

$\forall x[x \in (A \backslash B) \cup (A \cap B) \cup (B \backslash A) \iff (x \in A \land x \notin B) \lor (x \in A \land x \in B) \lor (x \in B \land x \notin A)$
$\iff [x \in A \land (x \in B \lor x \notin B)] \lor (x \in B \land x \notin A) \iff x \in A \lor (x \in B \lor x \notin A)$
$\iff (x \in A \lor x \in B) \land (x \in A \lor x \notin A) \iff x \in A \lor x \in B \iff x \in A \cup B]$
$\implies (A \backslash B) \cup (A \cap B) \cup (B \backslash A) = A \cup B$ □

It seems that we have already had enough axioms and results about sets. However, we still cannot transform each object of a set, so we have the following axiom:

Axiom 2.6 (Replacement) Let A be a set. For any object $x \in A$, and any object y, suppose we have a statement $P(x, y)$ pertaining to x and y, such that for each $x \in A$ there is at most one y for which $P(x, y)$ is true. Then there exists a set $\{y \mid x \in A, P(x, y)\}$, such that for any object z,

$$z \in \{y \mid x \in A, P(x, y)\} \iff \exists x \in A \land P(x, z).$$

Proposition 2.1.4 Axiom of Replacement implies the Axiom of Specification.

Proof. Let A be a set, and for each $x \in A$, let $P(x)$ be a property pertaining to x. Then let a statement pertaining to x and y that $Q(x, y) := P(x) \wedge x = y$.
Since $P(x)$ is either thue or false:

- If $P(x)$ is false, then $\forall y, Q(x, y)$ is false.
- If $P(x)$ is true, then $\exists! y = x, Q(x, y)$ is true.

Therefore, for each $x \in A$, at most one y for which $Q(x, y)$ is true.
Thus, according to Axiom of Replacement, $\exists B := \{y \mid x \in A, Q(x, y)\}$ such that for any object z,

$$z \in B \iff \exists x \in A \wedge Q(x, z).$$

Because:

- $z \in B \implies \exists x \in A \wedge Q(x, z) \implies \exists x \in A \wedge P(x) \wedge x = z \implies z \in A \wedge P(z)$
- $z \in A \wedge P(z) \implies \exists z \in A \wedge P(z) \implies \exists x \in A \wedge P(x) \wedge x = z \implies \exists x \in A \wedge Q(x, z) \implies x \in B$

we now have $z \in B \iff z \in A \wedge P(z)$.
Thus, we have shown that $\exists B$ such that for any object z,

$$z \in B \iff z \in A \wedge P(z),$$

where B can also be denoted as $\{x \in A \mid P(x)\}$.
Hence, Axiom of Replacement implies the Axiom of Specification. □

From here, it seems that the Axiom of Specification is not necessary. In fact, this axiom is sometimes omitted from the list of axioms in the Zermelo–Fraenkel set theory. However, why the Axiom of Specification is imoprtant is due to historical considerations which requires a detailed learning in Axiomatic Set Theory to be fully understand in further studies. In Chapter 3, we implicitly assumed in many examples that the natural numbers are actually objects. Let us formalize this as follows:

Axiom 2.7 (Infinity) There exists a set $\mathbb{N}$, whose elements are called natural numbers, as well as an object $0 \in \mathbb{N}$, and an object $n{+}{+}$ assigned to every natural number $n \in \mathbb{N}$, such that the Peano Axioms (Axioms 3.1–3.5) hold.

This is the more formal version of Assumption 3.1. It is called tha axiom of infinity[1] because it introduces the most basic example of an infinite set, namely the set of all natural numbers $\mathbb{N}$.

2.2 Rusell's paradox

We have introdcued many axioms just to define what a set is as well as what we can do to a set. This seems a bit sophisticated. However, in fact, this might be one of the few satifying ways of defining a set. Here we introduce a common incorrect way of defining a set, for it creates a logical contradiciton known as *Russell's paradox.* The axiom goes like this:

Axiom 2.8 (Universal specification/Comprehension) Suppose for every object x we have a property $P(x)$ pertaining to x so that for every x, $P(x)$ is either a true statement or a false statement. Then there exists a set $\{x \mid P(x)\}$ such that for very object y,

$$y \in \{x \mid P(x)\} \iff P(y).$$

This axiom assert that every property correponds to a set. In addition, this axiom also implies most of the axiom in the previous section.

Proposition 2.2.1 Axiom of Universal Specification implies the following axioms:

[1] We will define what finite and infinity mean in Section 2.6.

(a) **(Empty set)**
There exist a set $\emptyset$, known as empty set, which contains no element, *i.e.,* for every object x we have $x \notin \emptyset$.

(b) **(Singleton sets and pair sets)**
If a is an object, then there exists a set $\{a\}$ whoe only element is a, *i.e.,* for every object y we have $y \in \{a\}$ iff $y = a$; we refer to $\{a\}$ as the singleton set whose element is a. Furthermore, if a and b are both objects, then there exists a set $\{a, b\}$ whose only elements are a and b; *i.e.,* for every object y, we have $y \in \{a, b\}$ iff $y = a$ or $y = b$; we refer this set as the pair set formed by a and b.

(c) **(Pairwise union)**
Given two sets A, B, there exists a set $A \cup B$ of A and B, whose elements consists of all the elements which belong to A or B or both. In other words, for any object x,

$$x \in A \cup B \iff (x \in A \text{ or } x \in B)$$

(d) **(Axiom of specification/Axiom of seperation)**
Let A be a set, and for each $x \in A$, let $P(x)$ be a property pertaining to x (*i.e.,* $P(x)$ is either a true statement or a false statement). Then there exists a set, called $\{x \in A : P(x) \text{ is true}\}$ (or simply $\{x \in A : P(x)\}$ for short), whose elements are precisely the elements x in A for which $P(x)$ is true. In other words, for any object y,

$$y \in \{x \in A : P(x)\} \iff [y \in A \wedge P(x) \text{ is true}]$$

(e) **(Replacement)**
Let A be a set. For any object $x \in A$, and any object y, suppose we have a statement $P(x, y)$ pertaining to x and y, such that for each $x \in A$ there is at most one y for which $P(x, y)$ is true. Then there exists a set $\{y \mid x \in A, P(x, y)\}$, such that for any object z,

$$z \in \{y \mid x \in A, P(x, y)\} \iff \exists x \in A \wedge P(x, z).$$

If we assume that all natural numbers are objects, we can also obtain:

(f) **(Infinity)**
There exists a set $\mathbb{N}$, whose elements are called natural numbers, as well as an object $0 \in \mathbb{N}$, and an object n++ assigned to every natural number $n \in \mathbb{N}$, such that the Peano Axioms (Axioms 3.1–3.5) hold.

Proof.

(a) Let p be a statement pertaining to x, then let $P(x) := p \wedge \neg p$. Now by the Axiom of Comprehension, there exists such a set $\emptyset := \{x \mid P(x)\}$ that:

$$\forall x \in \emptyset \iff P(x) \iff p \wedge \neg p.$$

Since $\forall x\ p \wedge \neg p$ is false,

$$\forall x\ x \notin \emptyset.$$

Therefore, the Axiom of Comprehension implies the Axiom of Empty Set.

(b) Let $P(x) :=$ '$x = a$' and $Q(x) :=$ '$x = a$' $\vee$ '$x = b$'. Then by the Axiom of Comprehension there exists such two sets $\{a\} := \{x \mid P(x)\}$ and $\{a, b\} := \{x \mid Q(x)\}$ that:

$$\begin{aligned} x \in \{a\} &\iff P(x) \iff x = a \\ x \in \{a, b\} &\iff Q(x) \iff x = a \vee x = b \end{aligned}$$

Therefore, the Axiom of Comprehension implies the Axiom of Singleton Sets and the Axiom of Pair Sets.

(c) Let $P(x) := x \in A \vee x \in B$, then by the Axiom of Comprehension, there exists such a set $A \cup B := \{x \mid P(x)\}$ that:

$$x \in A \cup B \iff P(x) \iff x \in A \vee x \in B.$$

Therefore, the Axiom of Comprehension implies the Axiom of Pairwise Union.

(d) Let $P(x)$ be a property pertaining to x, then let $Q(x) := x \in A \wedge P(x)$. Then according to the Axiom of Comprehension, there exist such a set $\{x \in A \mid P(x)\} := \{x \mid Q(x)\}$ that $\forall y$:

$$y \in \{x \in A \mid P(x)\} \iff Q(y) \iff y \in A \wedge P(y).$$

Therefore, the Axiom of Comprehension implies the Axiom of Seperation.

(e) Let A be a set and $P(x, y)$ be a statement pertaining to x and y and for each $x \in A$ at most one y for which $P(x, y)$ is true. Now let $Q(y) := \exists x \in A \wedge P(x, y)$. Then according to the Axiom of Comprehension, there exists such a set $\{y \mid x \in A, P(x, y)\} := \{y \mid Q(y)\}$ that $\forall z$:

$$z \in \{y \mid x \in A, P(x, y)\} \iff Q(z) \iff \exists x \in A \wedge P(x, z).$$

Therefore, the Axiom of Comprehension implies the Axiom of Replacement.

(f) Let $P(x) :=$ '$x = 0$' $\vee\ [x = y\text{++} \wedge P(y)]$, then by the Axiom of Comprehension, there exists such a set $\mathbb{N} := \{x \mid P(x)\}$ that $\forall y$:

$$y \in \mathbb{N} \iff P(y) \iff y = 0 \vee [y = z\text{++} \wedge P(z)].$$

We now use induction to prove that all natural numbers are included in $\mathbb{N}$. In the base case where $n = 0$, $n = 0 \implies P(0) \implies 0 \in \mathbb{N}$. Now suppose inductively that $n \in \mathbb{N}$, then as to n++: $P(n) \implies P(n\text{++}) \implies n \in \mathbb{N}$. This closes the induction and hence forall natural number n, $n \in \mathbb{N}$.
Therefore, the Axiom of Comprehension implies the Axiom of Infinity. □

However, Axiom of Universal Specification is too good to be introduced into set theory. As we have said before, this axiom creates a logical contradiction discovered by the philosopher and logician Bertrand Russell (1872–1970) in 1901. The paradox runs as follows:
Let $P(x)$ be the statement:

$$P(x) \iff \text{`}x \text{ is a set, and } x \notin x\text{'};$$

i.e., $P(x)$ is true only when x is a set which does not contain itself. For example, $P(\{0\})$ is true since $\{0\}$ is a set and $\{0\} \notin \{0\}$. On the other hand, let S be the set of all sets[1], then $P(S)$ is false since S is a set but $S \in S$ because any set is an element of S. Now we use the Axiom of Universal Specification to create the set

$$\Omega := \{x \mid P(x)\} = \{x \mid x \text{ is a set} \wedge x \notin x\}$$

i.e., the set of all sets which do not contain themselves. Now here comes a question: does Ω contain itself, *i.e.,* is $\Omega \in \Omega$? Let see what will happen if $\Omega \in \Omega$ or $\Omega \notin \Omega$ is true:

- $\Omega \in \Omega \implies P(\Omega) \implies \Omega$ is a set $\wedge\ \Omega \notin \Omega \implies \Omega \notin \Omega$
- $\Omega \notin \Omega \implies \neg P(\Omega) \implies \Omega$ is not a set $\vee\ \Omega \in \Omega \implies \Omega \in \Omega$

This shows that either one of the statements is true will lead to the other statement being true, which is absurd.
The problem of this axiom is that it allows us to create sets which are so 'large' that they can contain themselves. For example, under the Axiom of Comprehension, the set of all objects contain itself since the set itself is also an object, which seems quite ridiculous from common sense.
To solve this problem, we must avoid constructing sets which contain themselves or the sets that is similar to them. Similarly, we should also prevent making sets consisting of 'larger' sets from occuring.
To realize this idea, one of the methods is to assign all objects with different levels and only allow construction higher level sets consisting of lower level object. For example, let the bottom level be all the non-sets objects named *primitive objects*. Then let $\emptyset$ and sets consisiting only of primitive objects be '*primitive sets*'. Then there are sets consisting only of primitive objects and primitive sets. After that we can form sets out of these objects and so forth. In this way, we can guarantee that we will never construct sets containing themselves.
If in the pure set theory where we have no primitive object, we can let $\emptyset$ be the only primitive set and follow the same method.
To actually formalize the above intuition is rather complicated, and we will not discuss this in detail here, but in Axiomatic Set Theory in the future. Nevertheless, we shall simply assume an axiom which ensures that Russell's Paradox do not occur.

[1] The set S exists because of the Axiom of Universal Specification.

Axiom 2.9 (Regularity/Foundation) If A is a non-empty set, then there is at least one element x of A which is either not a set, or $x \cap A = \emptyset$.

This axiom can lead the following results:

Proposition 2.2.2 If A and B are both sets, then:

- $A \notin A$.
- either $A \notin B$ or $B \notin A$ or both.

Proof.

- If $A = \emptyset$, then by the Axiom of Empty Set $\forall x\ x \notin \emptyset$. Since $\emptyset$ itself is also an object, $\emptyset \notin \emptyset$.
  If A is non-empty, then by the Axiom of Singleton Sets, there exists such a set $\{A\}$ that $x{=}A{\iff}x{\in}\{A\}$. Then according to the Axiom of Foundation, and because A is a set and also the only element of $\{A\}$, $A \cap \{A\} = \emptyset$. Now suppose for the sake of contradiction that $A \in A$. Then:

  $$A \in A \wedge A \in \{A\} \implies A \in A \cap \{A\} \implies A \cap \{A\} \neq \emptyset,$$

  a contradction. Therefore, $A \notin A$ if A is non-empty. In all, $A \notin A$.

- By the Axiom of Empty Set, $\exists \emptyset\ \forall x\ x \notin \emptyset$. Since A and B are sets and are therefore objects:
  - If $A = \emptyset$ and $B = \emptyset$, then $A \notin B$ and $B \notin A$.
  - If $A = \emptyset$ and $B \neq \emptyset$, then $B \notin A$.
  - If $A \neq \emptyset$ and $B = \emptyset$, then $A \notin B$.

  Now if $A \neq \emptyset$ and $B \neq \emptyset$, then by the Axiom of Pair Sets $\exists\{A, B\}\forall x\ x = A \vee x = B \iff x \in \{A, B\}$. Then according to the Axiom of Foundation, there is at least one element x of $\{A, B\}$ which is either not a set, or $x \cap \{A, B\} = \emptyset$. Since $\{A, B\}$ only consists of two element A and B which are both sets, then at least one of the statements $A \cap \{A, B\} = \emptyset$ and $A \cap \{A, B\} = \emptyset$ is true:

  - $A \cap \{A, B\} = \emptyset \implies \forall x[x \in \{A, B\} \implies x \notin A] \implies [x = A \vee x = B \implies x \notin A]$ $\implies [x = A \implies x \notin A \wedge x = B \implies x \notin A] \implies [A \notin A \wedge B \notin A] \implies B \notin A$
  - $B \cap \{A, B\} = \emptyset \implies \forall x[x \in \{A, B\} \implies x \notin B] \implies [x = A \vee x = B \implies x \notin B]$ $\implies [x = A \implies x \notin B \wedge x = B \implies x \notin B] \implies [A \notin B \wedge B \notin B] \implies A \notin B$

  Therefore, at least one of the statements $A \notin B$ and $B \notin A$ is true for two non-empty sets A and B. In all, if A and B are both sets, then either $A \notin B$ or $B \notin A$ or both. □

The following lemma explains why the Axiom of Comprehension is also called the Axiom of Universial Specification.

Lemma 2.2.1 The Axiom of Universial Specification is equivalent to the existence of a 'universial set' Ω consist of all objects, *i.e.,* $\forall x \implies x \in \Omega$.

Proof. We first show that the Axiom of Universial Specification implies the existence of a 'universial set' Ω. Let p be a statement pertaining to x, then let $P(x) := p \vee \neg p$. Therefore, $\forall x\ P(x)$ is true. Then according to the Axiom of Comprehension, there exists a set $\Omega := \{x \mid P(x)\}$ such that:

$$\forall x \in \Omega \iff P(x)$$

Since $\forall x\ P(x)$ is always true,

$$\forall x \in \Omega.$$

Hence, the Axiom of Universial Specification implies the existence of a 'universial set' Ω.
We then demonstrate that the existence of a 'universial set' Ω implies the Axiom of Universial Specification. Let $P(x)$ be a statement pertaining to x. Then according to the Axiom of Seperation, there exists a set $\{x \mid P(x)\} := \{x \in \Omega \mid P(x)\}$, for any object y:

$$y \in \{x \mid P(x)\} \iff x \in \Omega \wedge P(y).$$

Since $\forall x\ x \in \Omega$ is true,

$$y \in \{x \mid P(x)\} \iff P(y).$$

Hence, the existence of a 'universial set' Ω implies the Axiom of Universial Specification.
In all the Axiom of Universial Specification is equivalent to the existence of a 'universial set' Ω. □

Lemma 2.2.2 If the uniersial set Ω exist, then $\Omega \in \Omega$.

Proof. If the universial set Ω exists, then by definition $\forall x \in \Omega$. Since the set Ω is also an object, $\Omega \in \Omega$. □

Since this lemma is contradicting Proposition 2.2.2, the Axiom of Universial Specification is ruled out by the Axiom of Foundation.
Sadly, there are not many application of the Axiom of Foundation mostly beacuse this axiom is less intuitive than other axioms. In analysis, this axiom is almost never needed, because most objects we are dealing with areprimitive objects and primitive sets. Even in the worst situation, we are investigating the sets of sets of primitive sets. However it is still essential for the sake of completeness.

2.3 Functions

Previously, we have defined sets which means that we can gather similar objects to form a collection, and studying a group of objects at the same time will definitely more convenient than investigating an individual object several times. By following this idea, if we are going to study a transformation, it will also be reasonable to gather the same transformation of different objects together. Due to this, we now introduce the concept of a function. Informally, a function $f : X \to Y$ from one set X to another set Y is an operation which assigns each element $x \in X$ as input to a single element $y \in Y$ as output. Therefore, in a function the transformation itself as well as the sets as input and output are the two key elements of a function. We are going to focus on the transformation this section while we will investigate more on the sets in the next section. We first begin with the formal definition that goes as follows:

Definition 2.3.1 (Function) Let X and Y be sets, and let $P(x, y)$ be a property pertaining to an object $x \in X$ and an object $y \in Y$, such that $\forall x \implies \exists! y \in Y\ P(x, y)$.
Then we define the function $f : X \to Y$ defined by P on the domain X and range Y to be the object which, given any input $x \in X$, assigns an output $f(x) \in Y$, defined to be the unique object $f(x)$ for which $P(x, f(x))$ is true. Thus, for any $x \in X$ and $y \in Y$:

$$y = f(x) \iff P(x, y)$$

Remark 2.3.1

- Functions are also referred to as maps or transformations, depending on the text. They are also sometimes called morphisms, although to be more precise, a morphism refers to actual functions, depending on the context.
- The symbol '$\to$'(`\to`) and '$\mapsto$'(`\mapsto`) are different. Generally speaking '$\to$' connects domain and range, while '$\mapsto$' conncects representative expression of two sets. For example, the increment operation $f(n) := n{++}$ should be written as:
$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N}\backslash\{0\} \\ n &\mapsto n{++} \end{aligned}$$
- An explicit definition of a function is defined as the function is defined by giving the domain, range and how one generates the output $f(x)$ from each input. An implicit definition of a function is defined as a function is defined by speciying what property $P(x, y)$ links the input x with the output.
- To avoid vagueness, it is suggested to give all the possible details when defining a function. Sometimes those information are abbreviated for convenience. However, this can be dangerous since the domain and range can sometimes extremely important.

We can observe that functions obey the Axiom of Substitution:

Lemma 2.3.1 (Functions obey the Axiom of Substitution)

$$x = x' \implies f(x) = f(x').$$

Proof. For $f : X \to Y$:

$$x = x' \wedge y = f(x) \iff x = x' \wedge P(x, y) \implies P(x', y) \iff y = f(x') \iff f(x) = f(x').$$

Thus, $x = x' \implies f(x) = f(x')$. □

This shows that equal inputs implies equal outputs; however, unequal inputs do not ensure unequal outputs. Now we define some basic concepts and notions for the functions. We first begin with equality.

Definition 2.3.2 (Equality of functions) Two functions $f : X \to Y$, $g : X \to Y$ with the same domain and range are said equal, $f = g$ if and only if $f(x) = g(x)$ for all $x \in X$.

Remark 2.3.2 A rather boring example of a function is the empty function $f : \emptyset \to X$ from the empty set to an arbitary set X. Since the empty set has no elements, we don not have to specify what f does to any input. Nevertheless, the empty set i a set and the empty function is a function. Note the following lemma:

Lemma 2.3.2 For each set X, there is only one empty function, *i.e.,*

$$\left.\begin{aligned} f : \emptyset \to& X \\ g : \emptyset \to& Y \end{aligned}\right\} \implies f = g$$

Proof. By the Axiom of Empty Set, $\forall x \notin \emptyset$, therefore $\forall x \in \emptyset \implies f(x) = g(x) \implies f = g$ is vacuously true. □

Since we have defined the equality, we have to verify Axioms of equality.

Verify (Equality of function is well defined) Let X and Y be sets, and let $f : X \to Y$, $g : X \to Y$ and $h : X \to Y$. Then:

- (Reflexive) $f = f$
- (Symmetric) $f = g \implies g = f$
- (Transitive) $f = g \wedge g = h \implies f = h$

Proof.

- $\forall x \in X\ f(x) = f(x) \implies f = f$
- $f = g \implies \forall x \in X\ f(x) = g(x) \implies \forall x \in X\ g(x) = f(x) \implies g = f$
- $f = g \wedge g = h \implies \forall x \in X[f(x) = g(x) \wedge g(x) = h(x)] \implies \forall x \in X\ f(x) = h(x) \implies f = h$ □

We then define the operations for functions, one fundamental one is composition.

Definition 2.3.3 (Composition) Let X, Y and Z be sets, and let $f : X \to Y$ and $g : Y \to Z$ be functions, such that the range of f is the same set as the domain of g. We then define the composition $g \circ f : X \to Z$ of the two functions g and f to be the function defined explicitly by the formula:

$$(g \circ f)(x) := g[f(x)].$$

If the range of f does not match the domian of g, we leave the composition $g \circ f$ undefined.

As usual, we have to verify the Axiom of Substitution.

Verify (Composition is well-defined) Let X, Y and Z be sets, and let $f, \tilde{f} : X \to Y$ and $g, \tilde{g} : Y \to Z$ be functions such that $f = \tilde{f}$ and $g = \tilde{g}$. Then $g \circ f = \tilde{g} \circ \tilde{f}$.

Proof.
$f = \tilde{f} \implies \forall x \in X\ f(x) = \tilde{f}(x)$
$g = \tilde{g} \implies \forall y \in Y\ g(y) = \tilde{g}(y)$
$\forall x \in X\{(g \circ f)(x) = g[f(x)] = g[\tilde{f}(x)] = \tilde{g}[\tilde{f}(x)] = (\tilde{g} \circ \tilde{f})(x)\} \implies g \circ f = \tilde{g} \circ \tilde{f}$ □

It is easy to construct a counterexample to show that composition is not commutative *i.e.,*$\exists f, g\ f \circ g \neq g \circ f$. However, composition is still associative.

Counterexample 2.3.1 (Composition is not always commutative)
Let $f : x \mapsto x^2$ and $g : x \mapsto x + 1$, then: $f \circ g : x \mapsto x^2 + 2x + 1$ and $g \circ f : x \mapsto x^2 + 1$; $f \circ g \neq g \circ f$

Lemma 2.3.3 (Composition is still associative) Let X, Y, Z and W be sets and $f : Z \to W$, $g : Y \to Z$ and $h : X \to Y$ be functions. Then $[f \circ (g \circ h)](x) = [(f \circ g) \circ h](x)$.

Proof. Forall $x \in X$:

$$[f \circ (g \circ h)](x) = f[(g \circ h)(x)] = f\{g[h(x)]\} = (f \circ g)[h(x)] = [(f \circ g) \circ h](x)$$

Therefore, $[f \circ (g \circ h)](x) = [(f \circ g) \circ h](x)$. □

Remark 2.3.3 Note that in the composition $g \circ f$, g lies in the left of f but g is applied after f. This is a little bit confusing and we should be careful.

We now describe certain special types of function, we first give the definitions.

Definition 2.3.4 (One-to-one/Injective functions) A function $f : X \to Y$ is injective if:

$$x \neq x' \implies f(x) \neq f(x')$$

Equivalently, a function is injective if:

$$f(x) = f(x') \implies x = x'$$

Remark 2.3.4 If a function is not a one-to-one function, *i.e.,*$\exists x \neq x' \implies f(x) = f(x')$, then we say that ths function is two-to-one instead of one-to-one.

Definition 2.3.5 (Onto/Surjective functions) A function $f : X \to Y$ is surjective if $f(X) = Y$, *i.e.,*

$$\forall y \in Y \implies \exists x \in X\ f(x) = y.$$

Definition 2.3.6 (Invertible/Bijective functions) A function $f : X \to Y$ is bijective if f is both injective and surjective.

Remark 2.3.5

- Surjective and bijective both depend on what the function does as well as what its range is. Therefore, it is important to specify the domain and the range before discussing anything about a function.
- If a function $x \mapsto f(x)$ is bijective, then f is sometimes called a perfect matching or a one-to-one correspondence, and we use the notion $x \leftrightarrow f(x)$ instead of $x \mapsto f(x)$
- A common error is to say that a function $f : X \to Y$ is bijective iff $\forall x \in X \implies \exists! y \in Y\ y = f(x)$. This is not what it means for a bijective; rather this is just the definition of a function. A function cannot map one element to two different elements.

Definition 2.3.7 (Inverse function) Let $f : X \to Y$ be a bijective function, then $\forall y \in Y\ \exists! x \in X\ f(x) = y$. This value of x is denoted $f^{-1}(y)$; thus f^{-1} is a function from Y to X. We call f^{-1} the inverse of f.

Here we first verify the inverse of a function is indeed a function:

Verify (Inverse function is well-defined) Let $f : X \to Y$ be a bijection, then $\forall y \in Y\ \exists! x \in X\ f(x) = y$. This shows that x is also a function of y and by the definition above, is denoted as $f^{-1} : Y \to X$.

Proof. We first prove there exists at least one $x \in X$ for each $y \in Y$ that $f(x) = y$. This is trivial since f is surjective.
We then show that there exits at most one $x \in X$ for each $y \in Y$ that $f(x) = y$. Suppose for the sake of contradiction that $\exists x_1 \neq x_2 \in X\ \exists y \in Y\ f(x_1) = f(x_2) = y$. Since f is injective, $f(x_1) = f(x_2) \implies x_1 = x_2$, a contradiction.
Therefore, $\forall y \in Y\ \exists! x \in X\ f(x) = y$; x is also a function of y. □

We now show their properties; we begin with the duality of injection and surjection.

Lemma 2.3.4 Let $f : X \to Y$ and $g : Y \to Z$ be functions, then:

- f and g are both injective $\implies g \circ f$ is injective.
- f and g are both surjective$\implies g \circ f$ is surjective.

Proof.

- Since f and g are both injective,

$$\forall x_1 \neq x_2 \in X \implies f(x_1) \neq f(x_2) \text{ and } \forall y_1 \neq y_2 \in Y \implies g(y_1) \neq g(y_2).$$

  Then $\forall x_1 \neq x_2 \in X$:

$$x_1 \neq x_2 \implies g(x_1) \neq g(x_2) \implies f[g(x_1)] \neq f[g(x_2)] \implies (g \circ f)(x_1) \neq (g \circ f)(x_2).$$

  Therefore, $g \circ f$ is injective.

- Since f and g are both surjective,

$$\forall z \in Z\ \exists y \in Y\ f(y) = z \text{ and } \forall y \in Y\ \exists x \in X\ g(x) = y.$$

  Thus, $\forall z \in Z\ \exists x \in X\ (g \circ f)(x) = z$; $g \circ f$ is surjective. □

Lemma 2.3.5 The empty function $f : \emptyset \to X$ is always injective but only surjective (and therefore bijective) if and only if $f : \emptyset \to \emptyset$.

Proof.

- By the Axiom of Empty Set, $\forall x \notin \emptyset$. Therefore, $\forall x_1 \neq x_2 \in X \implies f(x_1) \neq f(x_2)$ is vacuously true; f is injective.
- We first prove that if f is surjective then $X = \emptyset$. Suppose for the sake of contradiction that $X \neq \emptyset$, then at least $\exists a \in X$. Since f is surjective, $\forall y \in X \implies \exists x \in \emptyset\ f(x) = y$, a contradiciton because of the Axiom of Empty Set that $\forall x \notin \emptyset$. Therefore, f is surjective implies $X = \emptyset$.
  We then prove that $f : \emptyset \to \emptyset$ is surjective. Again by the Axiom of Empty Set that $\forall x \notin \emptyset$,

$$\forall y \in \emptyset \implies \exists x \in \emptyset\ f(x) = y$$

  is vacuously true. Hence, $f : \emptyset \to \emptyset$ is surjective.

- Since f is always injective but only surjective when $X = \emptyset$, f is bijective if and only if $f : \emptyset \to \emptyset$. □

Proposition 2.3.1 (Cancellation laws for composition) Let $f : X \to Y$, $\tilde{f} : X \to Y$, $g : Y \to Z$ and $\tilde{g} : Y \to Z$ be functions. Then:

- $g \circ f = g \circ \tilde{f} \land g$ is injective $\implies f = \tilde{f}$.
- $g \circ f = \tilde{g} \circ f \land f$ is surjective $\implies g = \tilde{g}$.

Proof.

- Since g is injective, $\forall x_1, x_2 \in Z \implies [g(x_1) = g(x_2) \implies x_1 = x_2]$. Becasue $g \circ f = g \circ \tilde{f}$,

$$\forall x \in X[(g \circ f)(x) = (g \circ \tilde{f})(x)] \implies \forall x \in X[g[f(x)] = g[\tilde{f}(x)]] \implies \forall x \in X[f(x) = \tilde{f}(x)] \implies f = \tilde{f}.$$

  Therefore, $g \circ f = g \circ \tilde{f} \land g$ is injective $\implies f = \tilde{f}$.

- Since f is surjective, $\forall y \in Y\ \exists x \in X\ f(x) = y$. Because $g \circ f = \tilde{g} \circ f$:

$$\forall x \in X\ g[f(x)] = \tilde{g}[f(x)] \implies \forall f(x) \in Y\ g[f(x)] = \tilde{g}[f(x)] \implies \forall y \in Y\ g(y) = \tilde{g}(y).$$

  Therefore, $g \circ f = \tilde{g} \circ f \land f$ is surjective $\implies g = \tilde{g}$. □

Counterexample 2.3.2 (Counterexamples of cancellation law for composition)

- **The cancellation law $g \circ f = g \circ \tilde{f} \implies f = \tilde{f}$ is not true if g is not injective.**
  (Informal) Let $f, \tilde{f}, g : \mathbb{R} \to \mathbb{R}$ and $f : x \mapsto x$, $\tilde{f} : x \mapsto -x$, $g : x \mapsto x^2$. Then $f \neq \tilde{f}$ but $g \circ f = x^2 = g \circ \tilde{f}$
- **The cancellation law $g \circ f = \tilde{g} \circ f \implies g = \tilde{g}$ is not true if f is not surjective.**
  (Informal) Let $f : \mathbb{R}_+ \to \mathbb{R}$ and $f : x \mapsto 1/x$, then $\forall x \in \mathbb{R}_+ \; f(x) = 1/x > 0$.
  Now let $g, \tilde{g} : \mathbb{R} \to \mathbb{R}$, and $g : x \mapsto x^2$, $\tilde{g} : x \mapsto x|x|$. Then $g \neq \tilde{g}$ but $g \circ f = 1/x^2 = 1/x \cdot |1/x| = \tilde{g} \circ f$

Lemma 2.3.6 Let $f : X \to Y$ and $g : Y \to Z$ be functions, then:

- $g \circ f$ is injective $\implies$ f is injective
- $g \circ f$ is surjective $\implies$ g is surjective

Proof.

- Suppose for the sake of contradicition that $g \circ f$ is injective but f is not. Then:

$$\exists x_1 \neq x_2 \in X \;\; f(x_1) = f(x_2) \implies g[f(x_1)] = g[f(x_2)] \implies (g \circ f)(x_1) = (g \circ f)(x_2).$$

  This implies that $x_1 = x_2$ because $g \circ f$ is a injection, a contradiciton. Therefore, f must be injective.

- Suppose for the sake of contradiciton that g is not surjective but $g \circ f$ is a surjection. Then:

$$\exists z_0 \in Z \;\forall y \in Y \;\; g(y) \neq z.$$

  However, by the surjectivity of $g \circ f$,

$$\exists x_0 \in X \;\; (g \circ f)(x_0) = z_0 \implies \exists x_0 \in X \;\; g[f(x_0)] = z \implies \exists y_0 := f(x_0) \in Y \;\; g(y_0) = z_0,$$

  a contradicition. Therfore, g must be surjective. □

Counterexample 2.3.3

- **That $g \circ f$ is injective does not implies that g must also be injective.**
  (Informal) Let $f : \mathbb{R}_+ \to \mathbb{R}$ and $f : x \mapsto x$. Then let $g : \mathbb{R} \to \mathbb{R}$ and $g : x \mapsto x^2$ which is not injective. However, $g \circ f : \mathbb{R}_+ \to \mathbb{R}$ with the mapping $x \mapsto x^2$ is injective.
- **That $g \circ f$ is surjective does not implies that f must also be surjective.**
  (Informal) Let $f : \mathbb{R}_+ \to \mathbb{R}$ and $f : x \mapsto x$ which is not surjective. Then let $g : \mathbb{R} \to [-1, 1]$ and $g : x \mapsto \sin x$. However, $g \circ f : \mathbb{R}_+ \to [-1, 1]$ with the mapping $x \mapsto \sin x$ is surjective.

We then show the properties of bijection and inverse function.

Lemma 2.3.7 Let $f : X \to Y$ be a bijective function and let $f^{-1} : Y \to X$ be its inverse, then:

- $\forall x \in X \;\; f^{-1}[f(x)] = x$
- $\forall y \in Y \;\; f[f^{-1}(y)] = y$

Also, f^{-1} is also invertible, and has its inverse $(f^{-1})^{-1} = f$.

Proof. Since f is a bijection and f^{-1} is its inverse, then:

$$\forall x \in X \;\exists y \in Y \;\; f(x) = y \text{ and } \forall y \in Y \;\exists x \in X \;\; f^{-1}(y) = x.$$

Therefore:

- $\forall x \in X \;\exists y \in Y \;\; f(x) = y \wedge x = f^{-1}(y) \implies \forall x \in X \;\; f^{-1}[f(x)] = x$.(substitute y with $f(x)$)
- $\forall y \in Y \;\exists x \in X \;\; f^{-1}(y) = x \wedge y = f(x) \implies \forall y \in Y \;\; f^{-1}[f(x)] = x$.(substitute x with $f^{-1}(y)$)

We then show that f^{-1} is invertible. Suppose for the sake of contradiction that f^{-1} is not invertible, then f^{-1} is either not injective or surjective or both.

- If f^{-1} is not injective, then:

  $$\exists y_1 \neq y_2 \in Y\ f^{-1}(y_1) = f^{-1}(y_2) \implies \exists y_1 \neq y_2 \in Y\ f[f^{-1}(y_1)] = f[f^{-1}(y_2)] \implies \exists y_1 \neq y_2 \in Y\ y_1 = y_2,$$

  a contradicition; f^{-1} must be an injection.

- If f^{-1} is not surjective, then:

  $$\exists x_0 \in X\ \forall y \in Y\ f^{-1}(y) \neq x$$

  Since f is a function:

  $$\begin{aligned}\forall x \in X\ \exists y \in Y\ y = f(x) &\implies \exists y_0 \in Y\ f(x_0) = y_0\\ &\implies \exists y_0 \in Y\ f^{-1}[f(x_0)] = f^{-1}(y_0)\\ &\implies \exists y_0 \in Y\ f^{-1}(y_0) = x_0,\end{aligned}$$

  ridiculous; f^{-1} must also a surjection.

We finally show that $(f^{-1})^{-1} = f$.
As we have shown, f^{-1} is bijective, we have:

$$\begin{aligned}\forall y \in Y\ \exists x \in X\ f^{-1}(y) = x &\iff \forall x \in X\ \exists y \in Y\ f^{-1}(y) = x\\ &\implies \forall x \in X\ \exists y \in Y\ y = (f^{-1})^{-1}(x)\\ &\implies \forall x \in X\ \exists y \in Y\ f(x) = (f^{-1})^{-1}(x)\\ &\implies (f^{-1})^{-1} = f.\end{aligned}$$

Therfore, $(f^{-1})^{-1} = f$. □

Lemma 2.3.8 Let $f : X \to Y$ and $g : Y \to Z$ be functions, then if f and g are both bijective then $g \circ f$ is also bijective and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. By the Lemma 2.3.4, since f and g are both bijective, they are both injective and surjective. Then $g \circ f$ is also injective and surjective and therefore bijective.
Since $g \circ f : X \to Z$, forall $z \in Z$ by Lemma 2.3.7:

$$\begin{aligned}(g \circ f)[(g \circ f)^{-1}(z)] &= z\\ g[f((g \circ f)^{-1}(z))] &= z\\ g^{-1}[g[f((g \circ f)^{-1}(z))]] &= g^{-1}(z)\\ f[(g \circ f)^{-1}(z)] &= g^{-1}(z)\end{aligned}$$

Since $g^{-1}(z) \in Y$, we have:

$$\begin{aligned}f^{-1}[f[(g \circ f)^{-1}(z)]] &= f^{-1}[g^{-1}(z)]\\ (g \circ f)^{-1}(z) &= f^{-1}[g^{-1}(z)]\\ (g \circ f)^{-1}(z) &= (f^{-1} \circ g^{-1})(z)\end{aligned}$$

Hence, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

Lemma 2.3.9 If $X \subseteq Y$, let $\iota_{X \to Y} : X \to Y$ be the inclusion map from X to Y, defined by mapping $x \mapsto x$ forvall $x \in X$, *i.e.*, $\iota_{X \to Y}(x) := x$ for all $x \in X$. The map $\iota_{X \to X}$ is in particular called the identity map on X.

(*a*) $X \subseteq Y \subseteq Z \implies \iota_{Y \to Z} \circ \iota_{X \to Y} = \iota_{X \to Z}$.

(*b*) For any function $f : A \to B$, $f = f \circ \iota_{A \to A} = \iota_{B \to B} \circ f$.

(*c*) For a bijective function $f : A \to B$, $f \circ f^{-1} = \iota_{B\to B}$ and $f^{-1} \circ f = \iota_{A\to A}$.

(*d*) If $X \cap Y = \emptyset$, $f : X \to Z$ and $g : Y \to Z$ are functions, then $\exists! h : X \cup Y \to Z$ such that $h \circ \iota_{X\to X\cup Y} = f$ and $h \circ \iota_{Y\to X\cup Y} = g$.

Proof.

(*a*) Since $X \subseteq Y \subseteq Z \implies [(\forall x \in X \implies x \in Y) \wedge (\forall y \in Y \implies y \in Z)]$, then $\forall x \in X$:

$$\begin{aligned}(\iota_{X\to Z} \circ \iota_{X\to Y})(x) &= \iota_{Y\to Z}[\iota_{X\to Y}(x)] \\ &= \iota_{Y\to Z}(x) \\ &= x \\ &= \iota_{X\to Z}(x)\end{aligned}$$

Therefore, $\iota_{Y\to Z} \circ \iota_{X\to Y} = \iota_{X\to Z}$.

(*b*) For any function f, we have:

- $\forall x \in A[(f \circ \iota_{A\to A})(x) = f[\iota_{A\to A}(x)] = f(x)] \implies f = f \circ \iota_{A\to A}$
- $\forall x \in A[(\iota_{B\to B} \circ f)(x) = \iota_{B\to B}[f(x)] = f(x)] \implies f = \iota_{B\to B} \circ f$

Therefore, $f = f \circ \iota_{A\to A} = \iota_{B\to B} \circ f$.

(*c*) Since f is bijective, by Lemma 2.3.7 we have:

- $\forall x \in A\ (f^{-1} \circ f)(x) = f^{-1}[f(x)] = x = \iota_{A\to A}(x) \implies f^{-1} \circ f = \iota_{A\to A}$.
- $\forall y \in B\ (f \circ f^{-1})(y) = f[f^{-1}(y)] = y = \iota_{B\to B}(y) \implies f \circ f^{-1} = \iota_{B\to B}$.

(*d*) We first construct the function h by definition and prove its validity. Since $X \cup Y$ and Z are sets, $f : X \to Z$ and $g : Y \to Z$ are functions, $\forall x \in X \cup Y$ and $y \in Z$ let:

$$P(x, y) := [x \in X \wedge y = f(x)] \vee [x \in Y \wedge y = g(x)]$$

Because $x \in X \cup Y$ and $X \cap Y = \emptyset$, exactly one of the statements $x \in X \wedge x \notin Y$ and $x \in Y \wedge x \notin X$ is true. Then:

- $x \in X \implies \exists! y = f(x) \in Z\ P(x, y)$.
- $y \in Y \implies \exists! y = g(x) \in Z\ P(x, y)$.

In all, $\forall x \in X \cup Y\ \exists! y \in Z\ P(x, y)$; there exists a valid function $h : X \cup Y \to Z$ pertaining to the statement $P(x, y)$.
We then show that h satisfies all the requirements.

- $\forall x \in X[(h \circ \iota_{X\to X\cup Y})(x) = h(x) = f(x) \in Z] \implies h \circ \iota_{X\to X\cup Y} = f$.
- $\forall x \in Y\,[(h \circ \iota_{Y\to X\cup Y})(x) = h(x) = g(x) \in Z] \implies h \circ \iota_{Y\to X\cup Y} = g$.

We finally demonstrate that h is unique. Suppose for the sake of contradicition that $\exists h' : X \cup Y \to Z$ such that $h' \circ \iota_{X\to X\cup Y} = f$ and $h' \circ \iota_{Y\to X\cup Y} = g$.
Because $X \cap Y = \emptyset \implies \forall x \in X \cup Y[(x \in X \wedge x \notin Y) \vee (x \in Y \wedge x \notin X)]$, we discuss the statement in two cases:
$\forall x \in X$, we have:

$$\begin{aligned}(h \circ \iota_{X\to X\cup Y})(x) &= h[\iota_{X\to X\cup Y}(x)] = f(x) \\ &= h(x) \\ \implies \quad h(x) = f(x) & \\ (h' \circ \iota_{X\to X\cup Y})(x) &= h'[\iota_{X\to X\cup Y}(x)] = f(x) \\ &= h'(x) \\ \implies h'(x) = f(x) &\end{aligned}$$

Therefore, $\forall x \in X\ h'(x) = h(x)$.
$\forall x \in Y$, we have:

$$\begin{aligned}
(h \circ \iota_{Y \to X \cup Y})(x) &= h[\iota_{Y \to X \cup Y}(x)] = g(x) \\
&= h(x) \\
\implies\ h(x) = g(x) & \\
(h' \circ \iota_{Y \to X \cup Y})(x) &= h'[\iota_{Y \to X \cup Y}(x)] = g(x) \\
&= h'(x) \\
\implies\ h'(x) = g(x) &
\end{aligned}$$

Therefore, $\forall x \in Y\ h'(x) = h(x)$. In all, $\forall x \in X \cup Y\ h(x) = h'(x) \implies h = h'$, a contradiction; the function h must be unique. □

2.4 Images and inverse images

Under Construction.

2.5 Cartesian product

Under Construction.

2.6 Cardinality of sets

Under Construction.

Chapter 3

The Natural Numbers

Map:

$$\begin{tikzcd}\underset{\text{You Are Here}}{\mathbb{N}} \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Q}\end{tikzcd}$$

3.1 The Peano axiom

One of the standard ways of defining the natural number is by the *Peano axioms.* It was first laid out by Guiseppe Peano (1858-1932). Other alternative approach of defining natural numbers will be discussed later.

Definition 3.1.1 (Informal) A *natural number* is any element of the set

$$\mathbb{N} := \{0, 1, 2, 3, 4, ...\},$$

which is the set of all the numbers created by starting with 0 and then counting forward indefinitely. We call $\mathbb{N}$ the *set of natural numbers.*

Remark 3.1.1 The set $\{1, 2, 3, ...\}$ is called *the positive integers*, i.e., $\mathbb{Z}_+$, not the natural numbers. The natural numbers are sometimes called *whole numbers.*

However, there are two drawbacks in this definition. First, we need to define the concepts of 'set' and 'element'. Second, as to $\mathbb{N}$, there are many questions to be answered. For example, how can we gaurantee that we can keep counting indefinitely without counting back to 0? In addition, the action 'count forward' need to be defined rigorously.
As to the second question, it is necessary because we can always define complicated operation by simpler operations. For example, exponentiation is repeated multiplication, multiplication is repeated addiction, and addiction is repeated *counting forward*, or *incrementing.* But incrementing cannot be reduced to any simpler operation.
Therefore, the task of defining the natural numbers is broken down into two subtask:

- define the zero number 0,
- define the increment operation.

Here we denote the increment operation as '++' and 'n++' means the increment or *successor* of n.
So the set of the natural numbers can be written as:

$$\mathbb{N} := \{0, 0{+}{+}, (0{+}{+}){+}{+}, ((0{+}{+}){+}{+}){+}{+}, ...\}.$$

From this we could extract two axioms about 0 and ++:

Axiom 3.1 0 is a natural number.

Axiom 3.2 If n is a natural number, then n++ is also a natural number.

For the convenience of writing we introduce the following notation:

Definition 3.1.2 $1 := 0{+}{+}$[1]$, 2 := 1{+}{+}, 3 := 2{+}{+},$ etc.

Proposition 3.1.1 3 is a natural number.

Proof. By Axiom 3.2, 0 is a natural number. By Axiom 3.2, $1 = 0{+}{+}$ is a natural number. By Axiom 3.2 again, $2 = 1{+}{+}$ is a natural number. By Axiom 3.2 again, $3 = 2{+}{+}$ is a natural number. □

Now let's consider the first question. In order to *prevent* us from counting indefinitely back to 0, we should impose another axiom:

Axiom 3.3 0 is not the successor of any other natural number; i.e., we have $n{+}{+} \neq 0$ for every natural number n.

Proposition 3.1.2 4 is not equal to 0.

Proof. By definition, $4 = 3{+}{+}$. By Axiom 3.1 and 3.2, 3 is a natural number. Thus by Axiom 3.3, $3{+}{+} \neq 0$, i.e. $4 \neq 0$. □

However, even with these three axioms, the natural numbers are still not well-defined. Let's consider the following situation.

Example 3.1.1 Suppose that: $0{+}{+} = 1$, $1{+}{+} = 2$, $2{+}{+} = 3$, $3{+}{+} = 4$, but $4{+}{+} = 4$, $5{+}{+} = 4$, $6{+}{+} = 4$, etc. This situation does not violate Axiom 3.1, 3.2 and 3.3, even though it is not the system of natural numbers.
Another situation shows the similar pattern. Suppose that: $0{+}{+} = 1$, $1{+}{+} = 2$, $2{+}{+} = 3$, $3{+}{+} = 4$, but $4{+}{+} = 1$, $5{+}{+} = 2$, $6{+}{+} = 3$, etc.

To fix this problem, we introduce the following axiom:

Axiom 3.4 Suppose that n, m are natural numbers. If $n \neq m$, then $n{+}{+} \neq m{+}{+}$. Equivalently, if $n{+}{+} = m{+}{+}$, then $n = m$.

Therefore, we have:

Proposition 3.1.3 $6 \neq 2$

Proof. By Proposition 3.1.2, $4 \neq 0$. By Axiom 3.3, $4{+}{+} \neq 0{+}{+}$, i.e. $5 \neq 1$. By Axiom 3.3 again, $5{+}{+} \neq 1{+}{+}$, i.e. $6 \neq 2$. □

It seems that the natural numbers are well defined, but the fact is that we can construct another number system which satisfies Axiom 3.1-3.4 but is different from what we want.

Example 3.1.2 (Informal[2]) Suppose our number system $\mathbb{N}$, consists of the following collection of *integers* and *half-integers*:

$$\mathbb{N} := \{0, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, ...\}.$$

This problem is difficult to fix because it is not distinguishable between *integers* and *half-integers* in this scenario. Of course we can define that only numbers in $\mathbb{N}$ can be obtained from 0 and ++. However, it is difficult to quantify the meaning of the phrase 'can be obtained from'.
Fortunately, there is an ingenious way to try to capture this fact:

Axiom 3.5 (Principle of mathematical induction) Let $P(n)$ be any property pertaining to a natural number n. Suppose that $P(0)$ is true, and suppose that whenever $P(n)$ is true, $P(n{+}{+})$ is also true. Then $P(n)$ is true for every natural number n.

Remark 3.1.2 This axiom is different from the other four axioms beacuse this axiom refers not just to *variables* but also *properties*. So technically speaking, Axiom 3.5 is an *axiom schema*, i.e. a template for producing an (infinite) number of axioms.

[1] '$x := y$' means that x is *defined* to equal y

[2] This example is informal because we used some concepts (in italic) that we haven't defined.

Now by useing this axiom, we can fix the previous problem.
Suppose $P(n)$ is such that $P(0)$ is true, and such that whenever $P(n)$ is true, then $P(n{+}{+})$ is true. Then since $P(0)$ is true, $P(0{+}{+}) = P(1)$ is true. Since $P(1)$ is true, $P(1{+}{+}) = P(2)$ is true. Repeating this indefinitely, we see that $P(0), P(1), P(2), P(3)$, etc. are all true. However this line of reasoning will never let us conclude that $P(0.5)$, for instance, is true. Thus Axiom 3.5 should not hold for for number systems which contain 'unncecssary' elements such as 0.5.
In fact, we can give a 'proof'[1] to show this fact. Apply Axiom 3.5 to property that $P(n) = n$ is not a 'half-integer'[2]. Then $P(0)$ is true, and by Axiom 3.2 if $P(n)$ is true, then $P(n{+}{+})$ is true. Thus Axiom 3.5 asserts that $P(n)$ is true for all natural number n, i.e., no natural number can be a half-integer. In particular, 0.5 can not be a natural number.
Axiom 3.5 gives us a way to prove that a property $P(n)$ is true for every natural number n. Here is the 'template' of using mathematical induction in the proof.

Proposition 3.1.4 A certain property $P(n)$ is true for every natural number n.

Proof. We use induction. We first verify the base case $n = 0$, i.e., we prove $P(0)$. (Insert proof of $P(0)$ here). Now we suppose inductively that n is a natural number, and $P(n)$ has already been proven. We now prove $P(n{+}{+})$. (Insert proof of $P(n{+}{+})$, assuming that $P(n)$ is true, here). This closes the induction, and thus $P(n)$ is true for all numbers n. □

In a specific proof, we don't have to exactly copy this template. But any proof using mathematical induction has the same form as above generally. Also, we should point out that there are some other variants of induction such as backwards induction, strong induction and transfinite induction, which will be dicussed later.
Axioms 3.1-3.5 are known as the *Peano axioms* for the natural numbers. They are all very plausible, so we shall make:

Assumption 3.1 (Informal) There exists a number system $\mathbb{N}$, whose elements we will call natural numbers, for which Axioms 3.1-3.5 are true.

This assumption will be made more precisely later.

Remark 3.1.3 (Different natural number systems) Of course there are more than one natural number system. For example, we have the Hindu-Arabic number system $\{0, 1, 2, 3, ...\}$ and the Roman number system $\{O, I, II, III, IV, V, VI, ...\}$. But these number systems are clearly equivalent, or isomorphic in this situation, because we can create a one-to-one correspondence $0 \leftrightarrow O$, $1 \leftrightarrow I$, $2 \leftrightarrow II$. In addition, we can apply this method to other natural number systems. Therefore, all the natural number systems are equivalent, which means that there is no point in having distinct number systems. We can just use a single number system to do mathematics.

As to the Assumption 3.1, we will not going to prove it. Instead, we will include this in an axiom later. Also, Assumption 3.1 will be the only assumption that we make in defining the numbers.

Remark 3.1.4 (Informal) One interesting feature about the natural number is that while each individual natural number is finite, the *set* of natural numbers is infinite; i.e., $\mathbb{N}$ is infinite but consists of individually finite elements. (The whole is greater than any of its parts.) There are no infinite natural numbers; we can prove this by Axiom 3.5:

Proof. Clearly 0 is finite. Also if n is finite, then clearly $n{+}{+}$ is also finite. Hence by Axiom 3.5, all natural numbers are finite. □

So, natural numbers can *approach* infinity, but never actually *reach* it; infinity is not one of the natural numbers [3].

[1] This 'proof' is not rigorous. But this example can provide us some idea as to how to use Axiom 3.5 to prohibit any numbers other than the 'true' numbers from appearing in $\mathbb{N}$.

[2] an integer plus 0.5.

[3] There are some other number systems which admit 'infinte' numbers, such as cardinals, ordinals, and p-adics, but they do not obey the principle of mathematical induction.

Remark 3.1.5 Please not carefully that our definition of the natural numbers is *axiomatic* rather than *constructive.* We have not told you what the natural numbers *are* (so we do not address such questions as what the numbers are made of, are they physical objects, what do they measure, etc.) - we have only listed some things you can do with them (in fact, the only operation we have defined on them right now is the increment one) and some of the properties that they have.
This is just how mathematics works - it treats it objects abstractly, caring only about what properties the objects have, not what the objects are or what they mean. If one wants to mathematics, it does not matter whether a natural number means a certain arrangement of beads on an abacus, or a certain orgainization of bits in computer's memory, or some more abstract abstract concept with no physical substances; as long asyou can increment, see if two of the are equal, and later on do other arithmetic operation such as add and multiply, they qualify as numbers for mathematical purposes.
Of course it is possible to construct the natural numbers from other mathematical objects. For example, using sets, and in fact there are many ways to construct a working model of the natural numbers. However, this is pointless, at least from a mathematician's view, to argue which model is the 'true' one because as long as it obeys all the axiom and does all the right things, that is good enough to do maths.

Remark 3.1.6 Historically, it has not been a long time, about a hundred years, since people realized that numbers could be treated axiomatically. Before that time, numbers were generally understood to be inextricably connected to some external concept, such as ounting the cardinality of a set, measuring the length of a line segment, or the mass of a physical object, etc. This worked reasonably well, until one was forced to move from one number system to another; for instance, understanding numbers in terms of counting beads is great for conceptualizing the number 3 and 5, but doesn't work so well for -3 or $1/3$ or $\sqrt{2}$ or $3 + 4i$; thus each great advance in the theory of numbers - negative numbers, irrational numbers, complex numbers, even the number zero - led to a lot of unnecessary philosophical anguish.
The great discovery of the late 19th century was that numbers can be undestood abstractly via axioms, without necessarily needing a concrete model; of course a mathematician can use any of these models when it is convenient, to aid his or her intuition and understanding, but they can also be just as easily discarded when they begin to get in the way.

One consequence of the axioms is that we can now define sequence recursively. Suppose we want to build a sequence $a_0, a_1, a_2, ...$ of numbers by first defining $a_0 := c$ for some number c, and then by letting a_1 be some function of a_0, $a_1 := f_0(a_0)$, a_2 be some function of a_1, $a_2 := f_1(a_1)$, and so forth.
In general, we set $a_{n{+}{+}} = f_n(a_n)$ for some function f_n from $\mathbb{N}$ to $\mathbb{N}$. By using all the axioms together we will now conclude that this procedure will give a single value to the sequence element a_n for each natural number n. More precisely[1]:

Proposition 3.1.5 (Recursive definitions[2]) Suppose for each natural number n, we have some functions $f_n : \mathbb{N} \to \mathbb{N}$ from the natural numbers to natural numbers. Let c be a natural number. Then we can assign a unique natural number a_n to each natural number n, such that $a_0 = c$ and $a_{n{+}{+}} = f_n(a_n)$ for each number n.

Proof. (Informal) We use induction. First, this procedure gives a single value to a_0, namely c and this value will not be redefined by $a_{n{+}{+}} = f_n(a_n)$ because of Axiom 3.3. Now suppose inductively that the procedure gives a single value to a_n. Then it gives a single value to $a_{n{+}{+}}$, namely $a_{n{+}{+}} = f_n(a_n)$, and $a_{n{+}{+}}$ will not be redefined because of the Axiom 3.4. This completes the induction, and so a_n is defined for each natural number n, with a single value assigned to a_n. □

Recursive definitions are powerful because they prevent these two following things from appearing by making the definition itself malfunctioning.

- If a system has some sort of wrap-around, i.e. some of the elements would be constantly redefined. This would lead to a conflict that one element has at least two inequivalent definitions.
- If a system has superfluous elements such as $a_{0.5}$, then those elements will not be defined.

Therefore, recursive definitions are especially useful when defining things like addition and multiplication.

[1] Strictly speaking, the definition of a function will be introduced later. However, this will not be circular since the concept of a function does not require the Peano axioms.

3.2 Addition

The natural number system is very bare right now; we only have one operation - increment - and a handful of axioms. But fortunately, we have enough materials to build up more complex operations, such as addition. First, let's talk about how addition works. For example, let's try to add three to five:

$$\begin{array}{rlrl}
3+5 & \text{is the same as} & [(5{++}){++}]{++} & \text{(increment 5 for 3 times)} \\
[(5{++}){++}]{++} & \text{has one increment more than} & (5{++}){++} & \text{(the same as 2+5)} \\
(5{++}){++} & \text{has one increment more than} & 5{++} & \text{(the same as 1+5)} \\
5{++} & \text{has one increment more than} & 5 & \text{(the same as 0+5)}
\end{array}$$

From this example, it is clear that addition can be defined by using recursive definitions. Also, we can see that the key points of defining addition are:

- Defining '$a_0 = c$', i.e. defining $0 + m$ in this scenario.
- Defining '$a_{n{++}} = f_n(a_n)$', i.e. defining $(n{++} + m)$ using $n + m$ in this scenario.

Therefore, we have:

Definition 3.2.1 (Addition of natural numbers) Let m be a natural number. To add zero to m, we define $0 + m := m$. Now suppose inductively that we have defined how to add n to m. Then we can add $n{++}$ to m by defining $(n{++} + m) := (n + m){++}$.

Thus, for instance:

$$\begin{aligned}
3+5 &= (2{++}) + 5 = (2+5){++} \\
&= [(1{++}) + 5]{++} = [(1+5){++}]{++} \\
&= \{[(0{++}) + 5]{++}\}{++} = \{[(0+5){++}]{++}\}{++} \\
&= [(5{++}){++}]{++} = (6{++}){++} = 7{++} \\
&= 8
\end{aligned}$$

By using Axiom 3.1,3.2, and induction, we can prove that the sum of two natural numbers is still a natural number.

Proposition 3.2.1 If m and n are natural numbers, then $n + m$ is also a natural number.

Proof. Becasue m is a natural number, for natural 0, $0 + m = m$ is also a natural number. Suppose for a natural n that $n + m$ is a natural number. Then as to $n{++}$, $(n{++}) + m = (n + m){++}$ is also a natural number. This closes the induction and thus $n + m$ is a natural number for all the numbers n. □

Also, please note that this definition is asymmetric: $3 + 5$ is incrementing 5 three times, while $5 + 3$ is incrementing 3 five times.Of course they both yield the same value of 8. And more generally, it is a fact that $a + b = b + a$. Since this fact cannot be drawn from the definitions and axioms immediately, we shall begin with some basic lemmas.

Lemma 3.2.1 For any natural number n, $n + 0 = n$.

Please note that we cannot deduce this immediately form $0 + m = m$ because we have not known $a + b = b + a$ yet.

Proof. We use induction. Since 0 is a natural number and $0 + m = m$ for every natural number m, we have $0 + 0 = 0$. Now suppose inductively that $n + 0 = n$, then as to $n{++}$, we have $(n{++}) + 0 = (n + 0){++} = n{++}$. This closes the induction and thus $n + 0 = n$ for all natural number n. □

Lemma 3.2.2 For any natural numbers n and m, $n + (m{++}) = (n + m){++}$.

Same as the previou one, we cannot deduce this immediately form $(n{++}) + m = (n + m){++}$ because we have not known $a + b = b + a$ yet

Proof. We use induction. By keeping m fixed, in the case where $n = 0$, we have $0 + (m{++}) = m{++}$. Now suppose inductively that $n + (m{++}) = (n + m){++}$. Then as to $n{++}$, we have:

$$\begin{aligned}(n{++}) + (m{++}) &\overset{\text{Definition3.2.1}}{=\!=\!=\!=\!=} [n + (m{++})]{++}\\ &\overset{\text{Assumption}}{=\!=\!=\!=\!=} [(n + m){++}]{++}\\ &\overset{\text{Definition3.2.1}}{=\!=\!=\!=\!=} [(n{++}) + m]{++}\end{aligned}$$

This closes the induction and thus $n + (m{++}) = (n + m){++}$ is true for any natural numbers m and n. □

From Lemma 3.2.1 and 3.2.2, we have:

Corollary 3.2.1 $n{++} = n + 1$

Proof. We use induction. In the case $n = 0$, we have $0 + + = 1 = 0 + 1$ because of the definitions $0{++} = 1$ and $0 + m = m$. Now suppose inductively that $n{++} = n + 1$. Then as to $n{++}$, we have $(n{++}){++} = [(n{++}) + 0]{++} = (n{++}) + (0{++}) = (n{++}) + 1$. This closes the induction and thus $n{++} = n + 1$ for all natural number n. □

Now we are fully prepared and ready to prove that $a + b = b + a$.

Proposition 3.2.2 (Addition is commutative) For any natural numbers m and n, $n + m = m + n$.

Proof. We use induction. By keeping m fixed, in the base case $n = 0$, we show that $0 + m = m + 0$. By the definition of addition, we have $0 + m = m$. By Lemma 3.2.1, we have $m + 0 = m$. Therefore, $0 + m = m + 0$. Thus, the base case is done. Now suppose inductively that $n + m = m + n$, now we have to prove that $(n{++}) + m = m + (n{++})$. By the definition of addition, $(n{++}) + m = (n + m){++}$. By Lemma 3.2.2, $m + (n{++}) = (m + n){++} = (n + m){++}$. Thus, $(n{++}) + m = m + (n{++})$. This closes the induction and thus for any natural numbers m and n, $n + m = m + n$. □

Proposition 3.2.3 (Addition is associative) For any natural numbers a, b, c, we have $(a + b) + c = a + (b + c)$.

Proof. We use induction. By keeping a and b fixed, in the base case $c = 0$, we show that $(a+b)+0 = a+(b+0)$. By Lemma 3.2.1, $(a + b) + 0 = a + b$ and $a + (b + 0) = a + b$. Therefore, $(a + b) + 0 = a + (b + 0)$. Thus the base case is done. Now suppose inductively that $(a + b) + c = a + (b + c)$ we have to prove that as to $c{++}$, $(a + b) + (c{++}) = a + [b + (c{++})]$. In fact, we have:

$$\begin{aligned}(a + b) + (c{++}) &\overset{\text{Lemma3.2.2}}{=\!=\!=\!=\!=} [(a + b) + c]{++}\\ &\overset{\text{Assumption}}{=\!=\!=\!=\!=} [a + (b + c)]{++}\\ &\overset{\text{Lemma3.2.2}}{=\!=\!=\!=\!=} a + [(b + c){++}]\\ &\overset{\text{Lemma3.2.2}}{=\!=\!=\!=\!=} a + [b + (c{++})]\end{aligned}$$

This closes the induction and thus for any natural numbers a, b, c, we have $(a + b) + c = a + (b + c)$. □

Because of this assiociativity we can write sums such as $a + b + c$ without having to worry about which order the numbers are being added together. Now we develop the cancellation law.

Proposition 3.2.4 (Cancellation law) Let a, b, c be natural numbers such that $a + b = a + c$. Then we have $b = c$.

Please note that we cannot use subtraction or negative numbers to prove this proposition becasue these concepts have not ye defined. In fact this cancellation law is crucial in letting us define subtraction and negative numbers because it allows for a sort of 'virtual subtraction' even before subtraction is officially defined.

Proof. We prove this proposition by induction on a. In the base case where $a = 0$, we have $0 + b = 0 + c$ which implies that $b = c$ by definition of addition. Now suppose inductively that we have the cancellation law for a. Then as to $a{++}$, we show that if $(a{++}) + b = (a{++}) + c$, then $b = c$. By the definition of addition, we have $(a + b){++} = (a + c){++}$. Then by Axiom 3.4, we have $a + b = a + c$. And by the cancellation law for a, we have $b = c$. This closes the induction and thus for natural numbers a, b, c if $a + b = a + c$ then we have $b = c$. □

Now we discuss how addition interacts with positivity.

Definition 3.2.2 (Positive natural numbers) A natural number is said to be positive iff[1] it is not equal to 0.

Proposition 3.2.5 If a is positive and b is a natural number, then $a + b$ is positive. (So it is with $b + a$ by Proposition 3.2.2.)

Proof. We use induction on b. If $b = 0$, then $a + b = a + 0 = a$, which is positive. Now suppose inductively that $a + b$ is positive. Then $a + (b{+}{+}) = (a + b){+}{+}$ can not be zero by Axiom 3.3, and is hence positive. This closes the indcuction. □

Corollary 3.2.2 If a and b are natural numbers such that $a + b = 0$, then $a = 0$ and $b = 0$.

Proof. Suppose for the sake of contradiction that $a \neq 0$ or $b \neq 0$. If $a \neq 0$ then a is positive, and hence $a + b = 0$ is positive by Proposition 3.2.5, a contradiction. Similarly if $b \neq 0$ then again $a + b = 0$ is positive by Proposition 3.2.5, also a contradiction. Thus a and b must both be zero. □

Lemma 3.2.3 Let a be a positive number. Then there exists exactly one natural number b such that $b{+}{+} = a$.

Proof. The lemma is equivalent to another lemma that for any natural number a, exactly one of these two statements is true: (1) $a = 0$ or (2) there exists a unique natural number b such that $b{+}{+} = a$.
Now we use the induction.
We first prove the base case $P(0)$. Statement (1) is true since $0 = 0$, while by Axiom 3.3 statement (2) is not true. Therefore the base case is done.
Now suppose inductively that we have proved $P(a)$. Then we must show $P(a{+}{+})$. This means we need to show between (1) $a{+}{+} = 0$, and (2) there is a unique natural number whose succesor is $a{+}{+}$ there is exactly one true statement.
By Axiom 3.3 statement (1) is false. Then we let $b = a$ so that $b{+}{+} = a{+}{+}$. Hence we proved the existence of b. Now we prove the uniqueness of b. Suppose for the sake of contradiction that there are two such natural numbers b and b' that $b \neq b'$, $b{+}{+} = a$, and $b'{+}{+} = a$. Then we have $b{+}{+} = b'{+}{+}$, and by Axiom 3.4 we have $b = b'$, a contradiction.
Therefore there is a unique natural number whose succesor is $a{+}{+}$. Thus $P(a{+}{+})$ is proved, which closes the induction. Finally, the lemma is proved. □

Once we have a notion of addition, we can now begin defining a notion of *order.*

Definition 3.2.3 (Ordering of the natural numbers) Let n and m be natural numbers. We say that n is greater than or equal to m, and write $n \geq m$ or $m \leq n$, iff we have $n = m + a$ for some natural number a. We say that n strictly greater than m, and write $n > m$ or $m < n$, iff $n \geq m$ and $n \neq m$.

Lemma 3.2.4 For any natural number n, $n{+}{+} > n$.

Proof. We first prove that $n{+}{+} \geq n$. By Corollary 3.2.1, $n{+}{+} = n + 1$ and 1 is a natural number. Therefore, $n{+}{+} \geq n$.
We then prove that $n{+}{+} \neq n$. We use induction. In the base case where $n = 0$, by Axiom 3.3 $0{+}{+} \neq 0$. Hence $1 \neq 0$; the base case is done. Now suppose inductively that $n{+}{+} \neq n$. Then as to $n{+}{+}$, by Axiom 3.4 we have $(n{+}{+}){+}{+} \neq n{+}{+}$. This closes the induction and thus for all natural number n, we have $n{+}{+} \neq n$.
Finally, we have $n{+}{+} > n$. □

Corollary 3.2.3 There is no largest natural number n

Proof. Suppose for the sake of contradiction that n is the largest natural number. Then by Lemma 3.2.4, we have $n{+}{+} > n$, i.e. $n{+}{+}$ is larger than n, a contradiction. Thus there is no largest natural number. □

[1] 'Iff' is shorthand for 'if and only if'.

Proposition 3.2.6 (Basic properties of order for natural numbers) Let a, b, c be natural number.

(a) (Order is reflexive) $a \geq a$.
(b) (Order is transitive) If $a \geq b$ and $b \geq c$, then $a \geq c$.
(c) (Order is anti-symmetric) If $a \geq b$ and $b \geq a$, then $a = b$.
(d) (Addition preserves order) $a \neq b$ iff $a + c \neq b + c$.
(e) $a < b$ iff a++ $\leq b$.
(f) $a < b$ iff $b = a + d$ for some positive number d.

Proof.

- (a) By Lemma 3.2.1 $a = a + 0$, and 0 is a natural number. Therefore by Definition 3.2.3, $a \geq a$.
- (b) Since $a \geq b$ and $b \geq c$, there exists two natural numbers r and r' such that $a = b + r$ and $b = c + r'$. Thus, $a = c + (r + r')$ where $r + r'$ is also a natural number. Therefore by definition, $a \geq c$.
- (c) Since $a \geq b$ and $b \geq a$, there are two natural numbers r and r' such that $a = b + r$ and $b = a + r'$. Then we replace the a in the second equation by $b + r$ and get $b = b + r + r'$. Thus, left side of the equation is:$b = b + 0$ while the right side is:$(b + r) + r' = b + (r + r')$, and by cancellation law, we have $r + r' = 0$. Then by Corollary 3.2.2, $r = r' = 0$. Hence $a = b + 0 = b$.
- (d) We first prove that if $a \neq b$ then $a + c \neq b + c$. By cancellation law that $a + c = b + c \rightarrow a = b$. Thus, $a \neq b \rightarrow a + c \neq b + c$.
  We then prove that if $a + c \neq b + c$ then $a \neq b$. By substitution law and treating '$+c$' as an operation, we have $a = b \rightarrow a + c = b + c$. Thus, $a + c \neq b + c \rightarrow a \neq b$.
  Thus $a \neq b$ iff $a + c \neq b + c$.
- (e) We first prove that if $a < b$ then a++ $\leq b$. Since $a < b$, there is a natural number r such that $a + r = b$, and $a \neq b$. Now suppose for the sake of contradiction that $r = 0$, then $a = b$, a contradiction. Hence $r \neq 0$, which means that r is positive. According to Lemma 3.2.3, there exist a natural number p such that p++ $= r$. Thus, $b = a + (p\text{++}) = (a\text{++}) + p$, which shows that a++ $\leq b$.
  We then prove that if a++ $\leq b$, then $a < b$. By definition we have there exist a natural number q that $(a\text{++}) + q = b$. Thus $a + (q\text{++}) = b$, which show that $a \leq b$. By Axiom 3.3 we have q++ $\neq 0$. Now suppose for the contradiction that $a = b$, then as to $a + (q\text{++}) = b = 0 + b$ we have q++ $= 0$ via cancellation law, a contradiction. Hence, $a \neq b$. Therefore $a < b$.
- (f) We first prove that if $a < b$, then $b = a + d$ for some positive number d. By definition, there is a natural number d that $a + d = b$, and $a \neq b$. Now suppose for the sake of contradiction that $d = 0$, we have $b = a + 0 = a$, a contradiction. Hence $d \neq 0$, which shows that d is positive.
  We then prove that if $b = a + d$ for some positive number d, then $a < b$. By definition, we have $a \leq b$. Also, because d is positive, $d \neq 0$. Now we must show that $a \neq b$. Now suppose for the sake of contradiction that $a = b$. Then as to $a + d = b = b + 0$ we have $d = 0$ by cancellation law, a contradiction. Hence $a \neq b$ and $a < b$. □

Proposition 3.2.7 (Trichotomy of order for natural numbers) Let a and b be natural numbers. Then exactly one of the following statements is true: $a < b$, $a = b$, $a > b$.

Proof. We first prove that we cannot have more than one of the statements $a < b$, $a = b$, $a > b$ holding at the same time. If $a < b$, then by definition $a \neq b$. If $a > b$, then by definition again $a \neq b$. If $a < b$ and $a > b$, we have $a \leq b$ and $a \geq b$ and $a \neq b$. Then then by Proposition 3.2.6(c) $a \neq b$ and $a = b$, a contradiction.
We then prove that at least one of the statements is true. We use induction on a by keeping b fixed. In the base case where $a = 0$, we show that $0 \leq b$. Because $b = 0 + b$ and 0 is a natural number by Axiom 3.1, we have $0 \leq b$. Hence we have either $0 = b$ or $0 < b$ by previous conclusion. Now suppose inductively that we have proved the proposition for a, we must show the proposition for a++. By trichotomy for a, there are three cases: $a < b$, $a = b$, $a > b$. If $a < b$, then by Proposition 3.2.6(e), a++ $\leq b$ which means that either a++ $< b$ or a++ $= b$. If $a = b$, then by Proposition 3.2.6(f) a++ $> b$ because a++ $= b + 1$ and $1 = 0$++ $\neq 0$ is a positive number. If $a > b$, then we must show that a++ $> b$. Because of the fact that $a > b$, there is a positive number c that $a = b + c$. Then by Corollary 3.2.1, a++ $= a + 1$. Thus, a++ $= (b + c) + 1 = b + (c + 1)$. Then by Proposition 3.2.5, $c + 1$ is positive. Thus a++ $> b$.This closes the induction. □

Corollary 3.2.4 For all natural number n, $n \neq 0$ iff $n \geq 1$.

Proof. We first prove that □

The properties of order allow one to obtain some srtonger versions of the principle of induction.

Lemma 3.2.5 (General form of mathematical induction) Let $P(n)$ be any property pertaining to a natural number $n \geq m_0$. Suppose that $P(m_0)$ is true, and suppose that whenever $P(n)$ is true $P(n{+}{+})$ is also true. Then $P(n)$ is true for all natural number $n \geq m_0$.

Proof. We let $Q(n)$ be $P(n + m_0)$ is true. In the base case where $n = 0$, $Q(0)$ is true since $P(m_0)$ is true. Now uppose inductively that $Q(n)$ is true. Then $P(n + m_0)$ is true, thus $P(n + m_0{+}{+})$ is also true. So $Q(n{+}{+})$ is also true. This closes the induction and thus for all natural number n, $Q(n)$ is true, i.e. $P(n)$ is true for all natural number $n \geq m_0$. □

Proposition 3.2.8 (Strong principle of induction) Let m_0 be a natural number, and let $P(n)$ be a property pertaining to an arbitary natural number $n \geq m_0$. If the following two conditions are satisfied. (1) $P(m_0)$ is true. (2) if $P(m')$ is true for all natural numbers $m_0 \leq m' \leq n$, then $P(n{+}{+})$ is also true. Then we conclude that $P(n)$ is true for all natural numbers $n \geq m_0$.

Remark 3.2.1 In applications we usually use this principle with $m_0 = 0$ or $m_0 = 1$.

Proof. We let $Q(n)$ be that $P(m)$ is true for all $m_0 \leq m' \leq n$ where $m_0 \leq n$. We use induction.
In the base case where $n = m_0$, $Q(m_0)$ is true since $P(m_0)$ is true. Now suppose inductively that $Q(n)$ is true. Then $P(m')$ is true for all $m_0 \leq m' \leq n$. So $P(m')$ is true for all $m_0 \leq m' \leq n{+}{+}$. Hence, $Q(n{+}{+})$ is also true. This closes the induction. Therefore, for all $n \geq m_0$, $Q(n)$ is true, i.e. $P(m)$ is true for all natural numbers $m \geq m_0$. □

Proposition 3.2.9 (Principles of backwards induction) Let n be a natural number, and let $P(m)$ be a property pertaining to the natural numbers such that whenever $P(m{+}{+})$ is true, then $P(m)$ is true. Suppose that $P(n)$ is also true. Then $P(m)$ is true for all natural numbers $m \leq n$.

Proof. In the base case where $n = 0$. $P(m)$ is true for all natural numbers $m \leq 0$. Therefore the base case is done. Now uppose inductively that if $P(n)$ is true then $P(m)$ is ture for all natural numbers $m \leq n$. Then as to $n{+}{+}$. If $P(n{+}{+})$ is true, then $P(n)$ is alo true. So $P(m)$ is true for all natural numbers $m \leq n$. Thus, $P(m)$ is true for all natural numbers $m \leq n{+}{+}$. This close the induction. □

3.3 Multiplication

In the previous section, we have proved all the basic facts we know to be true of addition and order. To save space, we will use these rules without any further comment. For example, we may write $a + b + c = c + b + a$ without any further justification.
Now we introduce multiplication. Same as the previous one that addition is repeated increment, multiplication is repeated addition.

Definition 3.3.1 (Multiplication of natural numbers) Let m be a natural number. To multiply zero to m, we definr $0 \times m := 0$. Now suppose inductively that we have defined how to multiply n to m. Then we can multiply $n{+}{+}$ to m by defining $(n{+}{+}) \times m := (n \times m) + m$.

Verify The product of two natural numbers is a natural number

Proof. We use induction. In the base case where $n = 0$, by definition $0 \times m = 0$ is a natural number. Now suppose inductively that $n \times m$ is a natural number. Then as to $n{+}{+}$, $(n{+}{+}) \times m = (n \times m) + m$ is also a natural number since the sum of two natural numbers is stil a natural number. This closes the induction and thus the product of two natural numbers is a natural number □

Lemma 3.3.1 (Multiplication is commutative) Let n, m be natural numbers. Then $n \times m = m \times n$.

Proof. We first porve that $m \times 0 = 0$. We use induction. In the base case where $m = 0$, by definition of multiplication $0 \times 0 = 0$. Now suppose inductively that $m \times 0 = 0$ then as to m++ $(m\text{++}) \times 0 = m \times 0 + 0 = 0 + 0 = 0$. This closes induction and thus for any natural number m we have $m \times 0 = 0$
We hten prove that $n \times (m\text{++}) = n \times m + n$. We also use induction. In the base case where $n = 0$, we have $0 \times (m\text{++}) = 0 = 0 \times m + 0$. Now suppose inductively that $n \times (m\text{++}) = n \times m + n$, then as to n++ we have:

$$\begin{aligned}(n\text{++}) \times (m\text{++}) &= [n \times (m\text{++})] + (m\text{++}) \\ &= n \times m + n + (m\text{++}) \\ &= n \times m + n + m + 1 \\ &= n \times m + m + (n\text{++}) \\ &= (n\text{++}) \times m + (n\text{++})\end{aligned}$$

This closes the induction and thus for any natural numbers m, n weh have $n \times (m\text{++}) = n \times m + n$.
Finally we prove the commutative law. Again we use the induction by fixing m. In the base case $0 \times m = m \times 0$ is true since both side of the equation is 0. Now suppose inductively that $n \times m = m \times n$. Then as to n++, we have:

$$\begin{aligned}(n\text{++}) \times m &= n \times m + m \\ &= m \times n + m \\ &= m \times (n\text{++})\end{aligned}$$

This closes the induction and thus multiplication is commutative. □

We will now abbreviate $n \times m$ as nm, and use the usual convention that multiplication takes precedence over addition, thus for instance $ab + c$ means $(a \times b) + c$, not $a \times (b + c)$.[1]

Lemma 3.3.2 Let n, m be natural numbers. Then $n \times m = 0$ iff at least one of n, m is equal to zero. In particular, if n and m are both positive then nm is also positive.

Proof. We first prove the second lemma that if n and m are both positive then nm is also positive. We use induction by fixing m. In the base case where $n = 1$, $1 \times m = m$ is positive. Therefore the base case is done. Now suppose inductively that nm is positive, then as to $(n\text{++})m = nm + m$ is also positive because m is positive. This closes the induction. And hence for all positive number m and n, nm is positive.
We then prove that if $nm = 0$ then at least one of n, m is equal to zero. Suppose for the sake of contradiction that $m \neq 0$ and $n \neq 0$. Then nm is positive, a contradiciton. Thus $n = 0$ or $m = 0$. □

Proposition 3.3.1 (Distribution law) For any natural numbers a, b, c, we have $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Proof. As to $a(b + c) = ab + ac$,we use induction. In the base case where $a = 0$, we have $0 \times (b + c) = 0 = 0 + 0 = 0 \times b + 0 \times c$. Now suppose inductively that $a(b + c) = ab + ac$. Then as to a++, we have:

$$\begin{aligned}(a\text{++}) \times (b + c) &= a \times (b + c) + b + c \\ &= a \times b + a \times c + b + c \\ &= (a\text{++}) \times b + (a\text{++}) \times c.\end{aligned}$$

This closes the induction and thus we have $a(b + c) = ab + ac$ for any natural numbers a, b, c.
Then apply commutative law of multiplication, we have $(b + c)a = ba + ca$. □

Proposition 3.3.2 (Multiplication is associative) For any natural numbers a, b, c, we have $(a \times b) \times c = a \times (b \times c)$.

Proof. We use induction by fixing a and b. In the base case where $c = 0$, $ab \times 0 = a \times (b \times 0)$ which is true becasue both side is 0. Now suppose inductively that $(a \times b) \times c = a \times (b \times c)$. Then as to c++, we have:

$$\begin{aligned}(a \times b) \times (c\text{++}) &= (a \times b) \times c + a \times b \\ &= a \times (b \times c) + a \times b \\ &= a \times (b \times c + b) \\ &= a \times [b \times (c\text{++})]\end{aligned}$$

This closes the induction and thus multiplication is associative. □

[1] In oreder to save on using parentheses, we will also use usual notational conventions of precedence.

Proposition 3.3.3 (Multiplication preserves order) If a, b are natural numbers such that $a < b$, and c is positive, then $ac < bc$.

Proof. Since $a < b$, there is a positive number d sunc that $b = a + d$. Then by distribution law, we have $bc = (a + d)c = ac + dc$. By Lemma 3.3.2, dc is positive. Thus $ac < bc$. □

Corollary 3.3.1 (Cancellation law) Let a, b, c be natural numbers such that $ac = bc$ and c is non-zero. Then $a = b$.

Proof. By trichotomy of order for natural numbers, we have that exactly one of the following statement is true (1) $a < b$, (2) $a = b$, (3) $a > b$ when $ac = bc$ and $c \neq 0$. If $a > b$ then $ac > bc$, a contradiciton. If $a < b$, then $ac < bc$, ridiculous. Thus the only possible result is $a = b$. □

Since in any event we can always use $n + 1$ instead of n++, we will rarely see this primitive notion from now on.

Proposition 3.3.4 (Euclidean algorithm) Let n be a natural number, and let q be a positive number. Then there exist natural numbers m, r such that $0 \leq r < q$ and $n = mq + r$.

Remark 3.3.1 In other words, we can divide a natural number n by a positive number q to obtain a quotient m (which is another natural number) and a remainder r (which is less than q). This algorithm marks the beginning of number theory, which is a beautiful and important subject but one which iis beyond the scope of this text.

Proof. We use induction on n. In the base case where $n = 0$, we have $0 = 0 \times q + 0$. Hence the base case is done. Now suppose inductively that $n = mq + r$ then as to n++ we have $n\text{++} = mq + r + 1$. Since $0 \leq r < q$, there are two cases (1) $r\text{++} < q$, (2) $r\text{++} = q$. In the first case, we have $n = mq + (r\text{++})$. In the second case, we have $n = mq + q = (m + 1)q + 0$. Hence both of the two cases satisfy the requirement. This closes the induction. □

Via the same method, we can define exponentiation:

Definition 3.3.2 (Exponentiation for natural numbers) Let m be a natural number. To raise m to the power 0, we define $m^0 := 1$.[1] Now suppose inductively that m^n has benn defined for some natural number n then we define $m^{n\text{++}} := m^n \times m$.

Example 3.3.1 $x^1 = x^0 \times x = 1 \times x = x$; $x^2 = x^1 \times x = x \times x$; $x^3 = x^2 \times x = x \times x \times x$; and so forth.

We will not develop the theory of exponentiation too deeply here, but instead wait until we have defined the integers and rational numbers.

[1] When it comes to zero, some authors define $0^0 = 1$, whereas others leave it undefined.

Chapter 4

Integers and Rationals

In the previou chapter, we have well-defined the natural number via the Peano Axioms. Now we are going to expand our numbers. Before we actually performing the expansion, I would like to say something on th expansion itself. First, to some philosophical issue, once you expand the numbers, as the cost, the new defined numbers will lose some property. Second, I wish to talk about how we expand our numbers. First, we define. Then we verity the well-definedness. Finally, we give the related algebraic laws.

4.1 The integers

$$\mathbb{N} \longrightarrow \underset{\text{You Are Here}}{\mathbb{Z}} \longrightarrow \mathbb{Q}$$

In order to define integers, we need to first define the substraction as well. Then we are facing a problem. We need substraction to define integers; we need integers to define substraction. In order to avoid circularity, we do the following steps. We first define integers by a 'fake' substraction, for example, $a\text{—}b$. We then define subtraction($a - b$) via the integers. Finally, we prove that $a\text{—}b$ is equivalent to $a - b$ so we can discard the notation $a\text{—}b$. Now we begin our expansion by defining the integers.

Definition 4.1.1 (Integers) An integer is an expression of the form $a\text{—}b$, where a and b are natural numbers. Two integers are considered to be equal, $a\text{—}b = c\text{—}d$ iff $a+d = b+c$. We let $\mathbb{Z}$ to denote the set of all integers.

Since we have defined the condition of equality for integers we need to verify the Reflexive Axiom, Symmetry Axiom and Transitive Axiom of equality. And once an operation is defined, we need to verify the Substituttion Axiom. Only in this way can we show that the equality of the integers is well-defined.

Verify (Equality of the integers is well-defined) For any three integers $a\text{—}b$, $c\text{—}d$ and $e\text{—}f$. These following statements are true:

- (Reflexive Axiom) $a\text{—}b = a\text{—}b$;
- (Symmetry Axiom) If $a\text{—}b = c\text{—}d$, then $c\text{—}d = a\text{—}b$;
- (Transitive Axiom) If $a\text{—}b = c\text{—}d$ and $c\text{—}d = e\text{—}f$, then $a\text{—}b = e\text{—}f$.

Proof.
(Reflexive Axiom) Because $a + b = b + a$ therefore, $a\text{—}b = a\text{—}b$.
(Symmetry Axiom) Since $a\text{—}b = c\text{—}d$, $a + d = b + c$. Thus, $d + a = c + b$, i.e. $c\text{—}d = a\text{—}b$.
(Transitive Axiom) Becaue $a\text{—}b = c\text{—}d$ and $c\text{—}d = e\text{—}f$, we have $a + d = b + c$ and $d + e = c + f$. Then $a + d + c + f = b + c + d + e$, so $a + f = b + e$ via the Cancellation Law. Therefore, we have $a\text{—}b = e\text{—}f$. □

Now we define addition and multiplication of integers.

Definition 4.1.2 (Addition and multiplication of integers)

$$(a\text{—}b) + (c\text{—}d) := (a + c)\text{—}(b + d)$$
$$(a\text{—}b) \times (c\text{—}d) := (ac + bd)\text{—}(ad + bc)$$

As we have discussed, we need to first verify that addition and multiplication obey the Substitution Axiom.

Verify (Substitution law for addition and multiplication) Let $a—b$, $a'—b'$ and $c—d$ be any integers. If $a—b = a'—b'$, then:

- $(a—b) + (c—d) = (a'—b') + (c—d)$
- $(c—d) + (a—b) = (c—d) + (a'—b')$
- $(a—b) \times (c—d) = (a'—b') \times (c—d)$
- $(c—d) \times (a—b) = (c—d) \times (a'—b')$

Proof.

- $(a—b) + (c—d) = (a + c)—(b + d)$ and $(a'—b') + (c—d) = (a' + c)—(b' + d)$. Since $a—b = a'—b'$, $a + b' = b + a'$, $a + b' + c + d = a' + b + c + d$. Therefore $(a + c)—(b + d) = (a' + c)—(b' + d)$. Hence, $(a—b) + (c—d) = (a'—b') + (c—d)$.
- $(c—d) + (a—b) = (c + a)—(d + b)$ and $(c—d) + (a'—b') = (c + a')—(b' + d)$. Since $a + b' = b + a'$, $a + b' + c + d = a' + b + c + d$. Therefore, $(c + a)—(d + b) = (c + a')—(b' + d)$. Hence, $(c—d) + (a—b) = (c—d) + (a'—b')$.
- $(a—b) \times (c—d) = (ac+bd)—(ad+bc)$ and $(a'—b') \times (c—d) = (a'c+b'd)—(a'd+b'c)$. Since $a+b' = a'+b$, $(a + b')c + (a' + b)d = (a' + b)c + (a + b')d$. Hence, $ac + bd + a'd + b'c = ad + bc + a'c + b'd$, i.e. $(a—b) \times (c—d) = (a'—b') \times (c—d)$.
- $(c—d) \times (a—b) = (ca+db)—(cb+da)$ and $(c—d) \times (a'—b') = (ca'+db')—(cb'+da')$. Since $a+b' = a'+b$, $c(a + b') + d(a' + b) = c(a' + b) + d(a + b')$. Hence, $ca + db + cb' + da' = ca' + db' + cb + da$, i.e. $(c—d) \times (a—b) = (c—d) \times (a'—b')$. □

Since the integers are the expand of the natural numbers, we need to point out the integer form of the natural numbers. To do this, we first give the integer notation of the natural numbers. Then we verify the Peano Axioms on this notation.
It is not difficult or even obvious to find that $n—0$ should be the integer notation of the natural number n since $(n—0) + (m—0) = \mathbf{(n+m)}—0$ and $(n—0) + (m—0) = \mathbf{(nm)}—0$ where the part in bold is exactly the addition and multiplication of the natural numbers with the other part unchanged. So we can let:

Definition 4.1.3 (The value of integer with the form *n*—0) $n—0 := n$.

We don not have to verify the Peano Axioms with this notation since they ***are*** the naural numbers.
So we can let $n \equiv n—0$ to associate the natural number n with its integer form. And from now on, we will use the natural number notation instead of the integer notation wherever possible to avoid unnecessary writing. For example, we use 5 instead of 5—0.
We have already worked enough on the integers, now we are going to define substraction. Similar to the increment and addition, we try to break substraction into 'sub-operation's. And in fact, it is easy to break the notation $a - b$ into $a + (-b)$, i.e. substraction is the complex of addition(+) and negation(−). We now give the definition:

Definition 4.1.4 (Negation of integers) If $(a—b)$ is an integer, we define the negation $-(a—b) := (b—a)$. In particular $-n := 0—n$ for all natural number n.

As usual, since negation is an operation, we need to verify the Substitution Axiom.

Verify (Negation is well-defined) If $a—b = a'—b'$, then $-(a—b) = -(a'—b')$.

Proof. $-(a—b) = b—a$ and $-(a'—b') = b'—a'$. Since $a + b' = b + a'$ then $b—a = b'—a'$. Thus, $-(a—b) = -(a'—b')$. □

Clearly,

Lemma 4.1.1 $(-1) \times a = -a$

Proof. Let $a = x—y$, then:
$(-1) \times a = [-(1—0)] \times (x—y) = (0—1) \times (x—y) = y—x = -(x—y) = -a$ □

Lemma 4.1.2 $(-1) \times (-1) = 1$

Proof. $(-1) \times (-1) = (0—1) \times (0—1) = (0 \times 0 + 1 \times 1)—(0 + 1 \times 0) = 1—0 = 1$ □

Now we can show that the integers we defined behave just in the way we expect.

Lemma 4.1.3 (Trichotomy of integers) Let x be an integer. Then exactly one of the following statements is true: (a) x is zero; (b) x is equal to a positive natural number n; (c) x is the negation of a positive natural number n.

Proof. We first show that at least one of $(a), (b), (c)$ is true. By definition, $x = a—b$ for some natural numbers a, b. Then we have three cases: $a > b,\ a = b,\ a < b$. If $a > b$, then $a = b + c$ for some positive natural number c. Thus, $a—b = c—0 = c$, which is (b). If $a = b$, then $a—b = a—a = 0—0 = 0$, which is (a). If $a < b$, then $b > a$ which means $b—a = n$ for some positive natural number n. Then $a - b = -(b—a) = -n$.
We then show that no more than one of $(a), (b), (c)$ can hold at the same time. By definition, positive natural numbers are non-zero, so (a) and (b) can not be held at the same time. If (a) and (c) were simultaneously true, then $0 = -n$ for some positive natural number n. Thus $0—0 = 0—n$ so that $0 + 0 = 0 + n$ which shows that $n = 0$ a contradiction. If (b) and (c) were true at the same time, then $n = -m$, so that $n+m = 0+0 = 0$, a contradiction since $m + n$ is positive and therefore it is non-zero. Thus exactly one of $(a), (b), (c)$ is true for any integer x. □

If we have this definition:

Definition 4.1.5 If n is a positive natural number then we call $-n$ a negative integer.

Then for every integer is either positive, zero or negative.

Remark 4.1.1 The reason why we don't use this to define the integers is because if we do so, then for every rules of adition and multiplication we have to split it into many cases and their verification will be too messy.

We now summerize the algebraic properties of the integers.

Proposition 4.1.1 (Laws of algebra for integers) Let $x,\ y,\ z$ be integers, then we have:

$$\begin{aligned} x + y &= y + x \\ (x + y) + z &= x + (y + z) \\ x + 0 = 0 + x &= x \\ x + (-x) = (-x) + x &= 0 \\ xy &= yx \\ (xy)z &= x(yx) \\ x1 = 1x &= x \\ x(y + z) &= xy + xz \\ (y + z)x &= yx + zx \end{aligned}$$

Remark 4.1.2 The above set of nine identities have a name; they are asserting that the integers form a commutative ring. (If one deleted the identity $xy = yx$, then they could only asert the integers form aa ring). Although we have proved all these identities for the natural numbers, we still need to prove them for the integers since $\mathbb{N} \subseteq \mathbb{Z}$. in fact we need many of the propositions derived earlier for natural number to prove these identities.

Proof. Let $x = a—b$, $y = c—d$, $z = e—f$, where a, b, c, d, e are any natural numbers:

- $x + y = (a—b) + (c—d) = (a + c)—(b + d)$;
  $y + x = (c—d) + (a—b) = (c + a)—(d + b) = (a + c)—(b + d)$.
  Thus, $x + y = y + x$.

- $(x+y)+z = [(a—b)+(c—d)]+(e—f) = [(a+c)—(b+d)]+(e—f) = (a+c+e)—(b+d+f)$;
  $x+(y+z) = (a—b)+[(c—d)+(e—f)] = (a—b)+[(c+e)+(d+f)] = (a+c+e)—(b+d+f)$;
  Thus, $(x+y)+z = x+(y+z)$.

- $x+0 = (a—b)+(0—0) = a—b = x$. Then by $x+y = y+x$ which we have just proved, we have $0+x = 0$. Hence, $x+0 = 0+x = x$.

- $x+(-x) = (a—b)+(b—a) = (a+b)-(a+b) = 0—0 = 0$. Then by $x+y = y+x$ which we have just proved, we have $(-x)+x = 0$. Hence, $x+(-x) = (-x)+x = 0$.

- $xy = (a—b)\times(c—d) = (ac+bd)—(ad+bc)$;
  $yx = (c—d)\times(a—b) = (ca+db)—(cb+da)$.
  Thus, $xy = yx$.

- $$\begin{aligned}(xy)z &= [(a—b)\times(c—d)]\times(e—f) = [(ac+bd)—(ad+bc)]\times(e—f)\\ &= (ace+bde+adf+bcf)—(acf+bdf+ade+bce);\\ x(yz) &= (a—b)\times[(c—d)\times(e—f)] = (a—b)\times[(ce+df)—(cf+de)]\\ &= (ace+adf+bcf+bde)—(acf+ade+bce+bdf).\end{aligned}$$
  Thus, $(xy)z = x(yx)$.

- $x1 = (a—b)\times(1—0) = a—b = x$. Then by $xy = yx$ which we have just proved, we have $1x = x$. Hence, $x1 = 1x = x$.

- $$\begin{aligned}x(y+z) &= (a—b)\times[(c—d)+(e—f)] = (a—b)\times[(c+e)—(d+f)]\\ &= (ac+ae+bd+bf)—(ad+af+bc+be);\\ xy+xz &= (a—b)\times(c—d)+(a—b)\times(e—f) = (ac+bd)—(ad+bc)+(ae+bf)—(af+be)\\ &= (ac+ae+bd+bf)—(ad+af+bc+be).\end{aligned}$$
  Thus, $x(y+z) = xy+xz$

- By $xy = yx$ which we have just proved, we have $x(y+z) = (y+z)x$ and $xy+xz = yx+zx$. Thus, $(y+z)x = yx+zx$. □

As all the preparations are done, we now give the definition of substraction.

Definition 4.1.6 (Substration) The operation of substraction $x-y$ of two integers is defined by the formula: $x-y := x+(-y)$

Now we try to 'merge' $a—b$ with $a-b$:

Lemma 4.1.4 $a-b$=$a—b$.

Proof. $a-b = a+(-b) = (a—0)+[-(b—0)] = (a—0)+(0—b) = a—b$. □

So we can now discard the '—' notation and use '−' instead.
Now we can generalize some of the propositions of the natural numbers for the integers.

Proposition 4.1.2 (Integers have no zero divisors) Let a and b be integers such that $ab = 0$ then either $a = 0$ or $b = 0$.

Proof. We first prove that if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$. By the trichotomy of integers, there exits two positive natural numbers α, β such that exactly one of the statements $a = \alpha$ or $a = -\alpha$ is true and exactly one of the statemenents $b = \beta$ or $b = -\beta$ is true.
Then there are two cases: $ab = \alpha\beta$ and $ab = -\alpha\beta$. Since α and β are both positive, then $\alpha\beta$ is positive and $\alpha\beta \neq 0$. Then $-\alpha\beta \neq 0$ by trichotomy of integers. Therefore, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$. Hence, if $ab = 0$ then either $a = 0$ or $b = 0$. □

Corollary 4.1.1 (Cancellation law for integers) If a, b, c are integers such that $ac = bc$ and c is non-zero, then $a = b$.

Proof. Since $ac = bc$, then $ac-bc = bc-bc = c[b+(-b)] = 0$. Therefore, $(a-b)c = 0$. Because, c is non-zero. We have $a-b = 0$, hence $a-b+b = 0+b$ thus $a = b$ □

We now extend the notion of order, which was defined on the natural numbers, to the integers by repeating the definition verbatim:

Definition 4.1.7 (Order of the integers) Let n and m be integers. We say that n is greater than or equal to m and write $n \geq m$ or $m \leq n$ iff we have $n = m + a$ for some natural number a. We say that n is strictly greater than m, and write $n > m$ or $m < n$, iff $n \geq m$ and $n \neq m$.

For example, $5 > -3$ because $8 + (-3) = 5$ and $5 \neq -3$. Also, it is obvious that this notion is consistent with the notion of order on the natural numbers since we are using the same definition.
We then generalize the properties of order for the integers.

Proposition 4.1.3 (Properties of order) Let a, b, c be integers.

(a) $a > b$ iff $a - b$ is a positive natural number.

(b) (Addition preserves order) If $a > b$, then $a + c > b + c$.

(c) (Positive multiplication perserves the order) If $a > b$ and c is positive, then $ac > bc$.

(d) (Negation reverses the order) If $a > b$ then $-a < -b$.

(e) (Order is transitive) If $a > b$ and $b > c$, then $a > c$.

(f) (Order trichotomy) Exactly one of the statements $a > b$, $a < b$, or $a = b$ is true.

Proof.

(a) We first prove that if $a > b$ then $a - b$ is a positive natural number. Since $a > b$ and $a = b + (a - b)$, $a - b$ is a natural number and $a \neq b$. Then $a - b$ is non-zero. Thus $a - b$ is a positive natural number.
We then frove that if $a - b$ is a positive natural number then $a > b$. Since $a - b$ is a positive natural number and $a = b + (a - b)$, $a \geq b$. Because $a - b$ is positive, $a - b \neq 0$. Therefore $a \neq b$. Hence, $a > b$.
In all $a > b$ iff $a - b$ is a positive natural number.

(b) Because $a > b$, $a = b + r$ of a positive natural number r. Then $a + c = b + c + r$ by adding c to both sides. Hence, $(a + c) = (b + c) + r$. Therefore, $a + c > b + c$ for r is a positive natural number.

(c) Because $a > b$, there exits a positive natural number r such that $a = b + r$. By multiplying a positive natural number c to both side, $ac = (b + r)c = bc + rc$ with rc is positive. Thus, $ac > bc$.

(d) Because $a > b$, there exits a positive natural number r such that $a = b + r$. By multiplying a negative number $-c$ to both side where c i a positive natural number, $a(-c) = (b + r)(-c) = b(-c) - rc$ with rc is positive. Then $a(-c) + rc = b(-c)$. Hence, $a(-c) < b(-c)$.

(e) Because $a > b$ and $b > c$, there exist two positive natural numbers r and r' such that $a = b + r$ and $b = c + r'$. Then $a = c + r + r'$, so $a > c$ for $r + r'$ is also positive.

(f) Since a and b are both integers, then $a - b$ is also a integer. Then by trichotomy of integers, at exactly one of the following statements is true: (a) $a - b$ is zero; (b) $a - b$ is equal to a positive natural number n; (c) $a - b$ is the negation of a positive natural number n.
In case (a), we get $a = b$. In case (b), we have $a - b = n$ then $a = b + n$ where n is positive. Hence $a > b$.
In case (c), we have $a - b = -n$ then $a + n = b$ where n is positive. Hence $b > a$.
Since by trichotomy of integers exactly one of the statements is true. Then exactly one of the statements $a > b$, $a < b$, or $a = b$ is true. □

Finally, we should point out that the principle of mathematical induction does not apply directly to the integers. More precisely, we can give an example of a property $P(n)$ pertaining to an integer n such that $P(0)$ is true, and that $P(n)$ implies $P(n{+}{+})$ for all integers n, but that $P(n)$ is not true for all integers n. Thus induction is not as useful a tool for dealing with the integers as it is with the natural numbers. In fact, the situation becomes even worse with the rational numbers and real numbers which will be discussed later.
For example, we define $P(n)$ that $n + 1 > 0$. $P(0)$ is true since $0 + 1 = 1 > 0$. Now suppose inductively that $n + 1 > 0$ then as to $P(n + 1)$, $n + 1 + 1 = n + 2 > 0$. Then $P(n)$ is true for all integers. This is **NOT** true becsue when $n = -2$, $(-2) + 1 = -1 < 0$.

4.2 The rationals

$$\mathbb{N} \longrightarrow \mathbb{Z} \longrightarrow \underset{\text{You Are Here}}{\mathbb{Q}}$$

We have successfully constructed the integers with the operations of addition, substraction, muliplication, and order and verified all the expected algebraic and order-theoretic properties. Now we will sue the similar method to build the rationals by introducing division.
Just like what we did to the integers, we will first define rationals as '$a//b$' then define division as 'a/b' by first define reciprocal 'a^{-1}' finally we prove that $a//b$ is the same as a/b.
Obviouly in the notion '$a//b$', b should be non-zero or the rationals we will construct would not be self-consistent because we cannot have $(a/b) \times b = a$ and $c \times 0 = 0$ to be simultaneously true. So we define:

Definition 4.2.1 (Rationals) A rational is an experssion of the form $a//b$, where a and b are integers and b is non-zero; $a//0$ is not considered to be a rational number. Two rationals are considered equal $a//b = c//d$ iff $ad = bc$. The set of all rational numbers is denoted as $\mathbb{Q}$.

Now we hould verify that the definition of equality is valid.

Verify (Equality of the integers is well-defined) For any three rationals $a//b$, $c//d$ and $e//f$. These following statements are true:

- (Reflexive Axiom) $a//b = a//b$;
- (Symmetry Axiom) If $a//b = c//d$, then $c//d = a//b$;
- (Transitive Axiom) If $a//b = c//d$ and $c//d = e//f$, then $a//b = e//f$.

Proof.

- (Reflexive Axiom) Because $ab = ba$ therefore, $a//b = a//b$.
- (Symmetry Axiom) Since $a//b = c//d$, $ad = bc$. Thus, $da = cb$, i.e. $c//d = a//b$.
- (Transitive Axiom) Becaue $a//b = c//d$ and $c//d = e//f$, we have $ad = bc$ and $de = cf$. Then $adcf = bcde$, so $af = be$ via the Cancellation Law. Therefore, we have $a//b = e//f$. □

We then define the addition, multiplication and negation of rationals.

Definition 4.2.2 (Addition, multiplication and negtion of rationals) If $a//b$ and $c//d$ are rational numbers, we define their sum, product and negation:

$$\begin{aligned}(a//b) + (c//d) &:= (ad + bc)//(bd)\\ (a//b) \times (c//d) &:= (ac)//(bd)\\ -(a//b) &:= (-a)//b.\end{aligned}$$

Now we verify that these definitions are well-defined.

Verify For three rationals $a//b$, $a'//b'$ and $c//d$. If $a//b = a'//b'$, then these flowing three statements are true.

- $(a//b) + (c//d) = (a'//b') + (c//d)$
- $(a//b) \times (c//d) = (a'//b') \times (c//d)$
- $(c//d) + (a//b) = (c//d) + (a'//b')$
- $(c//d) \times (a//b) = (c//d) \times (a'//b')$
- $-(a//b) = -(a'//b')$

Proof. Because $a//b = a'//b'$, $ab' = a'b$.

- $(a//b) + (c//d) = (ad + bc)//(bd)$
  $(a'//b') + (c//d) = (a'd + b'c)//(b'd)$
  Since $b'd(ad + bc) = ab'd^2 + bb'dc = a'bd^2 + bb'dc = bd(a'd + b'c)$,
  $(a//b) + (c//d) = (a'//b') + (c//d)$.
- $(a//b) \times (c//d) = (ac)//(bd)$
  $(a'//b') \times (c//d) = (a'c)//(b'd)$
  Since $ab'cd = a'bcd$, $(a//b) \times (c//d) = (a'//b') \times (c//d)$
- $(c//d) + (a//b) = (ad + bc)//(bd)$
  $(c//d) + (a'//b') = (a'd + b'c)//(b'd)$
  Since $b'd(ad + bc) = ab'd^2 + bb'dc = a'bd^2 + bb'dc = bd(a'd + b'c)$,
  $(c//d) + (a//b) = (c//d) + (a'//b')$.
- $(c//d) \times (a//b) = (ac)//(bd)$
  $(c//d) \times (a'//b') = (a'c)//(b'd)$
  Since $ab'cd = a'bcd$, $(c//d) \times (a//b) = (c//d) \times (a'//b')$.
- $-(a//b) = (-a)//b$
  $-(a'//b') = (-a')//b'$
  Since $-ab' = -a'b$, $-(a//b) = -(a'//b')$ □

Now we find that $a//1$ behaves the same as integers, since:

- $(a//1) + (b//1) = (a + b)//1$
- $(a//1) \times (b//1) = (ab)/1$
- $-(a//1) = (-a)//1$
- $(a//1) = (b//1)$ iff $a = b$

Thus, we let:

Definition 4.2.3 (The value of the rationals with the form $a//1$) $a//1 := a$

We do not have to verify all the properties of integers since the identities above can guarantee the consistence of integers with rationals. From this we can also infer that $\mathbb{Z} \subset \mathbb{R}$. More generally, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{R}$
Also, here is some lemmae worth talking about.

Lemma 4.2.1 For a rational x, $x \times (-1) = -x$.

Proof. Let $x = a//b$.
$x \times (-1) = (a//b) \times (-1//1) = (-a)//b = -x$. □

Corollary 4.2.1 $-(-x) = x$.

Proof. Let $x = a//b$. $-(-x) = -[(-a)//b] = [-(-a)]//b = a//b = x$. □

Now we introduce a new operation, reciprocal:

Definition 4.2.4 (Recipeocal of rationals) If $x = a//b$ is non-zero, i.e. $a \neq 0$, then the reciprocal of x, $x^{-1} := b//a$.

As to this new operation, we should check the substitution axiom. Also, we should note that we leave 0^{-1} undefined.

Verify (Recipeocal is well-defined) If $a//b = a'//b'$, then $(a//b)^{-1} = (a'//b')^{-1}$.

Proof. SInce $a//b = a'//b'$ then $ab' = a'b$. Therefore, $b//a = b'//a'$, i.e. $(a//b)^{-1} = (a'//b')^{-1}$. □

Since all of the preparation work has been done, we now summerize the algebraic properties of the rationals.

Proposition 4.2.1 (Laws of algebra for rationals) Let x, y, z be rationals. Then the following laws of algebra hold:

$$\begin{aligned} x+y &= y+x \\ (x+y)+z &= x+(y+z) \\ x+0 &= 0+x = x \\ x+(-x) &= (-x)+x = 0 \\ xy &= yx \\ (xy)z &= x(yz) \\ x1 &= 1x = x \\ x(y+z) &= xy+xz \\ (y+z)x &= yx+zx \\ xx^{-1} &= x^{-1}x = 1 \quad \text{if } x \text{ is non-zero.} \end{aligned}$$

Proof. Let $x = a//b$, $y = c//d$, $z = e//f$.

- $x + y = (a//b) + (c//d) = (ad + bc)//(bd)$;
  $y + x = (c//d) + (a//b) = (cb + da)//(db) = (ad + bc)//(bd)$.
  Therefore, $x + y = y + x$.
- $(x + y) + z = (ad + bc)//(bd) + e//f = (adf + bcf + bde)//(bdf)$;
  $x + (y + z) = a//b + (cf + de)//(df) = (bcf + bde + adf)//(bdf)$.
  Therefore, $(x + y) + z = x + (y + z)$.
- $x + 0 = (a//b) + (0//1) = (a \times 1 + 0 \times b)//(b \times 1) = a//b = x$;
  $0 + x = x + 0$ by $x + y = y + x$.
  Therefore, $x + 0 = 0 + x = x$.
- $x + (-x) = (a//b) + [(-a)//b)] = [ab + (-ab)]//(b^2) = 0//b^2 = 0//1 = 0$;
  $(-x) + x = x + (-x)$ by $x + y = y + x$.
  Therefore, $x + (-x) = (-x) + x = 0$.
- $xy = (a//b) \times (c//d) = (ac)//(bd)$;
  $yx = (c//d) \times (a//b) = (ca)//(db) = (ac)//(bd)$.
  Therefore, $xy = yx$.
- $(xy)z = (ac//bd) \times (e//f) = ace//bdf$;
  $x(yz) = (a//b) \times (ce//df) = ace//bdf$.
  Therefore, $(xy)z = x(yz)$.
- $x1 = (a//b) \times (1//1) = a//b = x$;
  $1x = x1$ by $xy = yx$.
  Therefore, $x1 = 1x = x$.
- $x(y + z) = a//b \times (cf + de)//(df) = (acf + ade)//(bdf)$;
  $xy + xz = (ac)//(bd) + (ae)//(bf) = (acbf + abde)//(b^2dbf) = (acf + ade)//(bdf)$;
  Therefore, $x(y + z) = xy + xz$.
- By $xy = yx$ and $x(y + z) = xy + xz$, $(y + z)x = yx + zx$.
- When $x \neq 0$, i.e., $a \neq 0$, $xx^{-1} = (a//b) \times (b//a) = (ab)//(ab) = 1//1 = 1$;
  $x^{-1}x = xx^{-1}$ by $xy = yx$.
  Therefore, $xx^{-1} = x^{-1}x = 1$ □

Remark 4.2.1 The above ten propreties asserts that the rationals $\mathbb{Q}$ form a field. This i better than being a commutative ring because we have the tenth property $xx^{-1} = x^{-1}x = 1$.

We can now define the quotient of two rationals:

Definition 4.2.5 (Quotient of rationals) Given two rational numbers x and y, and y is non-zero. Then:

$$x/y = x \times y^{-1}.$$

Therefore, we can now discard the notion $a//b$.

Lemma 4.2.2 For every integer a and every non-zero integer b, $a/b = a//b$.

Proof. $a/b = a \times b^{-1} = (a//1) \times (b//1)^{-1} = (a//1) \times (1//b) = a//b$. □

In the similar spirit, we can define substraction.

Definition 4.2.6 (Substraction of rationals) $x - y := x + (-y)$.

As to substraction, we give some properties about it.

Lemma 4.2.3 For any rational x, y, z:

$$\begin{aligned}-(x-y) &= y - x;\\ -(x+y) &= (-x) + (-y) = -x - y;\\ -x - y &= -y - x;\end{aligned}$$

Proof.

- $-(x-y) = (-1) \times [x + (-y)] = (-1) \times x + (-1) \times (-y) = -x + [-(-y)] = y + (-x) = y - x$
- $-(x+y) = (-1) \times (x+y) = (-1) \times x + (-1) \times y = (-x) + (-y) = -x - y$
- $-x - y = -(x+y) = -(y+x) = -y - x$ □

In the previous section we organized all the integers into positive, zero and negative numbers. We now do the same for the rationals.

Definition 4.2.7 (Positive and negative rationals) A rational number number x is said to be positive iff we have $x = a/b$ for some positive integers a and b. It is said to be negative iff we have $x = -y$ for some positive rational y (i.e., $x = (-a)/b$ for some positive integers a and b).

This definition is consistent with the previous one because every positive integer is a positive rational and every negative integer is a negative rational.

Lemma 4.2.4 (Trichotomy of rationals) Let x be a rational number. Then exactly one of the following statements is true: (a) x is equal to 0. (b) x is positive rational number. (c) x is a negative rational number.

Proof. We first show that at last one of the statements is true.
By definition $x = a//b$ for some integers a, b and $b \neq 0$. According to trichotomy of integers, we have two major cases $a = 0$ and $a \neq 0$. If $a = 0$ then $x = a//b = 0//b = 0//1 = 0$. If $a \neq 0$ then there are four minor cases: (1), $a > 0$ and $b > 0$. (2), $a > 0$ and $b < 0$. (3), $a < 0$ and $b > 0$. (4), $a < 0$ and $b < 0$.

(1) By definition, if $a > 0$ and $b > 0$ then $x = a//b$ is positive.

(2) Since $a > 0$ and $b < 0$ then $b = -b'$ for some positive integer b'. Thus, $x = a//b = a//(-b') = (-a)//b'$ is negative by definition.

(3) Since $a < 0$ and $b > 0$ then $a = -a'$ for some positive integer a'. Thus, $x = a//b = (-a')//b$ is negative by definition.

(4) Since $a < 0$ and $b < 0$ then $a = -a'$ and $b = -b'$ for some positive integer a' and b'. Thus, $x = a//b = (-a')//(-b') = a'//b'$ is positive by definition.

We then prove that no more than one of $(a), (b), (c)$ can be hold at the same time.
If (a) and (b) are true at the same time, then $a//b = 0//1$ with positive integers a and b then $a = 0$, a contradiction by trichotomy of integers.
If (a) and (c) are simultaneously true, then $(-a)//b = 0//1$ with positive integers a and b then $-a = 0$. Hence, $a = (-1) \times (-a) = (-1) \times 0 = 0$, another contradiction by trichotomy of integers.
If (b) and (c) are both true, then $a//b = (-a')//b'$ with positive integers a, a', b, b' then $-a'b = ab'$ with $-a'b$ negative and ab' positive, which is impossible.
Therefore, exactly one of $(a), (b), (c)$ is true for any rational x. □

Definition 4.2.8 (Ordering of the rationals) Let x and y be rational numbers. We say that $x > y$ iff $x - y$ is positive rational number, and $x < y$ iff $x - y$ is negative rational number. We write $x \geq y$ iff either $x > y$ or $x = y$, and similarly define $a \leq y$.

Proposition 4.2.2 (Basic peoperties of order on the rationals) Let x, y, z be rational numbers. Then the following properties hold.

(a) (Order trichotomy) Exactly one of the three statements $x > y$, $x = y$, or $x < y$ is true.

(b) (Order is anti-symmetric) One has $x < y$ iff $y > x$.

(c) (Order is transitive) If $x < y$ and $y < z$, then $x < z$.

(d) (Addition perserves order) If $x < y$ then $x + z < y + z$.

(e) (Positive multiplication preserves order) If $x < y$ and z is positive, then $xz < yz$.

(f) (Negative multiplication preserves order) If $x < y$ and z is negative, then $xz > yz$.

We first prove a lemma:

Lemma 4.2.5 For any two integer α and β:

- $\alpha > 0$ iff α is positive.
- $\alpha\beta > 0$ if $\alpha > 0$ and $\beta > 0$.
- $\alpha + \beta > 0$ if $\alpha > 0$ and $\beta > 0$.

Proof.

- For any positive integer α, α is also a positive natural number by definition. Then $\alpha > 0$ because $\alpha - 0 = \alpha + (-0) = \alpha + [-(0—0)] = \alpha + (0—0) = \alpha + 0 = \alpha$ is a positive natural number.
  On the other hand, if $\alpha > 0$ then $\alpha - 0 = \alpha$ is a positive natural number so that α is positive.
- Since $\alpha > 0$ and β is positive, $\alpha\beta > 0\beta = 0$ since any natural number times 0 is 0. Hence, $\alpha\beta > 0$.
- For any positive integer α and β. $\alpha+\beta$ is also positive because α and β are also non-zero natural numbers and the sum of a positive natural number and a natural number is still positive. Thus, $\alpha + \beta > 0$. □

We now prove Proposition 4.2.8.

Proof.

- By trichotomy of rationals, there is exactly one of the statements is true: $x - y > 0$, $x - y = 0$ or $x - y < 0$. If $x - y > 0$ then $x > y$ by definition. If $x - y = 0$ then $x - y + y = 0 + y$ i.e., $x = y$. If $x - y < 0$ then $x < y$ by definition.
  Therefore, exactly one of the three statements $x > y$, $x = y$, or $x < y$ is true.
- We first prove that if $x < y$ then $y > x$. Since $x < y$ then $x - y$ is negative and $x - y = -a$ for some positive rational a. Thus, $y - x = -(x - y) = -(-a) = a$ is positive. Hence, $y > x$
  We then prove that if $y > x$ then $x < y$. Since $y > x$ then $y - x$ is positive and $y - x = b$ for some positive rational b. Then $x - y = -(y - x) = -b$ is negative. Thus, $x < y$.

- Since $x < y$ and $y < z$, $x - y < 0$ and $y - z < 0$. Therefore $x - y = -a$ and $y - z = -b$ for some positive rational $a = a'//a''$ and $b = b'//b''$ where a', a'', b', b'' are positive integers. Then $x - z = x + (-y) + y + (-z) = (x - y) + (y - z) = (-a) + (-b) = -(a + b) = [-(a'b'' + a''b')]//(a''b'')$ is negative by Lemma 4.2.5. Thus $x - z$ is negative and $x < z$.
- Since $x < y$ then $x - y$ is negative. Since $(x + z) - (y + z) = x + z + (-z) + (-y) = x - y$ is negtive. Therefore, $x + z < y + z$.
- Since $x < y$ then $x - y$ is negative. For a positive rational z, $xz - yz = xz + (-1)yz = z(x - y)$. Let $z = a//b$ and $x - y = (-c)//d$ for positive integers a, b, c, d, then $z(x - y) = (-ac)//bd$ is negative because ac and bd are positive by Lemma 4.2.5. Thus, $xz < yz$.
- Since $x < y$ then $x - y$ is negative. For a negative rational z, $xz - yz = xz + (-1)yz = z(x - y)$. Let $z = (-a)//b$ and $x - y = (-c)//d$ for positive integers a, b, c, d, then $z(x - y) = ac//bd$ is negative because ac and bd are positive by Lemma 4.2.5. Thus, $xz > yz$. □

Remark 4.2.2 With above five properties of order and ten algebraic properties on rationals, we can say that $\mathbb{Q}$ forms a ordered field.

4.3 Absolute value and exponentiation

Previously, we rigorously constructured $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ and proved $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{R}$. As to $\mathbb{Q}$, we carefully introduced the four basic arithmetic operations of addition, substracion, multiplication and the notion of order $<$, and gave several algebraic properties and properties of order. In short, we proved that the rationals $\mathbb{Q}$ formed an ordered field.

We can now introduce some more complicated operation via these basic operations. In addition, we don not have to verify the Substitution Axiom of equality for these new operation, because they are all derived from the basic operations which are already well-defined. There are many such operations we can construct, but here we are going to only introduce two operation of particular usage: the absolute value and the exponentiation. Also, we should point out that, since we have already well-defined the four basic operation and given all of their algebraic peoperties, we will not going to use any 'obvious' peoperties (e.g. x is positive iff $x > 0$) with any further comment.

Definition 4.3.1 (Absolute value) If x is a rational number, the absolute value of $|x|$ of x is defined as follows. If x is positive, then $|x| := x$. If x is zero, then $|x| := 0$. If x is negtive, then $|x| := -x$.

Definition 4.3.2 (Distance) Let x and y be rational numbers. The quantity $|x - y|$ is called the distance between x and y and is sometimes denoted as $d(x, y)$.

Proposition 4.3.1 (Basic properties of absolute value and distance) Let x, y, z be rational numbers.

(*a*) (Non-degeneracy of abolute value) We have $|x| \geq 0$. Also, $|x| = 0$ iff $x = 0$.

(*b*) (Triangle inequality for absolute value) We have $|x + y| \leq |x| + |y|$.

(*c*) We have the inequalities $-y \leq x \leq y$ iff $y \geq |x|$. In particular, $-|x| \leq x \leq |x|$.

(*d*) (Multiplicativity of absolute value) We have $|xy| = |x||y|$. In particular $|-x| = |x|$.

(*e*) (Non-degeneracy of distance) We have $d(x, y) \geq 0$. Also, $d(x, y) = 0$ iff $x = y$.

(*f*) (Symmetry of distance) $d(x, y) = d(y, x)$.

(*g*) (Triangle inequality for distance) $d(x, z) \leq d(x, y) + d(y, z)$.

Proof.

(*a*) If $x > 0$, then $|x| = x > 0$. If $x = 0$, then $|x| = 0 = 0$. If $x < 0$, then $|x| = -x > 0$. Therefore, $|x| \geq 0$. By trichotomy of rationals, for $|x| = 0$ then x can be either positive, negative or zero. If x is positive or negative, then $|x| > 0$. Thus, the only possible case is $x = 0$. Hence, $|x| = 0$ iff $x = 0$.

(*b*) Suppose we have proved (*c*). Then $-|x| \leq x \leq |x|$ and $-|y| \leq y \leq |y|$.
Therefore, $-(|x|+|y|) \leq x+y \leq |x|+|y|$. Hence, $|x|+|y| \geq |x+y|$

(*c*) We first prove that $-|x| \leq x \leq |x|$. If $x > 0$, then $-|x| = -x < 0 < x = |x|$. Thus $-|x| \leq x \leq |x|$. If $x = 0$, then $-|0| = 0 = |0|$. Thus, $-|x| \leq x \leq |x|$. If $x < 0$, then $-|x| = -(-x) = x < -x = |x|$. Thus, $-|x| \leq x \leq |x|$.
Then if $y \geq |x|$, then $-y \leq |x|$. Therefore, $-y \leq -|x| \leq x \leq |x| \leq y$. Hence, $-y \leq x \leq y$.
We finally need to show that if $-y \leq x \leq y$ then $|x| \leq y$. If $x > 0$ then $|x| = x \leq y$. If $x = 0$ then $|0| = 0 \leq y$. If $x < 0$ then $y \geq -x \geq -y$ so that $|x| = -x \leq y$. In all if $-y \leq x \leq y$ then $|x| \leq y$. Hence, $-y \leq x \leq y$ iff $y \geq |x|$.

(*d*) If $x = 0$ or $y = 0$ then the left side of the equation equals to $|0| = 0$, and right side of the equation will be $0|y| = 0$, $|x|0 = 0$ or $0 \times 0 = 0$. Therefore the equation is correct. If $x \neq 0$ and $y \neq 0$, then there will be four cases: (1) $x > 0$ and $y > 0$. (2) $x > 0$ and $y < 0$. (3) $x < 0$ and $y > 0$. (4) $x < 0$ and $y < 0$.

(1) $|xy| = xy$ since xy is positive; $|x||y| = xy$. Therefore the equation is correct.
(2) $|xy| = -xy$ since xy is negative; $|x||y| = x(-y) = -xy$. Therefore the equation is correct.
(3) $|xy| = -xy$ since xy is negative; $|x||y| = (-x)y = -xy$. Therefore the equation is correct.
(4) $|xy| = xy$ since xy is positive; $|x||y| = (-x)(-y) = xy$. Therefore the equation is correct.

Thus, in all, $|xy| = |x||y|$ and $|-x| = |-1||x| = |x|$ in particular.[1]

(*e*) $d(x,y) = |x-y| \geq 0$. Also, $d(x,y) = |x-y| = 0$ iff $x - y = 0$ i.e., $x = y$.

(*f*) $d(x,y) = |x-y| = |y-x| = d(y,x)$.

(*g*) $d(x,y) + d(y,x) = |x-y| + |y-z| \geq |x-y+y-z| = |x-z| = d(x,z)$. □

The absolute value is useful for measurng how 'close' two numbers are. Let us make a somewhat artificial definition:

Definition 4.3.3 (ϵ-closeness) Let $\epsilon > 0$ be a rational number, and let x, y be rational numbers. We say that y is ϵ-close to x iff we have $d(x,y) \leq \epsilon$.

Remark 4.3.1 This definition is not standard in mathematics textbooks; we will use it as 'scaffolding' to construct the more important notions of limits (and of Cauchy sequences) later on, and once we have those more advanced notions we will discard the notion of ϵ-close.

In this definition, ϵ is only positive because x and y are equal when $\epsilon = 0$ and x and y can never be ϵ-close when ϵ is negative.
Another thing that worth a comment is that it is a tradition that ϵ and δ should only denote small positive numbers.
We now give some properties of ϵ-closeness.

Proposition 4.3.2 Let x, y, z, w be rational numbers.

(*a*) If $x = y$, then x is ϵ-close to y for every $\epsilon > 0$. Conversely, if x is ϵ-close to y for every $\epsilon > 0$, then we have $x = y$.

(*b*) Let $\epsilon > 0$. If x is ϵ-close to y, then y is ϵ-close to x.

(*c*) Let $\epsilon, \delta > 0$. If x is ϵ-close to y and y is δ-close to z then x and z are $(\epsilon+\delta)$-close.

(*d*) Let $\epsilon, \delta > 0$. If x and y are ϵ-close, z and w are δ-close, then $x+z$ and $y+w$ are $(\epsilon+\delta)$-close, $x-z$ and $y-w$ are also $(\epsilon+\delta)$-close.

(*e*) Let $\epsilon > 0$. If x and y are ϵ-close, they are also ϵ'-close for every $\epsilon' > \epsilon$.

(*f*) Let $\epsilon > 0$. If y and z are both ϵ-close to x, and w is between y and z (i.e., $y \leq w \leq z$ or $z \leq w \leq y$), then w is also ϵ-close to x.

[1] By this way, we can also prove that $|\frac{x}{y}| = \frac{|x|}{|y|}$.

(*g*) Let $\epsilon > 0$. If x and y are ϵ-close, and z is non-zero, then xz and yz are $\epsilon|z|$-close.

(*h*) Let $\epsilon, \delta > 0$ If x and y are ϵ-close, and z and w are δ-close, then xz and yw are $(\epsilon|z| + \delta|x| + \epsilon\delta)$-close.

Proof.

(*a*) If $x = y$ then $|x - y| = 0 < \epsilon$. Therefore, x is ϵ-close to y for every $\epsilon > 0$.
If for every $\epsilon > 0$, $|x - y| < \epsilon$. We try to prove $x = y$. Suppose for the sake of contradiciton that $x \neq y$ then we have $a = x - y$ for a non-zero rational a. Thus, $|x - y| = |a| \neq 0$, so $|x - y| > \frac{1}{2}|a|$. Therefore, x and y are not $\frac{1}{2}|a|$-close, a contradiction. Hence, $x = y$.

(*b*) If x is ϵ-close to y then $|x - y| \leq \epsilon$. Thus, $|y - x| = |x - y| \leq \epsilon$, y is ϵ-close to x.

(*c*) If x is ϵ-close to y and y is δ-close to z, then $|x-y| \leq \epsilon$ and $|y-x| \leq \delta$. Therefore, $|x-z| = |x-y+y-z| \leq |x - y| + |y - z| = \epsilon + \delta$, x and z are $(\epsilon + \delta)$-close.

(*d*) Since x and y are ϵ-close, z and w are δ-close, $|x - y| \leq \epsilon$ and $|z - w| \leq \delta$.
Thus, $|x + z - (y + w)| \leq |x - y| + |z - w| \leq \epsilon + \delta$.
Also, $|x - z - (y - w)| \leq |x - y| + | - (z - w)| = |x - y| + |z - w| \leq \epsilon + \delta$. Hence, $x + z$ and $y + w$ are $(\epsilon + \delta)$-close, $x - z$ and $y - w$ are also $(\epsilon + \delta)$-close.

(*e*) If x are ϵ-close to y and $\epsilon' > \epsilon$. Then $|x - y| \leq \epsilon < \epsilon'$. Therefore, x and y are also ϵ'-close.

(*f*) Since y and z are both ϵ-close to x, $|x - y| \leq \epsilon$ and $|x - z| \leq \epsilon$. Therefore $-\epsilon \leq x - y \leq \epsilon$ and $-\epsilon \leq x - z \leq \epsilon$. Thus, $y - \epsilon \leq x \leq y + \epsilon$ and $z - \epsilon \leq x \leq z + \epsilon$
If $y \leq w \leq z$ then $y - \epsilon \leq w - \epsilon \leq z - \epsilon$ and $y + \epsilon \leq w + \epsilon \leq z + \epsilon$.
Therefore

$$w - \epsilon \leq z - \epsilon \leq x \leq y + \epsilon \leq w + \epsilon.$$

Thus,

$$w - \epsilon \leq x \leq w + \epsilon.$$

Hence,

$$-\epsilon \leq x - w \leq \epsilon$$

so that

$$|x - w| \leq \epsilon.$$

If $z \leq w \leq y$ then $z - \epsilon \leq w - \epsilon \leq y - \epsilon$ and $z + \epsilon \leq w + \epsilon \leq y + \epsilon$
Therefore

$$w - \epsilon \leq y - \epsilon \leq x \leq z + \epsilon \leq w + \epsilon.$$

Thus,

$$w - \epsilon \leq x \leq w + \epsilon.$$

Hence

$$-\epsilon \leq x - w \leq \epsilon$$

so that

$$|x - w| \leq \epsilon.$$

In all, w is ϵ-close to x.

(*g*) If x and y are ϵ-close, then $|x - y| \leq \epsilon$. Then for any non-zero rational z,

$$|zx - zy| = |z||x - y| \leq |z|\epsilon.$$

Therefore, zx and zy are $|z|\epsilon$-close.

(*h*) Since x and y are ϵ-close, and z and w are δ-close, we have $y = x + a$ and $w = z + b$ for $|a| \leq \epsilon$ and $|b| \leq \delta$ if we let $a := y - x$ and $b := w - z$. Then we have:

$$yw = (x + a)(y + b) = xy + xb + ya + ab$$

Thus

$$|yw - xz| = |az + bx + ab| \leq |az| + |bx| + |ab| = |a||z| + |b||x| + |a||b|.$$

Since $|a| \leq \epsilon$ and $|b| \leq \delta$, we thus have

$$|yw - xz| \leq \epsilon|z| + \delta|x| + \epsilon\delta$$

and thus that yw and xz are $(\epsilon|z| + \delta|x| + \epsilon\delta)$-close. □

Remark 4.3.2 One should compare statements $(a) - (c)$ of this proposition with the reflexive, symmetric, and transitive of equality. It is often useful to think of the notion of 'ϵ-close' as an approximate substitute for that of equality in analysis.

We now recursively define exponentiation for natural number exponents, extending the previous definition.

Definition 4.3.4 (Exponentiation to a natural number) Let x be a ratonal number. To raise x to the power of 0, we define $x^0 = 1$; in particular we define $0^0 := 1$. Now suppose inductively that x^n has been defined for some natural number n, then we define $x^{n+1} := x^n \times x$.

Proposition 4.3.3 (Properties of exponentiation, I) Let x, y be rational numbers, and let n, m be natural numbers.

(*a*) We have $x^n x^m = x^{n+m}$, $(x^n)^m = x^{nm}$, and $(xy)^n = x^n y^n$.

(*b*) Suppose $n > 0$. Then we have $x^n = 0$ iff $x = 0$.

(*c*) If $x \geq y \geq 0$, then $x^n \geq y^n \geq 0$. If $x > y \geq 0$ and $n > 0$, then $x^n > y^n \geq 0$.

(*d*) We have $|x^n| = |x|^n$.

(*e*) $2^N \geq N$ for all positive natural numbers N.

Proof.

(*a*) We first prove that $x^n x^m = x^{n+m}$ with induction on m by fixing n. In the base case where $m = 0$, $x^n x^0 = x^n \times 1 = x^n = x^{n+0}$. Now suppose inductively that $x^n x^m = x^{n+m}$ then as to $m + 1$, $x^n x^{m+1} = x^n x^m \times x = x^{n+m} \times x = x^{n+m+1}$. This closes the induction and thus for all natural number m, $x^n x^m = x^{n+m}$.
We then prove that $(x^n)^m = x^{nm}$. Again we use induction. In the base case where $m = 0$, $(x^n)^0 = 1 = x^0 = x^{n\times 0}$. Now suppose inductively that $(x^n)^m = x^{nm}$, then as to $m + 1$, $(x^n)^m + 1 = (x^n)^m \times x^n = x^{nm+n} = x^{n(m+1)}$. This closes the induction and thus for all natural number m, $(x^n)^m = x^{nm}$.
We finally prove that $(xy)^n = x^n y^n$ we use induction on n. In the base case where $n = 0$, $(xy)^0 = 1 = 1 \times 1 = x^0 y^0$. Now suppose inductively that $(xy)^n = x^n y^n$, then as to $n + 1$, $(xy)^{n+1} = (xy)^n \times xy = x^n y^n \times xy = x^{n+1} y^{n+1}$. This closes th induction, and hence $(xy)^n = x^n y^n$.

(*b*) We first prove that if $x = 0$ then $x^n = 0$ for all positive natural number n. We use induction, in the base case where $n = 1$, $0^1 = 0$. Now suppose inductively that $0^n = 0$, then as to $n + 1$, $0^{n+1} = 0^n \times 0 = 0$. This closes the induction and thus $0^n = 0$ for all $n > 0$.
We then prove that if $x \neq 0$ then $x^n \neq 0$. Since x is a rational number, we let $x = a//b \neq 0$ for some integer a and b, i.e., $a \neq 0$. Now we use induction. In the base case where $n = 1$, $x^1 = a//b = a^1//b^1 \neq 0$. Now suppose inductively that $x^n = a^n//b^n \neq 0$ then as to $n + 1$, $x^{n+1} = x^n \times x = (a^n//b^n) \times (a//b) = (a^n \times a)//(b^n \times b) = a^{n+1}//b^{n+1} \neq 0$ because $a^{n+1} = a^n \times n \neq 0$ since $a^n \neq 0$ by induction assumption and $a \neq 0$ due to the fact that integers have no zero divisors (Proposition 4.1.2). This closes the induction and thus if $x \neq 0$ then $x^n \neq 0$, which is equivalent to if $x^n = 0$ then $x = 0$.
Therefore, $x^n = 0$ iff $x = 0$ for all positive natural number n.

(*c*) We first prove that if $x \geq y \geq 0$, then $x^n \geq y^n \geq 0$. We use induction. In the base case where $n = 0$, $x^0 = 1 \geq 1 = y^0 \geq 0$. Now suppose inductively that $x^n \geq y^n \geq 0$, then as to $n+1$, $x^{n+1} = x \times x^n \geq xy^n \geq yy^n = y^{n+1} \geq y \times 0 = 0$, i.e., $x^{n+1} \geq y^{n+1} \geq 0$.
We then prove that if $x > y \geq 0$ and $n > 0$, then $x^n > y^n \geq 0$. Again, we use induction. In the base case where $n = 1$, $x^1 = x > y = y^1 \geq 0$. Now suppose inductively that $x^n > y^n \geq 0$, then as to $n+1$, $x^{n+1} = x \times x^n > xy^n > yy^n = y^{n+1} \geq y \times 0 = 0$, i.e., $x^{n+1} > y^{n+1} \geq 0$.

(*d*) We use induction on n. In the base case where $n = 0$, $|x^0| = 1 = |x|^0$. Now suppose inductively that $|x^n| = |x|^n$, then as to $n+1$, $|x^{n+1}| = |x^n \times x| = |x^n||x| = |x|^n|x| = |x|^{n+1}$. This closes the induction, and thus for all natural number n, $|x^n| = |x|^n$.

(*e*) We use induction. In the base case where $n = 1$, $2^1 = 2 \geq 1$. Now suppose inductively that $2^N \geq N$, then as to $N+1$, $2^{N+1} = 2^N \times 2 \geq 2N = N + N \geq N + 1$ since $N \geq 1$ for any positive natural number N. This closes the induction and thus for all positive natural number N, $2^N \geq N$. □

We now define exponentiation for negative integer exponents.

Definition 4.3.5 (Exponentiation to a negative number) Let x be a non-zero rational number. Then for any negative $-n$, we define $x^{-n} := 1/x^n$.

From this definition, we can conclude that $1/x^n = (1/x)^n$ by a simple induction whose induction step is $1/x^{n+1} = 1/(x \times x^n) = 1/x^n \times (1/x) = (1/x)^n \times (1/x) = (1/x)^{n+1}$.
We now have x^n defined for any integer n, whether n is positive, negative, or zero. Exponentiation with integer exponents has the following properties which supercede Proposition 4.3.3:

Proposition 4.3.4 Let x, y be non-zero rational numbers, and let n, m be integers.

(*a*) We have $x^n x^m = x^{n+m}$, $(x^n)^m = x^{nm}$, and $(xy)^n = x^n y^n$.

(*b*) If $x \geq y > 0$, then $x^n \geq y^n > 0$ if n is positive, and $0 < x^n \leq y^n$ if n is negative.

(*c*) If $x, y > 0$, $n \neq 0$, and $x^n = y^n$, then $x = y$.

(*d*) We have $|x^n| = |x|^n$.

Proof.

(*a*) – We have proved the case where $n \geq 0$ and $m \geq 0$, so we only have to show when there is one negative or two negative numbers among m, n.
We first talk about the case where $m < 0$ and $n < 0$. We have $n = -a$ and $m = -b$. Therefore,

$$x^n x^m = \frac{1}{x^a}\frac{1}{x^b} = \frac{1}{x^a x^b} = \frac{1}{x^{a+b}} = x^{-a-b} = x^{n+m}.$$

We then discuss the situation where one of n and m is negative. Because of the commutative law of addition and multiplication, that only $n < 0$ and only $m < 0$ are of the same case. Therefore, we here only discuss the case that $n < 0$ and $m \geq 0$. We lat $n = -a$ for some positive natural number a. Then we have,

$$x^n x^m = \frac{1}{x^a}x^m = \frac{x^m}{x^a}$$

By trichotomy of order, exactly one of $m > a$, $m = a$,and $m < a$ is true.
In the case where $m > a$ we have $m - a > 0$ then

$$\frac{x^m}{x^a} = \frac{x^a x^{m-a}}{x^a} = x^{m-a} = x^{m+n}.$$

In the case where $m = a$ we have $m - a = 0$ then

$$\frac{x^m}{x^a} = 1 = x^0 = x^{m-a} = x^{m+n}.$$

In the case where $m < a$ we have $a - m > 0$ then

$$\frac{x^m}{x^a} = \frac{x^m}{x^m x^{a-m}} = \frac{1}{x^{a-m}} = x^{m-a} = x^{m+n}.$$

In all we have $x^m x^n = x^{m+n}$.

– In Proposition 4.3.3, we have proved the case where $m \geq 0$ and $n \geq 0$. We noe need to show the cases where only $n < 0$, only $m < 0$, or $n < 0$ and $n < 0$.
If only $n < 0$, then we have $n = -a$ for some poitive natural number a. Therefore,

$$(x^n)^m = (\frac{1}{x^a})^m = \frac{1}{(x^a)^m} = \frac{1}{x^{ma}} = x^{-ma} = x^{mn}.$$

If only $m < 0$, then we then have $m = -b$ for some positive natural numebr b. Therefore,

$$(x^n)^m = \frac{1}{(x^n)^b} = \frac{1}{x^{nb}} = x^{-nb} = x^{mn}.$$

If $m < 0$ and $n < 0$, then we have $m = -b$ for some positive natrual number b. Therefore,

$$(x^n)^m = \frac{1}{(x^n)^b} \overset{\text{Case: } n<0,\ m>0}{\underset{\text{proved}}{=\!=\!=\!=\!=}} \frac{1}{x^{nb}} = x^{-nb} = x^{mn}.$$

In all, $(x^n)^m = x^{mn}$.

– The case $x \geq 0$ has been proved in Proposition 4.3.3, we now show that if n is negative i.e., $n = -k$ for some positive natural number k we have $(xy)^n = x^n y^n$. In fact, we have

$$(xy)^n = (xy)^{-k} = \frac{1}{(xy)^k} = \frac{1}{x^k y^k} = \frac{1}{x^k}\frac{1}{y^k} = x^{-k}y^{-k} = x^n y^n.$$

(b) In the case that n is positive, in proposition 4.3.3 we have if $x \geq y \geq 0$, then $x^n \geq y^n \geq 0$ for positive natural number n and $x^n = 0$ iff $x = 0$. Now because $y > 0$ so that $y \neq 0$ we have $y^n \neq 0$. Hence, $x^n \geq y^n > 0$.
In the case where n is negative, we have $n = -k$ for some positive integer k. Then

$$x^n - y^n = x^{-k} - y^{-k} = \frac{1}{x^k} - \frac{1}{y^k} = \frac{y^k - x^k}{x^k y^k}$$

As to k we have $x^k \geq y^k > 0$, so $y^k - x^k \leq 0$ and $x^k y^k > 0$. Then $\frac{y^k - x^k}{x^k y^k} \leq 0$ because if $\frac{y^k - x^k}{x^k y^k} > 0$ then by multiplying $x^k y^k$ to both sides we get $y^k - x^k > 0$, a contradiciton. Therefore $x^n - y^n \leq 0$ i.e., $x^n \leq y^n$. Also because $x^k > 0$ we have $x^n = x^{-k} > 0$ because if $x^n = x^{-k} \leq 0$ we have $1 \leq 0$ a contradiciton. Hence, $0 < x^n \leq y^n$.

(c) Since $x^n = y^n$, $(x^n)^{\frac{1}{n}} = (y^n)^{\frac{1}{n}}$. This is possible because $n \neq 0$ so that $\frac{1}{n}$ exists. Thus, $x^1 = y^1$ i.e., $x = y$.

(d) If n is positive or zero, i.e., n is a natural number, then we have proved it in Proposition 4.3.3. So we now only need to show that if n is a negative integer, we have $|x^n| = |x|^n$. Since n is a negative integer, we have $n = -k$ for some positive natural number k. Therefore,

$$|x^n| = |x^{-k}| = |x^{(-1)\times k}| = |(x^{-1})^k| = |x^{-1}|^k = |\frac{1}{x}|^k = (\frac{1}{|x|})^k = (|x|^{-1})^k = |x|^{-k} = |x|^n \quad \square$$

4.4 The decimal system

Under Construction.

4.5 Gaps in the rational numbers

Under Construction.