Foundations of Abstract Mathematics

Paul L. Bailey

Department of Mathematics, Southern Arkansas University
E-mail address: plbailey@saumag.edu
Date: January 21, 2009

Contents

Preface

1. Purpose

This manuscript collects the core curriculum of pregraduate abstract mathematics into one reference with a consistent style and predisposition. What is emphasized here are those theoretical aspects of mathematics which are lightly touched upon in the undergraduate curriculum but presupposed at the graduate level. Of particular interest are algebra and topology, which are often given short shrift to make way for calculus, differential equations, and so forth. We wish to expose how abstract thinking illuminates the computations of analysis.

This manuscript could serve as a guide to a capstone course for senior mathematics majors, intended to pull together and intertwine all that they have studied. This material could also serve as a reference for those who have been previously exposed to bits of this material, but perhaps have not glimpsed the interconnections. The style is blocked; each block depends only on preceding blocks, so the reader is always aware of what has been shown and what remains to show.

2. Description of the Blocks

Each sentence in the body of this manuscript is contained in commentary, developmental blocks, or orientation blocks.

2.1. Commentary. Commentary is the free floating verbiage found between the developmental blocks. This is what motivates the discussion, and binds it.

2.2. Developmental Blocks. The mathematics itself is entirely contained in developmental blocks, and in fact, the developmental blocks could stand alone without the rest of the manuscript. The developmental blocks are sequential, in the sense that a given block never depends on a later block; in this manner, it is impossible to create a circular argument. New terminology is introduced in Declarations and Definitions; each mathematical term occurring in developmental blocks is italicized exactly once in a declaration or definition, when it is first introduced.

Declaration: The introduction of primitive terminology.

Definition: The introduction of terminology built on previous terminology.

Proposition: A typical result.

Lemma: A result of a technical nature, which immediate precedes a Theorem.

Theorem: A landmark result.

Corollary: A result which follows immediately from a Theorem.

Problem: A result left for the reader to prove, at the end of a chapter. Unproven propositions also serve as problems.

2.3. Orientation Blocks. Orientation blocks rely on the previous knowledge and intuition of the reader, They reside outside of the development of the material, and so are not restricted to discuss only previously developed material. This allows the reader to place their previous experience into the framework of the developing material.

Example: Examples are sometimes given to illuminate the discussion, even though the theory supporting the ideas has not yet been built. Examples which are considered part of the theory are built in definitions and propositions.

Exercise: Exercises appear at the end of each chapter, and often involve examples. Results from exercises are not used in future developments.

3. Description of the Volumes

The manuscript consists of three volumes. Although each volume can be used independently, the material laid out in Volume I is presupposed throughout the next two volumes, and shortens their exposition. It significantly reduces the amount of print necessary to discuss groups, rings, and topological spaces, if, for example, the ideas of partial order, equivalence relation, or binary operators have already been firmly planted. The volumes are:

(I) Foundations of Abstract Mathematics
(II) Objects of Abstract Mathematics
(III) Categories of Abstract Mathematics

3.1. Foundations of Abstract Mathematics. This volume produces all of the set theoretical results used through the remaining work, and then develops the various standard systems of numbers. All numbers are defined, and their properties proven. The development is axiomatic.

3.2. Objects of Abstract Mathematics. This volume describes and produces results regarding the most fundamental underlying objects used in modern mathematics. The emphasis here is on theory and away from application. The volume provides a single source for definitions and proofs of the most commonly used objects and results. Examples are emphasized.

3.3. Categories of Abstract Mathematics. This volume introduces categories as a way of developing the interplay between different types of mathematical objects. Many new objects are introduced in this way. Category theory catalyzes the rapid absorbtion of new objects.

4. Description of this Volume

4.1. Goals. We aim to create a consistent system of mathematical thought in which we have a clear understanding of what is assumed and what has been proven from those assumptions. The modern starting point for such a development is the notion a set.

The beginning student of mathematical proofs is confronted with the perpetual question of what can be assumed in a proof. By clearly defining numbers from set theoretical axioms, we attempt to provide a source which can be cited in any exercise the student is likely to find.

This volume is in three parts. The first part consists of set theory, including functions, relations, families, and binary operations. The second part uses the

axioms of set theory to construct the natural numbers, the integers, the rational numbers, the real numbers, and the complex numbers. The third part moves on to the topics of cardinality, transfinite induction, and Zorn's Lemma.

It is impossible to define every mathematical word without creating a circular definition. Thus we need to begin with terms that have no definition; these terms are called primitive terms; what can be said about these terms is dictated by axioms.

The *Zermelo-Fraenkel* axioms with the Axiom of Choice (**ZFC**) are used to place set theory on a solid logical foundation. The *Morse-Kelley* (**MK**) class axioms are introduced later for the sake of cardinal numbers, and in anticipation of category theory.

4.2. Similar Treatments. The author knows of two books which, taken together, have similar treatments of some of the ideas contained in this volume. These are the excellent books by Halmos [**Ha60**] and Landau [**La66**]. Both of these books are recommended.

The author discovered [**Ha60**] during the first year of graduate, when it became necessary to be conversant with Zorn's Lemma. This exposition owes much to this book, specifically some points regarding ordered pairs, the Natural Numbers, and Zorn's Lemma. On the other hand, [**La66**] came to the author's attention only after the present vision of this material had been formulated.

We point out some of the differences between the present manuscript and these.

4.2.1. *Halmos's Book.* Halmos presents the axioms of set theory without.. [RETURN]

CHAPTER 1

Sets

1. Orientation

In this chapter, we lay the groundwork for the underlying language of abstract mathematics. This language is that of set theory; all of our work proceeds from the notions of set and element.

Intuitively, we know that we would like a set to be a collection of things, and the things in a set will be called elements of that set. We may specify the set with a list the elements in it, contained in braces, as in $A = \{1, 3, 5, 7, 9\}$; or by some property the set possesses, as in $A = \{x \mid x \text{ is an odd integer between 1 and 9}\}$. We would like to allow sets themselves to be elements, as in $B = \{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$.

However, it serves no purpose to define a set as a collection of elements, because the word "collection" has not been defined. We see immediately that we must begin with some undefined terms about which we have an intuitive but not formally logical understanding. These undefined words are known as *primitives*.

The approach of creating sets which are convenient without specified rules is sometimes referred to as *naive set theory*. This seems to work well, as long as we do not inadvertently stumble into a self-contradictory state. As an example of the type of problem that can arise, we mention *Russell's paradox*, which is predicated on the existence of a set of all sets.

Suppose that $\mathcal{U}$ is a that set has all sets as elements. We should like to be able to construct the set $A = \{x \in \mathcal{U} \mid p(x)\}$, where $p(x)$ is the proposition "x is not an element of x". Then the question arises, is $A \in A$? Well, if A is an element of A, it satisfies the condition which determines A; that is, $p(A)$ is true, so A is not an element of A, so A cannot be in A. But then A is not in A, so $p(A)$ is false, so $A \in A$. Thus it is impossible that A is in A, and it is impossible that A is not in A. This is a situation that we need to avoid.

The way around problems like this is to state clearly the rules under which sets can be constructed. Thus we use *axioms* which dictate which sets can be said to exist. There are several axiom systems which have been studied by logicians; our goal is not to delve into the complexities of mathematical logic, but rather to see how modern mathematics can be built from a given set theoretical axiom system.

The axiom system used here is known as *Zermelo-Fraenkel with Choice* (ZFC). We begin by listing all of the axioms, and proceed to develop from them the key ideas we need. In this development, all elements are actually sets. This simplifies the situation; we do not need to declare the existence of "element" as another undefined noun.

2. Axioms of Set Theory

Declaration 1. *Set* is a primitive noun; being an *element* of a set is a primitive relation. If a and A are sets, either a is an element of A, or a is not an element of A. If a is an element of A, we write $a \in A$, and may say that a is a *member* of A, or that a is a *point* in A, or that a is *contained* in A, or simply that a is in A. If a is not an element of A, we write $a \notin A$.

Axiom 1. (Axiom of Extension)
Two sets are equal if and only if they have the same elements. If A equals B, we write $A = B$. If A is not equal to B, we write $A \neq B$.

Axiom 2. (Axiom of the Empty Set)
There is a set with no elements, called the empty set. *The empty set is denoted $\varnothing$.*

Axiom 3. (Axiom of Pairing)
If A and B are sets, then there is a set containing A and B as its only elements. This set is denoted $\{A, B\}$.

Axiom 4. (Axiom of Union)
If A is a set, there is a set whose elements are precisely the elements of the elements of A. This set is denoted $\cup A$.

Axiom 5. (Axiom of Infinity)
There is a set X such that $\varnothing$ is in X and whenever A is in X, so is $\cup\{A, \{A\}\}$.

Axiom 6. (Axiom of Powers)
If A is a set, there is a set whose elements are precisely the subsets of A. This set is denoted $\mathcal{P}(A)$.

Axiom 7. (Axiom of Regularity)
If A is a nonempty set, there is an element of A which contains no elements in A.

Axiom 8. (Axiom of Specification)
Given any set A and any proposition $p(x)$, there is a set containing precisely those elements x in A for which $p(x)$ is true. This set is denoted $\{x \in A \mid p(x)\}$.

Axiom 9. (Axiom of Replacement)
Given any set A and any proposition $p(x, y)$ where $p(x, y_1)$ and $p(x, y_2)$ implies $y_1 = y_2$, there is a set containing precisely those y for which $p(x, y)$ is true for some x in A.

Axiom 10. (Axiom of Choice)
Given any set of nonempty sets, there is a set the contains exactly one element in each of the nonempty sets.

Axiom 1 (the Axiom of Extension) says that a set is completely determined by its elements. Thus, even though we may sometimes think of a set as a list of elements, we need to keep in mind that the order in which the elements are listed is not information included in the set; moreover, listing an element more than once has no effect on the set.

Axiom 2 (the Axiom of the Empty Set) asserts the existence of at least one set, that being the empty set. Since a set is completely determined by the elements it contains, the empty set is unique.

Axiom 5 (the Axiom of Infinity) also supplies an existing set, which happens to contain $\varnothing$. We note that the existence of $\varnothing$ actually follows from Axiom 8 (the Axiom of Specification) together with the existence of any set X, because $\varnothing = \{x \in X \mid x \neq x\}$.

Axiom 7 rules out certain constructions from being sets.

Axioms 3, 4, 6, 8, 9, and 10 supply the means of constructing new sets from existing ones.

We assume familiarity with standard set notation using braces.

Example 1.1. Assume that

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

is a set. Then Axiom 8 states that

$$B = \{a \in A \mid a \text{ is odd}\} = \{1, 3, 5, 7, 9\}$$

and

$$C = \{a \in A \mid 4 \leq a \leq 6\} = \{4, 5, 6\}$$

are sets. Now Axiom 3 states that $\{B, C\}$ is a set, and Axiom 4 implies that

$$\cup\{B, C\} = \{1, 3, 4, 5, 6, 7, 9\}$$

is a set. Axiom 6 states that

$$\mathcal{P}(C) = \{\varnothing, \{4\}, \{5\}, \{6\}, \{4, 5\}, \{4, 6\}, \{5, 6\}, C\}$$

is a set.

Proposition 1.1. *Let A, B, and C be sets. Then*

- *$A = A$ (reflexivity of equality);*
- *$A = B$ implies $B = A$ (symmetry of equality);*
- *$A = B$ and $B = C$ implies $A = C$ (transitivity of equality).*

Definition 1.2. A *singleton* is a set of the form $\{A\}$, where A is a set.

Proposition 1.3. *Let A be a set. Then $\{A\}$ is a set.*

Proof. By Axiom 3 (the Axiom of Pairing), $\{A, A\}$ is a set. By Axiom 1 (the Axiom of Extension), $\{A, A\} = \{A\}$. So $\{A\}$ is a set. □

Proposition 1.4. *Let A be a set. Then $A \notin A$.*

Proof. By Axiom 3, $\{A, A\}$ is a set; call it B. By Axiom 1, $B = \{A\}$. By Axiom 7, B contains an element which contains no elements from B. The only element in B is A, so A contains no elements in B. Since $A \in B$, $A \notin A$. □

3. Subsets

Definition 1.5. Let A and B be sets. We say that A is a *subset* of B, or that B is *contained in* A, and write $A \subset B$, if every element of A is an element of B.

Proposition 1.6. *Let A and B be sets. Then*

$$A = B \;\Leftrightarrow\; [x \in A \Leftrightarrow x \in B].$$

Proof. This is a formulaic restatement of Axiom 1. □

Proposition 1.7. *Let A and B be sets. Then*

$$A \subset B \;\Leftrightarrow\; [x \in A \Rightarrow x \in B].$$

Proof. This is a formulaic restatement of Definition 1.5. □

Proposition 1.8. *Let A and B be sets. Then*

$$A = B \Leftrightarrow [A \subset B \text{ and } B \subset A].$$

Proof. If $A = B$, then $x \in A \Leftrightarrow x \in B$. Thus $x \in A \Rightarrow x \in B$ and $x \in B \Rightarrow x \in A$. From this, $A \subset B$ and $B \subset A$.

On the other hand, if $A \subset B$ and $B \subset A$, then $x \in A \Rightarrow x \in B$, and $x \in B \Rightarrow x \in A$. Thus $x \in A \Leftrightarrow x \in B$, so $A = B$. □

We often use Proposition 1.8 to show that two sets are equal; that is, we show that each is contained in the other.

Proposition 1.9. *Let A be a set. Then $\varnothing \subset A$.*

Proof. The statement $x \in \varnothing$ is always false, so the statement $x \in \varnothing \Rightarrow x \in A$ is always true. Thus $\varnothing \subset A$. □

Proposition 1.10. *Let A, B, and C be sets. Then*

(a) *$A \subset A$;*
(b) *$A \subset B$ and $B \subset A$ implies $A = B$;*
(c) *$A \subset B$ and $B \subset C$ implies $A \subset C$.*

Proof. Part **(a)** is Proposition 1.8 with $B = A$. Part **(b)** is one direction of Proposition 1.8. To prove **(c)**, suppose that $A \subset B$ and $B \subset C$. Let $a \in A$. Since $a \in A$, $a \in B$ because $A \subset B$. Since $a \in B$, $a \in C$ because $B \subset C$. Since a was arbitrary, every element of A is an element of C. Thus $A \subset C$. □

Definition 1.11. Let A and B be sets. We say that A is a *proper subset* of B, and write $A \subsetneq B$, if $A \subset B$ and $A \neq B$.

4. Set Operations

Definition 1.12. Let A and B be sets.

The *union* of A and B is

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

The *intersection* of A and B is

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

The *complement* of B with respect A is

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

We wish to show that these operations produce sets, according to the rules of set construction set forth in the axioms. Note that we cannot apply Axiom 8 (the Axiom of Specification) directly, since it allows us to specify elements in a given set. We must first construct a single set from which to extract the elements. To do this, we use the Axiom of Pairing and the Axiom of Union.

Proposition 1.13. *Let A and B be sets. Then $A \cup B$, $A \cap B$, and $A \setminus B$ are sets.*

Proof. By Axiom 3 (the Axiom of Pairing), the set $C = \{A, B\}$ exists. Thus the set $\cup C$ exists by Axiom 4 (the Axiom of Union). This axiom states that $\cup C$ consists of the elements of the elements of C, so $x \in \cup C$ if and only if x is an element of an element of C. The elements of C are A and B, so $x \in \cup C$ if and only if $x \in A$ or $x \in B$; that is, $\cup C = A \cup B$, so $A \cup B$ is a set.

Now

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

and

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

are sets by Axiom 8 (the Axiom of Specification). □

Definition 1.14. Let A and B be sets. We say that A and B are *distinct* if $A \neq B$. We say that A and B are *disjoint* if $A \cap B = \varnothing$.

Example 1.2. Let $A = \{1, 3, 5, 7, 9\}$ and $B = \{3, 4, 5, 6, 7\}$. Then

- $A \cup B = \{1, 3, 4, 5, 6, 7, 9\}$;
- $A \cap B = \{3, 5, 7\}$;
- $A \setminus B = \{1, 9\}$;
- $B \setminus A = \{4, 6\}$.

Note that $A \setminus B$ and $B \setminus A$ are disjoint (in this case).

Example 1.3. Let A and B be two distinct nonparallel lines in a plane. We may consider A and B as a set of points. Their intersection is a single point, their union is crossing lines, and the complement of A with respect to B is A minus the point of intersection.

Example 1.4. A *sphere* is the set of points in space equidistant from a given point, called its *center*; the common distance to the center is called that *radius* of the sphere. Thus a sphere is the surface of a solid ball.

Take two points in space such that the distance between them is 10, and imagine two spheres centered at these points. Let one of the spheres have radius 5. If the radius of the other sphere is less than 5 or greater than 15, then the spheres are disjoint. If the radius of the other sphere is exactly 5 or 15, the intersection is a single point. If the radius of the other sphere is between 5 and 15, the spheres intersect in a circle.

Proposition 1.15. *Let A be a set. Then*

- $A = A \cup A$;
- $A = A \cap A$;
- $\varnothing \cap A = \varnothing$;
- $\varnothing \cup A = A$.

In order to show that $A = B$, we show that $A \subset B$ and $B \subset A$. In order to show that $A \subset B$, we select an arbitrary member of A, and using the defining property of A, we show that this arbitrary member also satisfies the defining property of B. We give an example is verbose form, then an analogous example in compressed form.

Proposition 1.16. *Let A and B be a sets. Then $A \subset B \Leftrightarrow A \cap B = A$.*

Proof. To prove an if and only if statement, we prove implication in both directions.

($\Rightarrow$) Assume that $A \subset B$. We wish to show that $A \cap B = A$. To show that two sets are equal, we show that each is contained in the other.

($\subset$) To show that $A \cap B \subset A$, it suffices to show that every element of $A \cap B$ is in A. Thus we select an arbitrary element $c \in A \cap B$ and show that it is in A. Now by definition of intersection, $c \in A \cap B$ means that $c \in A$ and $c \in B$. Thus $c \in A$. Since c was arbitrary, every element of $A \cap B$ is contained in A. Thus $A \cap B \subset A$.

($\supset$) Let $a \in A$. We wish to show that $a \in A \cap B$. Since $A \subset B$, then every element of A is an element of B. Thus $a \in B$. So $a \in A$ and $a \in B$. By definition of intersection, $a \in A \cap B$. Thus $A \subset A \cap B$.

Since $A \cap B \subset A$ and $A \subset A \cap B$, we have $A \cap B = A$.

($\Leftarrow$) Assume that $A \cap B = A$. We wish to show that $A \subset B$. Let $a \in A$. It suffices to show that $a \in B$. Since $A \cap B = A$, then $a \in A \cap B$. Thus $a \in A$ and $a \in B$. In particular, $a \in B$. □

Proposition 1.17. *Let A and B be a sets. Then $A \subset B \Leftrightarrow A \cup B = B$.*

Proof. We prove both directions of the double implication.

($\Rightarrow$) Assume that $A \subset B$. Clearly $B \subset A \cup B$, so we show that $A \cup B \subset B$. Let $c \in A \cup B$. Then $c \in A$ or $c \in B$. If $c \in B$ we are done, so assume that $c \in A$. Since $A \subset B$, then $c \in B$ by definition of subset. Thus $A \cup B \subset B$.

($\Leftarrow$) Assume that $A \cup B = B$ and let $a \in A$. Thus $a \in A \cup B$, and since $A \cup B = B$, $a \in B$. Thus $A \subset B$. □

Proposition 1.18. (Properties of Union and Intersection)
Let A, B, and C be sets. Then

- $A \cap B = B \cap A$
- $A \cup B = B \cup A$
- $(A \cap B) \cap C = A \cap (B \cap C)$;
- $(A \cup B) \cup C = A \cup (B \cup C)$;
- $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$;
- $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

The preceding properties state that union and intersection are commutative and associative operations, and that they distribute over each other. Since

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

parentheses are useless and we write $A \cap B \cap C$. This extends to four sets, five sets, and so on. Similar remarks apply to unions.

Proposition 1.19. (Properties of Complement)
Let A, B, and C be sets. Then

- $A \subset B \Rightarrow A \cup (B \setminus A) = B$;
- $A \subset B \Rightarrow A \cap (B \setminus A) = \varnothing$;
- $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap B \cap C)$;
- $(A \setminus B) \setminus C = A \setminus (B \cup C)$.

Proposition 1.20. (DeMorgan's Laws)
Let A, B, and C be sets. Then

- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

Definition 1.21. Let A and B be sets. The *symmetric difference* of A and B is

$$A \triangle B = \{x \mid x \in A \text{ or } x \in B, \text{ but not both}\}.$$

Proposition 1.22. *Let A and B be sets. Then $A \triangle B$ is a set, and*

$$A \triangle B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

Example 1.5. Let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{4, 5, 6, 7, 8, 9\}$. Then

$$A \triangle B = \{1, 2, 3, 7, 8, 9\}.$$

Each of these set operations corresponds to a logical operator:

- union $\leftrightarrow$ or;
- intersection $\leftrightarrow$ and;
- complement $\leftrightarrow$ not;
- symmetric difference $\leftrightarrow$ exclusive or.

5. Cartesian Product

Definition 1.23. Let a and b be sets. The *ordered pair* of a and b is denoted (a, b) and is defined as

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

We call a the *first coordinate* of (a, b) and we call b the *second coordinate* of (a, b).

Proposition 1.24. *Let a and b be sets. Then (a, b) is a set.*

Proof. By Proposition 1.3, $\{a\}$ is a set. Apply Axiom 3 to the sets a and b to see that $\{a, b\}$ is a set. Once more apply Axiom 3 to $\{a\}$ and $\{a, b\}$ to see that $(a, b) = \{\{a\}, \{a, b\}\}$ is a set. □

The definition we are using for ordered pair is due to Kuratowski. The motivation for the definition is that such ordered pairs satisfy the following "defining property".

Proposition 1.25. *Let a, b, c, and d be sets. Then*

$$(a, b) = (c, d) \Leftrightarrow [a = c \text{ and } b = d].$$

Proof. We accept that if $a = c$ and $b = d$, then $(a, b) = (c, d)$. We would like to see that $(a, b) = (c, d)$ implies $a = c$ and $b = d$.

Suppose that $(a, b) = (c, d)$. Then $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Then $\{a\} \in \{\{c\}, \{c, d\}\}$, so $\{a\} = \{c\}$ or $\{a\} = \{c, d\}$. In either case, $c \in \{a\}$, so $c = a$.

Now $\{a, b\} = \cup(a, b) = \cup(c, d) = \{c, d\}$, and since $a = c$, this may be written as $\{a, b\} = \{a, d\}$, so $d \in \{a, b\}$, and $d = a$ or $d = b$. If $d = b$ we are done, so consider the case when $d = a$. In this case, we have $\{d, b\} = \{a, b\} = \{a, d\} = \{d\}$, so $b \in \{d\}$, and $b = d$. □

Definition 1.26. Let A and B be sets. The *cartesian product* of A and B is

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

Proposition 1.27. *Let A and B be sets. Then $A \times B$ is a set.*

Proof. We use Axiom 6, (the Axiom of Powers), which say that given any set X, there exists a set $\mathcal{P}(X)$ whose elements are exactly the subsets of X.

If $a \in A$ and $b \in B$, then $\{a\}, \{a, b\} \subset A \cup B$, so $\{a\}, \{a, b\} \in \mathcal{P}(A \cup B)$. Therefore $\{\{a\}, \{a, b\}\} \subset \mathcal{P}(A \cup B)$, so $(a, b) = \{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$. We have found one set, $\mathcal{P}(\mathcal{P}(A \cup B))$, which contains all of the ordered pairs in which we are interested. This allows us to use Axiom 8 (the Axiom of Specification) to declare that

$$A \times B = \{x \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid x = (a, b) \text{ for some } a \in A, b \in B\}$$

is a set. □

Proposition 1.28. *Let A, B, C, and D be sets. Then*

$$A \times B = C \times D \Leftrightarrow [A = C \text{ and } B = D].$$

Proof. It is evident that if $A = C$ and $B = D$, then $A \times B = C \times D$. Conversely, suppose that $A = C$ and $B = D$.Thus let $x \in A \times B$. Then $x = (a, b)$ for some $a \in A$ and $b \in B$. Then $a \in C$ and $b \in D$, so $(a, b) \in C \times D$. Therefore $A \times B \subset C \times D$. Similarly, $C \times D \subset A \times B$. □

Example 1.6. Let $A = \{1, 3, 5\}$ and let $B = \{1, 4\}$. Then

$$A \times B = \{(1, 1), (1, 4), (3, 1), (3, 4), (5, 1), (5, 4)\}.$$

In particular, this set contains 6 elements.

Proposition 1.29. (Properties of Cartesian Product)
Let A, B, and C be sets. Then

- $(A \cup B) \times C = (A \times C) \cup (B \times C)$;
- $(A \cap B) \times C = (A \times C) \cap (B \times C)$;
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Proposition 1.30. *Let A, B, C, and D be sets. Then*

$$(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D).$$

Proof. We use the defining property of an ordered pair to show equality of sets by showing containment in both directions.

($\subset$) Let $\alpha \in (A \times B) \cap (C \times D)$. Then $\alpha \in A \times B$ and $\alpha \in C \times D$. Then $\alpha = (a, b)$, where $a \in A$ and $b \in B$, and $\alpha = (c, d)$, where $c \in C$ and $d \in D$. Since $(a, b) = (c, d)$, we have $a = c$ and $b = d$.

Now $a \in A$ and $a = c \in C$, so $a \in A \cap C$. Also $b \in B$ and $b = d \in D$, so $b \in B \cap D$. Therefore $(a, b) \in (A \cap C) \times (B \cap D)$.

($\supset$) Let $\alpha \in (A \cap C) \times (B \cap D)$. Then $\alpha = (x, y)$, where $x \in A \cap C$ and $y \in B \cap D$. Thus $x \in A$ and $x \in C$. Also $y \in B$ and $y \in D$. So $(x, y) \in A \times B$ and $(x, y) \in C \times D$. Therefore $(x, y) \in (A \times B) \cap (C \times D)$. □

Example 1.7. Cartesian product is not an associative operation. For example, let $A = \{1, 2\}$, $B = \{3\}$, and $C = \{4, 5\}$. Then

$$(A \times B) \times C = \{((1, 3), 4), ((2, 3), 4), ((1, 3), 5), ((2, 3), 5)\};$$
$$A \times (B \times C) = \{(1, (3, 4)), (2, (3, 4)), (1, (3, 5)), (2, (3, 5))\}.$$

We could now attempt to define "ordered triples" in one of these ways:

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

The first two of these have the obvious technical difficulty that they lead to different definitions; $((a,b),c)$ is not actually equal to $(a,(b,c))$ if a, b, and c are distinct. All three of these possibilities have the problem that we would need a new definition for each number of entries in an "ordered tuple", and we will have problems with infinite tuples. We will use a different approach after we develop functions.

6. Relations

Sets of ordered pairs are very useful in building more complex structures involving sets, so we give a brief account which involves winding and unwinding their definitions. We will use the results here when studying mappings and functions.

Definition 1.31. A *relation* is a set whose elements are ordered pairs.

Let R be a relation.

The *domain* of R is

$$\mathrm{dom}(R) = \{a \mid (a,b) \in R \text{ for some } b\}.$$

The *range* of R is

$$\mathrm{rng}(R) = \{b \mid (a,b) \in R \text{ for some } a\}.$$

Proposition 1.32. *Let R be a relation. Then* $\mathrm{dom}(R)$ *and* $\mathrm{rng}(R)$ *are sets.*

Proof. By two applications of Axiom 4, $\cup(\cup R)$ is a set. The elements of R are of the form $\{\{a\},\{a,b\}\}$, so

$$\cup R = \{\{a\} \mid (a,b) \in R\} \cup \{\{a,b\} \mid (a,b) \in R\}.$$

Thus

$$\begin{aligned}\cup(\cup(R)) &= \{a \mid (a,b) \in R\} \cup \{c \mid c = a \text{ or } c = b \text{ for some } (a,b) \in R\} \\ &= \{a \mid (a,b) \in R\} \cup \{b \mid (a,b) \in R\}.\end{aligned}$$

Now

$$\mathrm{dom}(R) = \{a \in \cup(\cup(R)) \mid (a,b) \in R\}$$

and

$$\mathrm{rng}(R) = \{b \in \cup(\cup(R)) \mid (a,b) \in R\}$$

are sets, by Axiom 8. □

Proposition 1.33. *Let R be a relation. Then*

(a) $\cup(\cup(R)) \subset (\mathrm{dom}(R) \cup \mathrm{rng}(R))$*;*
(b) $R \subset \mathrm{dom}(R) \times \mathrm{rng}(R)$.

Example 1.8. Let $R = \{(1,2),(2,4),(3,6),(4,8)\}$. Then

$$\begin{aligned}R &= \{\{\{1\},\{1,2\}\},\{\{2\},\{2,4\}\},\{\{3\},\{3,6\}\},\{\{4\},\{4,8\}\}\};\\ \cup R &= \{\{1\},\{1,2\},\{2\},\{2,4\},\{3\},\{3,6\},\{4\},\{4,8\}\};\\ \cup(\cup R) &= \{1,1,2,2,2,4,3,3,6,4,4,8\} = \{1,2,3,4,6,8\};\\ \mathrm{dom}(R) &= \{1,2,3,4,5\};\\ \mathrm{rng}(R) &= \{2,4,6,8,10\}.\end{aligned}$$

7. Numbers

In due course, we will formally develop all of these standard number systems from the axioms of set theory. For the time being, we use these familiar sets only in commentary, examples, and exercises. Since they are useful for intuition into general set constructions, at this time we specify the standard names for the common sets of numbers. These are the standard sets of numbers:

$$\begin{aligned}
\text{Natural Numbers:} &\quad \mathbb{N} = \{0, 1, 2, 3, \dots\} \\
\text{Integers:} &\quad \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \\
\text{Rational Numbers:} &\quad \mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\} \\
\text{Real Numbers:} &\quad \mathbb{R} = \{\text{decimal expansions}\} \\
\text{Complex Numbers:} &\quad \mathbb{C} = \{a + ib \mid a, b \in \mathbb{R} \text{ and } i^2 = -1\}
\end{aligned}$$

We view $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

The first three sets, $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$, have an algebraic nature; they are the minimum sets of numbers which allow us to add and multiply ($\mathbb{N}$), subtract ($\mathbb{Z}$), and divide ($\mathbb{Q}$). The real numbers ($\mathbb{R}$) are obtained by filling in gaps in $\mathbb{Q}$ to obtain a set which is geometrically a line. The complex numbers allow us to factor all quadratic equations, and are geometrically a plane.

Certain connected sets of real numbers are called "intervals", and they are expressed using the following standard notation:

$$\begin{aligned}
[a, b] &= \{x \in \mathbb{R} \mid a \leq x \leq b\} & (-\infty, b] &= \{x \in \mathbb{R} \mid x \leq b\} \\
(a, b) &= \{x \in \mathbb{R} \mid a < x < b\} & (-\infty, b) &= \{x \in \mathbb{R} \mid x < b\} \\
[a, b) &= \{x \in \mathbb{R} \mid a \leq x < b\} & [a, \infty) &= \{x \in \mathbb{R} \mid a \leq x\} \\
(a, b] &= \{x \in \mathbb{R} \mid a < x \leq b\} & (a, \infty) &= \{x \in \mathbb{R} \mid a < x\}
\end{aligned}$$

The notation for ordered pair (a, b) is the same as the standard notation for open interval of real numbers, but its meaning is entirely different. This is standard, and you must decide from the context which meaning is intended.

Example 1.9. Let $A = [1, 5]$ be the closed interval of real numbers between 1 and 5 and let $B = (10, 16)$ be the open interval of real numbers between 10 and 16. Let $C = A \cup B$. Let $\mathbb{N}$ be the set of natural numbers. How many elements are in $C \cap \mathbb{N}$?

Solution. The set $C \cap \mathbb{N}$ is the set of natural numbers between 1 and 5 inclusive and between 10 and 16 exclusive. Thus $C \cap \mathbb{N} = \{1, 2, 3, 4, 5, 11, 12, 13, 14, 15\}$. Therefore $C \cap \mathbb{N}$ has 10 elements. □

Example 1.10. Let $A = [1, 3]$, $B = [3, 8]$, and $C = (0, 3)$ be intervals of real numbers. The set $A \times B \times C$ forms a cube in $\mathbb{R}^3$, which is closed on its sides (it contains its boundary there) but open on the top and bottom (it does not contain its boundary there). How many elements are in $(A \times B \times C) \cap (\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})$?

Solution. By generalizing a previous proposition, we have

$$(A \times B \times C) \cap (\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}) = (A \cap \mathbb{Z}) \times (B \cap \mathbb{Z}) \times (C \cap \mathbb{Z}).$$

Now $A \times \mathbb{Z} = \{1, 2, 3\}$, $B \times \mathbb{Z} = \{3, 4, 5, 6, 7, 8\}$, and $C \times \mathbb{Z} = \{1, 2\}$. Thus $(A \times B \times C) \cap (\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})$ has $3 \cdot 6 \cdot 2 = 36$ elements. □

8. Problems and Exercises

Problem 1.1. Let A, B, and C sets. Show that

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

Problem 1.2. Let A, B, and C be sets. Show that

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

Problem 1.3. Let A, B, and C be sets. Prove the following identities.

(a) $A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C)$;
(b) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$;
(c) $(A \smallsetminus B) \smallsetminus C = A \smallsetminus (B \cup C)$.

Exercise 1.1. Let A, B, and C be any sets. Determine which of the following statements is true.

(a) $A \subset B \Rightarrow A \cap B = A$;
(b) $A \subset B \Rightarrow B \smallsetminus A = B$;
(c) $A \smallsetminus (B \cup C) = (A \smallsetminus B) \cup (A \smallsetminus C)$;
(d) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

Exercise 1.2. Let A, B, and C be the following subsets of $\mathbb{N}$:

- $A = \{n \in \mathbb{N} \mid n < 25\}$;
- $E = \{n \in A \mid n \text{ is even}\}$;
- $O = \{n \in A \mid n \text{ is odd}\}$;
- $P = \{n \in A \mid n \text{ is prime}\}$;
- $S = \{n \in A \mid n \text{ is a square}\}$.

Compute the following sets:

(a) $(E \cap P) \cup S$;
(b) $(E \cap S) \cup (P \smallsetminus O)$;
(c) $P \times S$;
(d) $(O \cap S) \times (E \cap S)$.

Exercise 1.3. Let A, B, and C be the following subsets of $\mathbb{R}$:

- $A = [0, 100)$;
- $B = [\frac{1}{2}, \frac{505}{7}]$;
- $C = (-8, \pi]$.

Compute the number of points in the set $((A \times B) \times C) \cap ((\mathbb{Z} \times \mathbb{Z}) \times \mathbb{Z})$.

Exercise 1.4. For $a, b \in \mathbb{R}$, let $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ be the closed interval between a and b. How many elements are contained in the following sets?

(a) $([-2, 3] \cup [5, 9]) \cap \mathbb{Z}$
(b) $([\sqrt{2}, \pi] \cup (3^3, 2^5]) \cap \mathbb{Z}$
(c) $([1, 5] \times (3, 6)) \cap (\mathbb{Z} \times \mathbb{Z})$

CHAPTER 2

Functions

1. Mappings

Mappings are relations together with addition information; the domain and range must be subsets of some specified sets, called the source and target. This allows us to say that mappings are distinct if they have different sources or targets.

Definition 2.1. Let A and B be sets. A *mapping* between A and B is an ordered pair $r = ((A, B), R)$, where $R \subset A \times B$.

Let $r = ((A, B), R)$ be a mapping.

The *source* of r is $\text{src}(r) = A$.

The *target* of r is $\text{trg}(r) = B$.

The *domain* of r is $\text{dom}(r) = \{a \in A \mid (a, b) \in R \text{ for some } b \in B\}$.

The *range* of r is $\text{rng}(r) = \{b \in B \mid (a, b) \in R \text{ for some } a \in A\}$.

The *graph* of r is $\text{grf}(r) = R$.

If $(a, b) \in R$, we say that r *maps* a *to* b.

Example 2.1. Suppose that M is a set of men and F is a set of women. Let $R = \{(m, f) \in M \times F \mid m \text{ is the uncle of } f\}$. Then $((M, F), R)$ is a mapping.

Example 2.2. Let $\mathbb{R}$ be the set of all real numbers. Let

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}.$$

We know that the graph of R is a circle. Let $r = ((\mathbb{R}, \mathbb{R}), R)$. Then r is the mapping which pairs the sine and cosine of a given angle. Let $I = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$. Then $\text{src}(r) = \mathbb{R}$, $\text{trg}(r) = \mathbb{R}$, $\text{dom}(r) = I$, and $\text{rng}(r) = I$.

Proposition 2.2. *Let $r = ((A, B), R)$ and $s = ((C, D), S)$ be mappings. Then $r = s$ if and only if $A = C$, $B = D$, and $R = S$.*

Proof. This follows from two applications of Proposition 1.25. □

Definition 2.3. Let $r = ((A, B), R)$ be a mapping.

We say that r is *total* if $A = \{a \in A \mid (a, b) \in R \text{ for some } b \in B\}$; otherwise, we say that r is *partial*.

We say that r is *single-valued* if $(a, b_1), (a, b_2) \in R$ implies $b_1 = b_2$; otherwise, we say that r is *multi-valued*.

Example 2.3. Let $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$. Then $((\mathbb{R}, \mathbb{R}), R)$ is total but multi-valued.

Example 2.4. Let $R = \{(m, n) \in \mathbb{N} \times \mathbb{Z} \mid 2m = 3n - 5\}$. Then $((\mathbb{N}, \mathbb{Z}), R)$ is single valued but partial.

2. Functions

Functions are a type of mapping in which the source and the domain coincide, and a point in the domain is mapped to exactly one point in the target; that is, it is total and single-valued.

Definition 2.4. Let A and B be sets. A *function* from A to B is an ordered pair $f = ((A, B), F)$, where $F \subset A \times B$, satisfying the condition that for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in F$.

Let $f = ((A, B), F)$ be a function from A to B. We say that f *maps* A *into* B, and write $f : A \to B$.

The *source* of f is $\mathrm{src}(f) = A$,

The *target* of f is $\mathrm{trg}(f) = B$.

The *domain* of f is $\mathrm{dom}(f) = \{a \in A \mid (a, b) \in F \text{ for some } b \in B\}$.

The *range* of f is $\mathrm{rng}(f) = \{b \in B \mid (a, b) \in F \text{ for some } a \in A\}$.

The *graph* of f is $\mathrm{grf}(f) = F$.

If $a \in A$, the unique element $b \in B$ such that $(a, b) \in F$ is denoted $f(a)$, so that $f(a) = b$. We say that f *maps* a *to* b, and write $f : a \mapsto b$. Symbolically, our definition of function becomes

$$f : A \to B \;\Leftrightarrow\; \forall a \in A\, \exists! b \in B \ni f(a) = b.$$

Proposition 2.5. *Let f be a function. Then* $\mathrm{src}(f) = \mathrm{dom}(f)$.

Let $f = ((A, B), F)$ be a function. Then $\cup(\cup(F)) \subset (A \cup B)$, so we may use Axiom 8 to recover the domain A from the graph F as

$$A = \{a \in \cup(\cup(F)) \mid (a, b) \in F \text{ for some } b \in \cup(\cup(F))\}.$$

However, we cannot recover B from F. We see that B is actually extra information which is embedded in the function but not available through the graph F.

Some authors define a function as a set of ordered pairs which is the graph for a function, like our F above. Under that approach, any set containing the range can be the target. With our approach, two functions must have the same range to be equal.

Proposition 2.6. *Let $f : A \to B$ and $g : C \to D$. Then $f = g$ if and only if $A = C$, $B = D$, and $f(a) = g(a)$ for every $a \in A$.*

Proof. Since f and g are functions, we have $f = ((A, B), F)$ and $g = ((C, D), G)$ for some $F \subset A \times B$ and $G \subset C \times D$.

Suppose $f = g$; then by Proposition 1.25, $(A, B) = (C, D)$ and $F = G$, so by another application of Proposition 1.25, $A = C$ and $B = D$. Let $a \in A$ and set $b = f(a)$; then $(a, b) \in F$, so $(a, b) \in G$. Thus b is the unique member of B such that $(a, b) \in G$, which we write as $g(a) = b$. Thus $f(a) = g(a)$.

On the other hand, suppose that $A = C$, $B = D$, and $f(a) = g(a)$ for every $a \in A$. Then $(A, B) = (C, D)$. To show that $f = g$, it remains to show that $F = G$. Let $x \in F$. Then $x = (a, b)$ for some $a \in A$ and $b \in B$. Now $b = f(a) = g(a)$, so $x = (a, b) = (a, g(b)) \in G$. Thus $F \subset G$. Similarly, $G \subset F$. □

Example 2.5. If the domain of a function $f : A \to B$ is sufficiently small, we may explicitly describe the function by listing the elements of A and where they go; for example, if $A = \{1, 2, 3\}$ a perfectly good function $A \to A$ is given by $\{1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 1\}$.

However, if A is large, the functions on A which are easiest to understand are those which are specified by some *rule* or *algorithm*. The common functions of single variable calculus are of this nature.

A "real-valued function of a real variable" is a function whose domain and whose target is the set of real numbers. For example, let $\mathbb{R}$ be the set of real numbers; then $f(x) = x^3 + 3x + 5$ describes a function $f : \mathbb{R} \to \mathbb{R}$. Keep in mind that technically, the function consists of the ordered pair $(\mathbb{R}, \mathbb{R})$ specifying the domain and target, together with the graph of the function, which is the set $F = \{(x, y) \mid y = f(x)\}$.

Some functions are constructed from existing functions by specifying cases; again with $\mathbb{R}$ being the real numbers, we can describe a function $f : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = \begin{cases} 0 & \text{if } x < 0; \\ x^3 & \text{if } x \geq 0. \end{cases}$$

3. Images and Preimages

Definition 2.7. Let $f : A \to B$ and let $C \subset A$. The *image of C under A* is

$$f(C) = \{b \in B \mid b = f(a) \text{ for some } a \in A\}.$$

The *image of f*, denoted $\text{img}(f)$, is the image of the domain of f.

If $f : A \to B$, then $\text{rng}(f) = \text{img}(f)$; the terms range of f and image of f are synonymous.

Definition 2.8. Let $f : A \to B$ and let $D \subset B$. The *preimage of D under f* is

$$f^{-1}(D) = \{a \in A \mid f(a) \in D\}.$$

If $b \in B$, we may write $f^{-1}(b)$ to mean $f^{-1}(\{b\})$.

Note that images and preimages have been constructed via Axiom 8 as subsets of given sets. Thus images and preimages are themselves sets.

Proposition 2.9. *Let $f : X \to Y$ be a function and let $A, B \subset X$. Then*

(a) $f(A \cup B) = f(A) \cup f(B)$;
(b) $f(A \cap B) \subset f(A) \cap f(B)$.

Proof. Let $y \in f(A \cup B)$. Then $y = f(x)$ for some $x \in A \cup B$. Now $x \in A$ or $x \in B$, so $f(x) \in f(A)$ or $f(x) \in f(B)$. Thus $y = f(x) \in f(A) \cup f(B)$.

Let $y \in f(A) \cup f(B)$. Thus $y \in f(A)$ or $y \in f(B)$, so $y = f(x)$ for some $x \in A$, or $y = f(x)$ for some $x \in B$. That is, $y = f(x)$ for some $x \in A \cup B$. Thus $y \in f(A \cup B)$. This proves **(a)**.

Let $y \in f(A \cap B)$. Then $y = f(x)$ for some $x \in A \cap B$. Now $x \in A$ and $x \in B$, so $f(x) \in f(A)$ and $f(x) \in f(B)$. Thus $f(x) \in f(A) \cap f(B)$. This proves **(b)**. □

Problem 2.1. Let $f : X \to Y$ be a function and let $C, D \subset Y$.
(a) Show that $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
(b) Show that $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

4. Injective and Surjective Functions

Definition 2.10. Let $f : A \to B$. We say that f is *injective* (or *one-to-one*) if whenever a_1 and a_2 are distinct member of A, then $f(a_1)$ and $f(a_2)$ are distinct members of B; in symbols,

$$\forall a_1, a_2 \in A, f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$

Proposition 2.11. *Let $f : A \to B$. The following conditions are equivalent:*

(i) *f is injective;*
(ii) *for every $b \in B$, $f^{-1}(b)$ contains at most one element.*

Definition 2.12. Let $f : A \to B$. We say that f is *surjective* (or *onto*) if for every $b \in B$ there exists $a \in A$ such that $f(a) = b$; in symbols,

$$\forall b \in B \; \exists a \in A \ni f(a) = b.$$

Proposition 2.13. *Let $f : A \to B$. The following conditions are equivalent:*

(i) *f is surjective;*
(ii) $\operatorname{rng}(f) = \operatorname{trg}(f)$*;*
(iii) $\operatorname{img}(f) = \operatorname{trg}(f)$.

Definition 2.14. Let $f : A \to B$. We say that f is *bijective* if it is injective and surjective.

Example 2.6. A "real-valued function of a real variable" is a function such that This simply means that the domain and the target of the function is the set of real numbers.

- $f(x) = x^3$ is bijective;
- $g(x) = x^2$ is neither injective nor surjective;
- $h(x) = x^3 - 2x^2 - x + 2$ is surjective but not injective;
- $a(x) = \arctan(x)$ is injective but not surjective.

Let $A = \{-1, 1, 2\}$. Some of the images and preimages of A are:

- $f(A) = \{-1, 1, 8\}$;
- $g(A) = \{1, 4\}$;
- $h(A) = \{0\}$;
- $f^{-1}(A) = \{-1, 0, \sqrt[3]{2}\}$;
- $g^{-1}(A) = \{-\sqrt[3]{2}, -1, 1, \sqrt[3]{2}\}$;
- $a^{-1}(A) = \varnothing$.

5. Restrictions and Constrictions

Restrictions and constrictions allow us to focus our attention on a particular part of the domain or target of the original function.

Definition 2.15. Let $f : A \to B$. Let $C \subset A$ and $D \subset B$.

The *restriction of f to C* is the function

$$f \downharpoonright_C \colon C \to B \quad \text{given by} \quad f \downharpoonright_C (c) = f(c).$$

The *constriction of f from D* is the function

$$f \upharpoonright^D \colon f^{-1}(D) \to D \quad \text{given by} \quad f \upharpoonright^D (a) = f(a).$$

One use of constriction is to let $D = \operatorname{rng}(f)$; then $f \upharpoonright^D$ is surjective.

One use of restriction is to select $C \subset \operatorname{dom}(f)$ so that $f(c_1) = f(c_2) \Rightarrow c_1 = c_2$ for $c_1, c_2 \in C$, so that $f \downharpoonright_C$ is injective. We see momentarily why we may need an injective function.

Proposition 2.16. *Let $f : A \to B$ be injective and let $C \subset A$.*
Then $f \downharpoonright_C \colon C \to B$ is injective.

Proposition 2.17. *Let $f : A \to B$ be surjective and let $D \subset B$.*
Then $f\restriction^D : f^{-1}(D) \to D$ is surjective.

Let $f : A \to B$ and let $D \subset B$. If $D \subset f(A)$, we normally refer to the constriction of f to D also as f. The reader should infer the meaning from the context.

6. Composition of Functions

Definition 2.18. Let $f : A \to B$ and $g : B \to C$. Then *composition of f and g* is the function

$$g \circ f : A \to C \quad \text{given by} \quad (g \circ f)(a) = g(f(a)).$$

The domain of $g \circ f$ is the domain of f and the target of $g \circ f$ is the target of g. The range of $g \circ f$ is the image under g of the image under f of the domain of f.

Proposition 2.19. *Let $f : A \to B$ and $g : B \to C$ be injective.*
Then $g \circ f : A \to C$ is injective.

Proof. To show that a function is injective, we select two elements in the domain and assume that they are sent to the same place; it then suffices to show that they were originally the same element.

Let $h = g \circ f$. Let $a_1, a_2 \in A$ and suppose that $h(a_1) = h(a_2) = c$. Let $b_1 = f(a_1)$ and let $b_2 = f(a_2)$. Since $h(a) = g(f(a))$ for each $a \in A$, we have $g(f(a_1)) = g(b_1)$ and $g(f(a_2)) = g(b_2)$. Thus $g(b_1) = g(b_2) = c$. Since g is injective, it follows that $b_1 = b_2$ by the definition of injectivity. Since f is injective, it follows that $a_1 = a_2$, again by definition. □

Problem 2.2. Let $f : A \to B$ and $g : B \to C$ be surjective.
Show that $g \circ f : A \to C$ is surjective.

The next proposition says that function composition is associative.

Proposition 2.20. *Let $f : A \to B$, $g : B \to C$, and $h : C \to D$.*
Then $h \circ (g \circ f) = (h \circ g) \circ f$.

Proof. By Proposition 2.6, to show that two functions with the same domain and target are equal, it suffices to show that they act the same way on an arbitrary element of the domain.

Let $a \in A$. Then

$$(h \circ (g \circ f))(a) = h(g \circ f(a)) = h(g(f(a)) = h \circ g(f(a) = ((h \circ g) \circ f)(a).$$

□

7. Identities and Inverses

Definition 2.21. Let A be a set. The *identity function* on A is defined to be

$$\mathrm{id}_A : A \to A \quad \text{given by} \quad \mathrm{id}_A(a) = a.$$

Proposition 2.22. *Let $f : A \to B$. Then $f \circ \mathrm{id}_A = f$ and $\mathrm{id}_B \circ f = f$.*

Definition 2.23. Let $f : A \to B$. We say that f is *invertible* if there exists a function $g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. In this case we call g the *inverse* of f. The inverse of a function f is often denoted f^{-1}.

Proposition 2.24. *Let $f : A \to B$ be invertible with inverses $g_1, g_2 : B \to A$. Then $g_1 = g_2$.*

Proof. Since g_1 and g_2 are inverses for f, and function composition is associative, we have

$$g_1 = g_1 \circ \mathrm{id}_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_A \circ g_2 = g_2.$$

□

If $f : A \to B$ is invertible and $b \in B$, we have two definitions for the notation $f^{-1}(b)$; it could mean the preimage set or the preimage point. That is, if $f(a) = b$, then $f^{-1}(b)$ could mean $\{a\}$ or it could mean a. One must decide from the context which meaning is intended.

Proposition 2.25. *Let $f : A \to B$ be a function.*
Then f is invertible if and only if f is bijective.

Proof. We prove both directions of the double implication.

($\Rightarrow$) Suppose that f is invertible and let g be an inverse for f. We wish to show that f is bijective, so we show that f is both injective and surjective.

To show surjectivity, select an arbitrary element $b \in B$ and find an element $a \in A$ such that $f(a) = b$. We let $a = g(b)$. Thus $f(a) = f(g(b)) = \mathrm{id}_B(b) = b$. This shows that f is surjective.

To show injectivity, select two arbitrary elements $a_1, a_2 \in A$ and assume that $f(a_1) = f(a_2)$. Now it suffices to show that $a_1 = a_2$. Since $f(a_1) = f(a_2)$, we have $g(f(a_1)) = g(f(a_2))$. Thus $\mathrm{id}_A(a_1) = \mathrm{id}_A(a_2)$, so that $a_1 = a_2$. Hence f is injective.

($\Leftarrow$) Suppose that f is bijective. We wish to show that f is invertible. Since f is surjective, for each $b \in B$, there exists $\widehat{b} \in A$ such that $f(\widehat{b}) = b$. Since f is injective, $\widehat{b}$ is unique with this property. Define a function $g : B \to A$ by $b \mapsto \widehat{b}$.

Let $b \in B$. Then have $f(g(b)) = f(\widehat{b}) = b$, so $f \circ g = \mathrm{id}_B$.

Let $a \in A$ and set $b = f(a)$. Then $a = \widehat{b}$ and $g(f(a)) = g(b) = \widehat{b} = a$, so $g \circ f = \mathrm{id}_A$. This completes the proof. □

8. Retractions and Sections

Definition 2.26. Let $f : A \to B$. We say that f is *left invertible* if there exists $g : B \to A$ such that $g \circ f = \mathrm{id}_A$; we call g a *left inverse*, or *retraction*, of f.

Proposition 2.27. *Let $f : A \to B$. Then f is left invertible if and only if f is injective.*

Proof. We show both directions of the double implication.

($\Rightarrow$) Suppose that f is left invertible. To show that f is injective, we select $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$, and show that $a_1 = a_2$.

Since f is left invertible, there exists $g : B \to A$ such that $g \circ f = \mathrm{id}_A$. Then $f(a_1) = f(a_2)$ implies that $g(f(a_1)) = g(f(a_2))$. But $g \circ f = \mathrm{id}_B$, so $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$.

($\Leftarrow$) Suppose that f is injective. For each $b \in \mathrm{rng}(f)$, there exists $\widehat{b} \in A$ such that $f(\widehat{b}) = b$. Since f is injective, $\widehat{b}$ is unique with this property. Define a function $g : B \to A$ by $b \mapsto \widehat{b}$.

Let $a \in A$ and set $b = f(a)$. Then $a = \widehat{b}$ and $g(f(a)) = g(b) = \widehat{b} = a$, so $g \circ f = \mathrm{id}_A$. Thus g is a left inverse for f, and f is left invertible. This completes the proof. □

Definition 2.28. Let $f : A \to B$. We say that f is *right invertible* if there exists $g : B \to A$ such that $f \circ g = \mathrm{id}_B$; we call g a *right inverse*, or *section*, of f.

Proposition 2.29. *Let $f : A \to B$. Then f is right invertible if and only if f is surjective.*

Proof. We show both directions of the double implication.

($\Rightarrow$) Suppose that f is right invertible. Then there exists $g : B \to A$ such that $f \circ g = \mathrm{id}_B$. Let $b \in B$ and let $g(b) = a$. Then $f(a) = f(g(b)) = b$, so f is surjective.

($\Leftarrow$) Suppose that f is surjective. Let $A_b = f^{-1}(b)$, so that for $a \in A$, $a \in A_b$ means $f(a) = b$. Use Axiom 8 to create the set

$$\mathcal{C} = \{C \in \mathcal{P}(A) \mid C = A_b \text{ for some } b \in B\}.$$

Since f is surjective, the empty set is not an element of $\mathcal{C}$. By Axiom 10 (the Axiom of Choice), there exists a set E which contains exactly one element from each of the member of $\mathcal{C}$, so for every $b \in B$, there exists a unique $\widehat{b} \in E$ such that $\widehat{b} \in A_b$. Since $\widehat{b} \in A_b$, we have $f(\widehat{b}) = b$. Define a function $g : B \to A$ by $g(b) = \widehat{b}$.

Let $b \in B$. Then have $f(g(b)) = f(\widehat{b}) = b$, so $f \circ g = \mathrm{id}_B$. Thus g is a right inverse for f, and f is right invertible. □

The above proof employs our first use of Axiom 10 (the Axiom of Choice). It is traditional to point out when the Axiom of Choice is used, since it flags an essentially non-constructive argument.

Proposition 2.30. *Let $f : A \to B$ Then f is invertible if and only if f is both left invertible and right invertible.*

Proof. We have seen that f is invertible if and only if f is bijective, which means that f is both injective and surjective. But f is both injective and surjective if and only if f is both left invertible and right invertible. □

9. Monos and Epis

Definition 2.31. Let $f : A \to B$. We say that f is *monic*, or is a *mono*, if for every set X and functions $g_1, g_2 : X \to A$ satisfying $f \circ g_1 = f \circ g_2$, we have $g_1 = g_2$.

A function is monic if it is "left cancellable".

Proposition 2.32. *Let $f : A \to B$. Then f is injective if and only if f is monic.*

Proof. We prove both directions of the double implication.

($\Rightarrow$) Suppose f is injective, and let $g_1, g_2 : X \to A$ satisfy $f \circ g_1 = f \circ g_2$. Since f is injective, it is left invertible; let $h : B \to A$ be a left inverse of f, so that $h \circ f = \mathrm{id}_A$. Compose both sides of the equation $f \circ g_1 = f \circ g_2$ on the left with h to obtain $h \circ (f \circ g_1) = h \circ (f \circ g_2))$. Associativity of function composition produces $(h \circ f) \circ g_1 = (h \circ f) \circ g_2$. Thus $\mathrm{id}_A \circ g_1 = \mathrm{id}_A \circ g_2$, so $g_1 = g_2$. Therefore f is monic.

($\Leftarrow$) Here we prove the contrapositive; thus suppose f is not injective. Then there exist distinct elements $a_1, a_2 \in A$ with $f(a_1) = f(a_2) = b$ for some $b \in B$. For $i = 1, 2$, define $g_i : A \to A$ by $g_i(a) = a_i$. Since $a_1 \neq a_2$, $g_1 \neq g_2$. However, for $i = 1, 2$ and every $a \in A$, $f \circ g_i(a) = f(a_i) = b$; thus $f \circ g_1 = f \circ g_2$. Therefore f is not monic. □

Definition 2.33. Let $f : A \to B$. We say that f is *epic*, or is an *epi*, if for every set X and functions $g_1, g_2 : B \to X$ satisfying $g_1 \circ f = g_2 \circ f$, we have $g_1 = g_2$.

A function if epic if it is "right cancellable".

Proposition 2.34. *Let $f : A \to B$. Then f is surjective if and only if f is epic.*

Proof. We prove both directions of the double implication.

($\Rightarrow$) Suppose that f is surjective, and let $g_1, g_2 : B \to X$ satisfy $g_1 \circ f = g_2 \circ f$. Since f is surjective, it is right invertible; let $h : B \to A$ be a right inverse, so that $f \circ h = \mathrm{id}_B$. Composing $g_1 \circ f = g_2 \circ f$ on the right with h produces $(g_1 \circ f) \circ h = (g_2 \circ f) \circ h$. Associativity of function composition allows us to rewrite this as $g_1 \circ (f \circ h) = g_2 \circ (f \circ h)$. This implies $g_1 \circ \mathrm{id}_B = g_2 \circ \mathrm{id}_B$, so $g_1 = g_2$. Therefore f is epic.

($\Leftarrow$) Suppose that f is not surjective. Then there exists $c \in B$ such that c is not in the range of f. Let $Z = \varnothing$, $O = \{\varnothing\}$, and $X = \{Z, O\}$. Define functions

$$g_1 : B \to X \quad \text{given by} \quad g_1(b) = Z \quad \text{for all } b \in B;$$

$$g_2 : B \to X \quad \text{given by} \quad g_2(b) = \begin{cases} Z & \text{if } b \neq c; \\ O & \text{if } b = c. \end{cases}$$

Now $g_1(b) \neq g_2(b)$, so $g_1 \neq g_2$. However, for every $a \in A$ we have $g_1(f(a)) = Z$, and since $f(a) \neq b$, we also have $g_2(f(a)) = Z$. Thus $g_1 \circ f = g_2 \circ f$. Therefore f is not epic. □

10. Inclusions and Projections

Definition 2.35. Let A and X be nonempty sets such that $A \subset X$. The *inclusion map* from A to X is the function

$$\iota_A : A \to X \quad \text{given by} \quad \iota_A(a) = a.$$

Proposition 2.36. *Let A and X be sets such that $A \subset X$. Let $a \in A$ and consider the function*

$$\rho_a : X \to A \quad \textit{given by} \quad \rho_a(x) = \begin{cases} x & \textit{if } x \in A; \\ a & \textit{if } x \notin A. \end{cases}$$

Then ρ_a is a retraction of ι_A.

Definition 2.37. Let A and B be nonempty sets and let $X = A \times B$. The *projection map* from X to A is the function

$$\pi_A : X \to A \quad \text{given by} \quad \pi_A(a, b) = a.$$

Proposition 2.38. *Let A and B be nonempty sets and let $X = A \times B$. Let $b \in B$ and consider the function*

$$\sigma_b : A \to X \quad \textit{given by} \quad \sigma_b(a) = (a, b).$$

Then σ_b is a section of π_A.

11. Problems and Exercises

Problem 2.3. Let $f : X \to Y$ and $g : Y \to Z$ be surjective functions.
Show that $g \circ f : X \to Z$ is surjective.

Problem 2.4. Let $f : X \to Y$ and $g : Y \to Z$ be functions.

- **(a)** Show that if f is surjective and $g \circ f$ is injective, then g is injective.
- **(b)** Show that if g is injective and $g \circ f$ is surjective, the f is surjective.

Exercise 2.1. Let $f : X \to Y$ and $g : Y \to Z$ be functions. Refer to Problem 2.4.

- **(a)** Give an example where $g \circ f$ is injective but g is not.
- **(b)** Give an example where $g \circ f$ is surjective, but f is not.

Exercise 2.2. Let $f : X \to Y$ be a function and let $A, B \subset X$.
In reference to Proposition 2.9, give an example where $f(A \cap B) \neq f(A) \cap f(B)$.

Exercise 2.3. Let P be the set of all people who ever lived (assume P is a set). Which of the following sets is the graph of a function from P to P?

- **(a)** $\{(a, b) \in P \times P \mid b \text{ is a father of } a\}$
- **(b)** $\{(a, b) \in P \times P \mid a \text{ is a father of } b\}$
- **(c)** $\{(a, b) \in P \times P \mid b \text{ is a grandmother of } a\}$
- **(d)** $\{(a, b) \in P \times P \mid b \text{ is a youngest son of the paternal grandmother of } a\}$
- **(e)** $\{(a, b) \in P \times P \mid b \text{ is a youngest son of the maternal grandmother of } a\}$

Exercise 2.4. Let $\mathbb{N}$ be the set of natural numbers and let $\mathbb{Z}$ be the integers. Find examples of functions $f : \mathbb{Z} \to \mathbb{N}$ such that:

- **(a)** f is bijective;
- **(b)** f is injective but not surjective;
- **(c)** f is surjective but not injective;
- **(d)** f is neither injective nor surjective.

Exercise 2.5. Let $\mathbb{N}$ be the set of natural numbers. Let A be a subset of $\mathbb{N}$ given by $A = [50, 70] \cap \mathbb{N}$, where $[50, 70]$ is an interval of real numbers between 50 and 70, including the endpoints. Define a function $f : \mathbb{N} \to \mathbb{N}$ by $f(n) = 3n$. Note that A is in both the domain and the target of f.

- **(a)** Find the image $f(A)$.
- **(b)** Find the preimage $f^{-1}(A)$.
- **(c)** Show that f is injective.
- **(d)** Show that f is not surjective.

Exercise 2.6. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^3 - 6x^2 + 11x - 3$.
Find $f^{-1}(\{3\})$.

Exercise 2.7. We would like to define a function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$ by $(p, q) \mapsto \frac{p}{q}$. Unfortunately, this does not make sense. Fix the problem, and show that the resulting function is surjective but not injective.

Exercise 2.8. We would like to define a function $f : \mathbb{Q} \to \mathbb{Z}$ by $\frac{p}{q} \mapsto pq$. Unfortunately, this is not "well-defined". Figure out what this means and fix the problem. Is the resulting function injective?

CHAPTER 3

Collections

1. Collections

Definition 3.1. A *collection* is a set whose elements are sets.

In our axiomatic approach, the elements of any set are themselves sets. So, there is no logical distinction between sets and collections. We use the word to emphasize that we may be looking inside the sets that are elements of a given collection.

By convention, we often used a script font like $\mathcal{A}$, $\mathcal{B}$, or $\mathcal{C}$ to further emphasize that we are working with a collection.

Definition 3.2. Let $\mathcal{C}$ be a collection.

The *union* of $\mathcal{C}$ is

$$\cup\mathcal{C} = \{a \mid a \in A \text{ for some } A \in \mathcal{C}\}.$$

The *intersection* of $\mathcal{C}$ is

$$\cap\mathcal{C} = \{a \mid a \in A \text{ for all } A \in \mathcal{C}\}.$$

Proposition 3.3. *Let $\mathcal{C}$ be a collection. Then $\cup\mathcal{C}$ and $\cap\mathcal{C}$ are sets.*

Proof. That $\cup\mathcal{C}$ is a set is exactly Axiom 4. Then apply Axiom 8 to see that

$$\cap\mathcal{C} = \{a \in \cup\mathcal{C} \mid a \in A \text{ for all } A \in \mathcal{C}\}$$

is a set. □

Example 3.1. Let $A = \{n \in \mathbb{N} \mid n < 25\}$, $O = \{n \in A \mid n \text{ is odd}\}$, $P = \{n \in A \mid n \text{ is prime}\}$, and $S = \{n \in A \mid n \text{ is a square}\}$. Let $\mathcal{C} = \{O, P, S\}$. Then

- $\cap\mathcal{C} = \varnothing$, because no square is a prime;
- $\cup\mathcal{C} = \{2, 3, 4, 5, 7, 9, 11, 13, 15, 16, 17, 19, 21, 23\}$.

Proposition 3.4. *Let $\mathcal{A}$ and $\mathcal{B}$ be collections. Then*

$$\cup(\mathcal{A} \cup \mathcal{B}) = (\cup\mathcal{A}) \cup (\cup\mathcal{B}).$$

2. Power Sets

Definition 3.5. Let X be a set. The *power set* of X is

$$\mathcal{P}(X) = \{A \mid A \subset X\};$$

the is the collection of all subsets of X.

Proposition 3.6. *Let X be a set. Then $\mathcal{P}(X)$ is a set.*

Proof. This is exactly Axiom 6 (the Axiom of Powers). □

Example 3.2. The power set of a set X is the set of all subsets of X. Here are a few examples:

- $X = \varnothing \Rightarrow \mathcal{P}(X) = \{\varnothing\}$;
- $X = \{0\} \Rightarrow \mathcal{P}(X) = \{\varnothing, \{0\}\}$;
- $X = \{0, 1\} \Rightarrow \mathcal{P}(X) = \{\varnothing, \{0\}, \{1\}, X\}$;
- $X = \{0, 1, 2\} \Rightarrow \mathcal{P}(X) = \{\varnothing, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, X\}$.

Proposition 3.7. *Let A and B be sets. Then*

- $B \subset A \Rightarrow \mathcal{P}(B) \subset \mathcal{P}(A)$;
- $\cap\mathcal{P}(A) = \varnothing$;
- $\cup\mathcal{P}(A) = X$.

Proposition 3.8. (DeMorgan's Laws)
Let X be a set and let $\mathcal{A} \subset \mathcal{P}(X)$. Let

$$\mathcal{C} = \{C \in \mathcal{P}(X) \mid C = X \setminus A \text{ for some } A \in \mathcal{A}\}.$$

Then

(a) $X \setminus \cap\mathcal{A} = \cup\mathcal{C}$;
(b) $X \setminus \cup\mathcal{A} = \cap\mathcal{C}$.

3. Mapping Sets

Proposition 3.9. *Let A and B be sets. Then there exists a set of all mappings from A to B.*

Proof. A mapping is a set of the form $r = ((A, B), R)$, with $R \subset A \times B$. We see that (A, B) is a set, so $\{(A, B)\}$ is a set. Also $R \in \mathcal{P}(A \times B)$, which is a set. Thus $U = \{(A, B)\} \times \mathcal{P}(A \times B)$ is a set, and $r \in U$. So by Axiom 8,

$$\{r \in U \mid r \text{ is a mapping}\}$$

is a set, and is the set of all mappings on A. □

4. Function Sets

Definition 3.10. Let A and B be sets. The *function set* from A to B is

$$\mathcal{F}(A, B) = \{f : A \to B\};$$

this is the collection of all functions from A to B.

Proposition 3.11. *Let A and B be sets. Then $\mathcal{F}(A, B)$ is a set.*

Proof. As usual, we need to find a big set in which all such functions live, then apply the Axiom of Specification.

Let $f : A \to B$. According to Definition 2.4, $f = ((A, B), F)$, where F is a certain type of subset of $A \times B$. Now (A, B) is a set by Proposition 1.24, so $\{(A, B)\}$ is a set by Proposition 1.3. Also $\mathcal{P}(A \times B)$ is a set by Proposition 3.6, and $F \in \mathcal{P}(A \times B)$. Finally, set $U = \{(A, B)\} \times \mathcal{P}(A \times B)$; this is a set by 1.27, and $f \in \{(A, B)\} \times \mathcal{P}(A \times B)$. Thus

$$\mathcal{F}(A, B) = \{f \in U \mid f \text{ is a function}\}$$

is a set by Axiom 8. □

Example 3.3. Let $A = \{1, 2\}$ and $B = \{5, 6, 7\}$. Then $\mathcal{F}(A, B)$ contains the following functions:

- $1 \mapsto 5$ and $2 \mapsto 5$;
- $1 \mapsto 5$ and $2 \mapsto 6$;
- $1 \mapsto 5$ and $2 \mapsto 7$;
- $1 \mapsto 6$ and $2 \mapsto 5$;
- $1 \mapsto 6$ and $2 \mapsto 6$;
- $1 \mapsto 6$ and $2 \mapsto 7$;
- $1 \mapsto 7$ and $2 \mapsto 5$;
- $1 \mapsto 7$ and $2 \mapsto 6$;
- $1 \mapsto 7$ and $2 \mapsto 7$.

Also $\mathcal{F}(B, A)$ contains the following functions:

- $5 \mapsto 1$, $6 \mapsto 1$, $7 \mapsto 1$;
- $5 \mapsto 1$, $6 \mapsto 1$, $7 \mapsto 2$;
- $5 \mapsto 1$, $6 \mapsto 2$, $7 \mapsto 1$;
- $5 \mapsto 1$, $6 \mapsto 2$, $7 \mapsto 2$;
- $5 \mapsto 2$, $6 \mapsto 1$, $7 \mapsto 1$;
- $5 \mapsto 2$, $6 \mapsto 1$, $7 \mapsto 2$;
- $5 \mapsto 2$, $6 \mapsto 2$, $7 \mapsto 1$;
- $5 \mapsto 2$, $6 \mapsto 2$, $7 \mapsto 2$.

Definition 3.12. Let X be a set. A *permutation* of X is a bijective function $\phi : X \to X$. The set of permutations of X is

$$\mathrm{Sym}(X) = \{\phi : X \to X \mid \phi \text{ is bijective } \}.$$

Proposition 3.13. *Let X be a set. Then* $\mathrm{Sym}(X)$ *is a set.*

Proof. Actually,

$$\mathrm{Sym}(X) = \{\phi \in \mathcal{F}(X, X) \mid \phi \text{ is bijective}\},$$

which is a set by Axiom 8. □

5. Characteristic Functions

Eventually we will define zero to be the empty set, one to be the set which contains the empty set, and two to be the set which contains zero and one. So Z, O, and T in the next definition actually will be 0, 1, and 2.

Definition 3.14. Let A and X be sets. Let $Z = \varnothing$, $O = \{\varnothing\}$, and $T = \{Z, O\}$. The *characteristic function* of A on X is defined to be

$$\chi_A : X \to T \quad \text{given by} \quad \chi_A(x) = \begin{cases} Z & \text{if } x \notin A; \\ O & \text{if } x \in A. \end{cases}$$

Let X be any set and let $T = \{Z, O\}$. A given function $f : X \to T$ may be viewed as a subset of X by thinking of f as saying, for a given element, whether or not it is in the subset. The element O is thought of as "ON" and the element Z is thought of as "OFF". Specifically, given $f : X \to T$, define A to the preimage of O:

$$A = \{x \in X \mid f(x) = O\};$$

that is, $A = f^{-1}(O)$.

On the other hand, given a subset of X, we can construct a function $\chi_A : X \to T$ by defining $\chi_A(x) = O$ if $x \in A$, and $\chi_A(x) = Z$ otherwise. This is just the characteristic function of the subset A.

Thus the power set of X corresponds to the set of functions from X into T in a natural way. Another way of stating this is that there exists a bijective function between $\mathcal{P}(X)$ and $\mathcal{F}(X,T)$. We now give a formal proof of this.

Proposition 3.15. *Let X be a set. Define a function*

$$\chi : \mathcal{P}(X) \to \mathcal{F}(X,T) \quad \textit{given by} \quad \chi(A) = \chi_A.$$

Then χ is a bijective function.

Proof. We prove that χ is injective and surjective.

Let $A, B \subset X$ such that $\chi(A) = \chi(B)$ so that $\chi_A = \chi_B$; we wish to show that $A = B$. Let $a \in A$. Then $\chi_A(a) = O$, so $\chi_B(a) = O$, so $a \in B$. Thus $A \subset B$, and similarly, $B \subset A$. Thus $A = B$, so χ is injective.

Let $f : X \to T$ be an arbitrary member of $\mathcal{F}(X,T)$. Let

$$A = \{x \in X \mid f(x) = O\}$$

Now if $x \in A$, $f(x) = O$, and if $x \notin A$, then $f(x) \neq O$; but since $f(x) \in T$, $f(x) = Z$. Thus f is the characteristic function of A, so $\chi(A) = f$. Thus χ is surjective. □

6. Products

An element of the cartesian product of two distinct sets may be viewed as a choice of one element from each set. To generalize this idea, we would like the product of a collection of sets to be the set of all possible ways of selecting one element from each set.

Definition 3.16. Let $\mathcal{C}$ be a nonempty collection of nonempty sets. The *product* of $\mathcal{C}$, denoted $\times\mathcal{C}$, is the set of all functions from $\mathcal{C}$ to $\cup\mathcal{C}$ such that each member of $\mathcal{C}$ is mapped to an element of itself:

$$\times\mathcal{C} = \{f \in \mathcal{F}(\mathcal{C}, \cup\mathcal{C}) \mid f(C) \in C \text{ for all } C \in \mathcal{C}\}.$$

Proposition 3.17. *Let $\mathcal{C}$ be a nonempty collection of nonempty sets. Then $\times\mathcal{C}$ is a nonempty set.*

Proof. Since $\times\mathcal{C}$ was constructed using Axiom 8 (the Axiom of Specification), it is a set. By Axiom 10 (the Axiom of Choice), there exists a set E which consists of exactly one member of each set in $\mathcal{C}$. That is, for $C \in \mathcal{C}$, $C \cap E = \{e_C\}$ for some unique element $e_C \in C$. Since $E \subset \cup\mathcal{C}$, this produces a function

$$f : \mathcal{C} \to \cup\mathcal{C} \quad \text{given by} \quad f(C) = e_C.$$

Thus $f \in \times\mathcal{C}$, so $\times\mathcal{C}$ is nonempty. □

Let $f \in \times\mathcal{C}$. For each $C \in \mathcal{C}$, we have $f(C) \in C$. Thus f picks one element out of each of the sets in $\mathcal{C}$. This is what we want to cartesian product to be: it is the set of all possible ways to pick one element out of each of the constituent sets.

We needed to define the cartesian product of two sets in order to define the concept of function, and now we use the concept of function to generalize the concept of product to more than two sets.

Next we show how to identify our previous definition of cartesian product with our new definition of product.

Proposition 3.18. *Let A and B be nonempty sets, and let $\mathcal{C} = \{A, B\}$. Define a function*

$$\Gamma : \times\mathcal{C} \to A \times B \quad \text{given by} \quad \Gamma(f) = (f(A), f(B)).$$

Then Γ is bijective.

Proof. Let $f_1, f_2 \in \times\mathcal{C}$ such that $\Gamma(f_1) = \Gamma(f_2)$ To show that Γ is injective, we wish to show that $f_1 = f_2$. Since f_1 and f_2 are functions from $\mathcal{C}$ to $\cup\mathcal{C}$, they have the same domain and target, so Proposition 2.6 says that it suffices to show that $f_1(C) = f_2(C)$ for every $C \in \mathcal{C}$.

Now $\Gamma(f_1) = \Gamma(f_2)$ implies $(f_1(A), f_1(B)) = (f_2(A), f_2(B))$, so by Proposition 1.25, $f_1(A) = f_2(A)$ and $f_1(B) = f_2(B)$. Since $\mathcal{C} = \{A, B\}$, $f_1(C) = f_2(C)$ for every $C \in \mathcal{C}$. Thus $f_1 = f_2$, and Γ is injective.

Let $(a, b) \in A \times B$. To show that Γ is surjective, we wish to find $f \in \times\mathcal{C}$ such that $\Gamma(f) = (a, b)$. We know that $a \in A$ and $b \in B$, and we define

$$f : \mathcal{C} \to \cup\mathcal{C} \quad \text{by} \quad f(C) = \begin{cases} a & \text{if } C = A; \\ b & \text{if } C = B. \end{cases}$$

Then $f \in \times\mathcal{C}$, and $\Gamma(f) = (a, b)$. □

7. Coproducts

We would like to produce a set which is similar to taking the union of a collection of sets, without merging the overlapping elements. The concept of coproduct is the mathematicians response to this desire.

Definition 3.19. Let $\mathcal{C}$ be a nonempty collection of nonempty sets. The *coproduct* of $\mathcal{C}$, denoted $\sqcup\mathcal{C}$, is the set of all ordered pairs (C, c), where $C \in \mathcal{C}$ and $c \in C$:

$$\sqcup\mathcal{C} = \{(C, c) \mid C \in \mathcal{C} \text{ and } c \in C\}.$$

Proposition 3.20. *Let $\mathcal{C}$ be a nonempty collection of nonempty sets. Then $\sqcup\mathcal{C}$ is a nonempty set.*

Proof. To show that $\sqcup\mathcal{C}$ is a set, we need to find a set which we know contains all the elements of the form (C, c). But this is easy, since $c \in \cup\mathcal{C}$, so $(C, c) \in \mathcal{C} \times \cup\mathcal{C}$, and

$$\sqcup\mathcal{C} = \{(C, c) \mid C \in \mathcal{C} \text{ and } c \in C\}$$

is a set.

Now since $\mathcal{C}$ is nonempty, there exists some $C \in \mathcal{C}$; also by hypothesis, C is nonempty, so there exists some $c \in C$. Now $(C, c) \in \sqcup\mathcal{C}$, so $\sqcup\mathcal{C}$ is nonempty. □

Coproduct is sometimes called *disjoint union*. An example is the best way to see why this is so.

Example 3.4. Let $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$. Let $\mathcal{C} = \{A, B\}$. Then

$$\cup\mathcal{C} = \{1, 2, 3, 4\};$$
$$\sqcup\mathcal{C} = \{(A, 1), (A, 2), (A, 3), (B, 2), (B, 3), (B, 4)\}.$$

The coproduct contains a distinct element for each element of each set, so it is like taking the union of disjoint sets.

8. Families

Collections are a convenient way of dealing with lots of distinct sets which are not listed in any particular order. However, we often wish to consider multiple copies of the same set, or to force each set into a particular position in some ordering. The concept of family allows us to do these things.

Definition 3.21. Let I and X sets. A *family of subsets of X indexed by I* is a function

$$A : I \to \mathcal{P}(X).$$

For $i \in I$, the set $A(i)$ is usually denoted A_i. The image of the family is written

$$\text{img}(I) = \{A_i \mid i \in I\};$$

this image is the *collection induced by the family.*

It is often written, "Let $\{A_i \mid i \in I\}$ be a family of sets." What is meant by this is that $\{A_i \mid I\}$ is the image of a family of sets.

Every collection $\mathcal{C}$ can be written as a family by taking $I = \mathcal{C}$. However, families admit constructions which are not possible with collections, because the same set can be repeated in a family and not in a collection. Then products and coproducts of families actually differ from products and coproducts of the induced collection.

Definition 3.22. Let $A : I \to \mathcal{P}(X)$ be a family of subsets of X. Let $\mathcal{A} = \text{img}(I)$ be the collection induced by the family.

The *union* of the family is

$$\cup_{i \in I} A_\alpha = \cup \mathcal{A}.$$

The *intersection* of the family is

$$\cap_{i \in I} A_\alpha = \cap \mathcal{A}.$$

The *product* of the family is

$$\times_{i \in I} A_i = \{f \in \mathcal{F}(I, \cup \mathcal{A}) \mid f(i) \in A_i\}.$$

The *coproduct* of the family is

$$\sqcup_{i \in I} A_i = \{x \in \mathcal{A} \times \cup \mathcal{A} \mid x = (i, a) \text{ for some } i \in I \text{ and some } a \in A_i\}.$$

Proposition 3.23. *The union, intersection, product, and coproduct of a family of nonempty sets are nonempty sets.*

Proposition 3.24. (DeMorgan's Laws)
Let $\{A_i \mid i \in I\}$ be a family of sets. Then

(a) $\cap_{i \in I}(X \setminus A_i) = X \setminus \cup_{i \in I} A_i$;
(b) $\cup_{i \in I}(X \setminus A_i) = X \setminus \cap_{i \in I} A_i$.

Example 3.5. Let A be a nonempty set and let $I = \{1, 2, 3\}$. Consider the family $\{A_1, A_2, A_3\}$ where $A_i = A$ for $i = 1, 2, 3$. Then $\times_{i=1}^{3} A_i$ may be viewed as the set of ordered triples of elements of A. This construction is not possible with collections, since $\{A_1, A_2, A_3\} = \{A\}$.

9. Partitions

If we had a set of marbles in three different colors, the set of all marbles would consist of three disjoint subsets, one for each color. Partitions are the device used to study breaking sets up into non-overlapping blocks.

Definition 3.25. Let X be a set and let $\mathcal{C} \subset \mathcal{P}(X)$. We say that $\mathcal{C}$ *covers* X if $\cup\mathcal{C} = X$. We say that $\mathcal{C}$ is *mutually disjoint* if $\cap\mathcal{C} = \varnothing$. We say that $\mathcal{C}$ is *pairwise disjoint* if for every two distinct sets $C, D \in \mathcal{C}$, we have $C \cap D = \varnothing$.

Example 3.6. Let $X = \{1, 2, 3\}$ and let $\mathcal{C} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$. Then

$$\cup\mathcal{C} = (\{1, 2\} \cup \{2, 3\}) \cup \{2, 3\} = \{1, 2, 3\} \cup \{2, 3\} = \{1, 2, 3\} = X,$$

so the sets in $\mathcal{C}$ cover X. Also

$$\cap\mathcal{C} = (\{1, 2\} \cap \{1, 3\}) \cap \{2, 3\} = \{1\} \cap \{2, 3\} = \varnothing,$$

so the sets in $\mathcal{C}$ are mutually disjoint. They are not, however, pairwise disjoint.

Let $\mathcal{D} = \{\{1, 2\}, \{3\}\}$. Then $\mathcal{D}$ covers X with pairwise disjoint sets.

Definition 3.26. Let X be a set and let $\mathcal{R} \subset \mathcal{P}(X)$. We say that $\mathcal{R}$ is a *partition* of X if

- **(P0)** $\varnothing \notin \mathcal{R}$;
- **(P1)** $\cup\mathcal{R} = X$ ($\mathcal{R}$ covers X);
- **(P2)** $C \cap D = \varnothing$ for every distinct $C, D \in \mathcal{R}$ ($\mathcal{R}$ is pairwise disjoint).

The members of a partition are called *blocks*.

Proposition 3.27. *Let X be a set and let $\mathcal{R} \subset \mathcal{P}(X)$ be a partition of X. Let $x \in X$. Then there exists a unique element of $\mathcal{R}$ which contains x. We call this element the* block of x, *and denote it by* $[x]_{\mathcal{R}}$.

Proof. Since $\mathcal{R}$ covers X, x is in at least one member of $\mathcal{R}$. Now if there exist $C_1, C_2 \in \mathcal{R}$ such that $x \in C_1$ and $x \in C_2$, then $x \in C_1 \cap C_2$. Then $C_1 \cap C_2$ is nonempty, so $C_1 = C_2$, because the elements of the partition $\mathcal{R}$ are pairwise disjoint. Thus there is exactly one member of $\mathcal{R}$ which contains x. □

Example 3.7. Let x be a point in a space and let $S(x, r)$ be a sphere of radius r with center x. Then the collection $\mathcal{S} = \{S(x, r) \mid r \in \mathbb{R} \text{ and } r \geq 0\}$ is a partition of space; the blocks of this partition are spheres centered at x. This is true since each point in space has a unique distance from the point x.

Example 3.8. Let C be the set of cards in a deck and let S be the set of suits. That is, C contains 52 elements and $S = \{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\}$. There is a natural function $f : C \to S$ which sends a given card to its suit. The preimage of a suit under f is the set of cards in that suit, for example:

$$f^{-1}[\spadesuit] = \{2\spadesuit, 3\spadesuit, 4\spadesuit, 5\spadesuit, 6\spadesuit, 7\spadesuit, 8\spadesuit, 9\spadesuit, 10\spadesuit, \text{J}\spadesuit, \text{Q}\spadesuit, \text{K}\spadesuit, \text{A}\spadesuit\}.$$

Let $\mathcal{S} = \{f^{-1}(s) \mid s \in S\}$. Then $\mathcal{S}$ is a collection of subsets of C, each subset consisting of all the cards in a given suit. It is clear that $\mathcal{S}$ covers C and that the sets within $\mathcal{S}$ are pairwise disjoint. Thus $\mathcal{S}$ is a partition of C. This is a general phenomenon: functions induce partitions on their domains. We will explore this in depth later.

One more thing to notice here. There are as many elements in $\mathcal{S}$ as there are in S. Indeed, in some philosophical way, $\mathcal{S}$ is *essentially the same* as the set S.

10. Problems and Exercises

Problem 3.1. Let X be a set and let $A, B \subset X$.
(a) Show that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
(b) Show that $\mathcal{P}(A) \cup \mathcal{P}(B) \subset \mathcal{P}(A \cup B)$.

Problem 3.2. Let X be a set. Define a function $\phi : \mathcal{P}(X) \to \mathcal{P}(X)$ by $A \mapsto X \setminus A$. Show that ϕ is bijective.

Problem 3.3. Let X be a set and let $\beta \in \mathrm{Sym}(X)$.
(a) Show that $\beta \circ \phi \in \mathrm{Sym}(X)$ for every $\phi \in \mathrm{Sym}(X)$.
(b) Define $f : \mathrm{Sym}(X) \to \mathrm{Sym}(X)$ by $f(\phi) = \beta \circ \phi$. Show that f is bijective.

Exercise 3.1. Let X be a set and let $A, B \subset X$. In reference to Problem 3.1, find an example such that $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$.

Exercise 3.2. In reference to Proposition 3.4, find examples of collections $\mathcal{A}$ and $\mathcal{B}$ where $\cap(\mathcal{A} \cap \mathcal{B}) \neq (\cap\mathcal{A}) \cap (\cap\mathcal{B})$.

Exercise 3.3. Design a collection $\mathcal{C}$ of subsets of $\mathbb{N}$ such that
(1) $\mathcal{C}$ covers $\mathbb{N}$ ($\cup\mathcal{C} = \mathbb{N}$);
(2) distinct sets in $\mathcal{C}$ are disjoint ($C, D \in \mathcal{C}$ and $C \neq D \Rightarrow C \cap D = \varnothing$);
(3) each set $C \in \mathcal{C}$ contains infinitely many elements;
(4) $\mathcal{C}$ contains exactly 7 subsets of $\mathbb{N}$.

Recall a partition of $\mathbb{N}$ is a collection of sets satisfying the first two properties.

Exercise 3.4. Let $\mathbb{R}$ be the set of real numbers.
(a) Find a collection of subsets of $\mathbb{R}$ which covers $\mathbb{R}$ but whose members are not mutually disjoint.
(b) Find a collection of subsets of $\mathbb{R}$ which covers $\mathbb{R}$ and whose members are mutually disjoint but not pairwise disjoint.
(c) Find three different partitions of $\mathbb{R}$, each containing a different number of blocks.

Exercise 3.5. Let $X = \{1, 2, 3, 4, 5\}$ and let $Y = \{1, 2, 3\}$. Find five different partitions of the set $\mathcal{F}(X, Y)$, each of which contains three blocks.

Exercise 3.6. Let X be a set. Find an injective function $\phi : X \to \mathcal{P}(X)$.

Exercise 3.7. Let X be as set, and let $\phi : X \to \mathcal{P}(X)$. Construct a set $A \subset X$ which is not in the image of ϕ. Conclude that there does not exist a surjective function $\phi : X \to \mathcal{P}(X)$.

Exercise 3.8. Let X be a set containing n elements. Try to count the size of the set $\mathcal{P}(X)$.

Exercise 3.9. Let A and B be sets containing m and n elements respectively. Try to count the size of the set $\mathcal{F}(A, B)$.

Exercise 3.10. Let A be a set containing n elements. Try to count the size of the set $\mathcal{F}(A, A)$.

Exercise 3.11. Let X be a set containing n elements. Try to count the number of functions in $\mathrm{Sym}(X)$.

Exercise 3.12. Let X be a set containing n elements and let $\mathfrak{P}$ be the set of all partitions of X. Try to count the size of the set $\mathfrak{P}$ for $n = 1, 2, 3, 4$.

CHAPTER 4

Relations

1. Relations

Definition 4.1. Let A be a set. A *relation on* A is a subset $R \subset A \times A$. If R be a relation on A, we write aRb to mean $(a, b) \in R$.

Recall Definition 1.31, which says that if R is a set of ordered pairs, then its domain is

$$\mathrm{dom}(R) = \{a \mid (a, b) \in R \text{ for some } b\},$$

and its range is

$$\mathrm{rng}(R) = \{b \mid (a, b) \in R \text{ for some } a\}.$$

Example 4.1. The concept of "less than or equal to" can be expressed as a relation. Let $\mathbb{R}$ be the set of all real numbers. Let $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$. Then R is a relation, which in effect describes what it means for x to be less than or equal to y by listing all instances of this phenomenon.

Example 4.2. Let $\mathbb{R}$ be the set of all real numbers. Let

$$R = \left\{ (x, y) \in \mathbb{R} \times \mathbb{R} \,\middle|\, \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \right\}.$$

Then R is a relation on the set $\mathbb{R}$; we know that the graph of R is an ellipse. Note that $\mathrm{dom}(R) = [-a, a]$ and $\mathrm{rng}(R) = [-b, b]$.

Example 4.3. Suppose that A is the set of all inhabitants of some island. Let U be the subset of $A \times A$ given by $(a, b) \in U \Leftrightarrow a$ is the uncle of b. Let N be the subset of $A \times A$ given by $(a, b) \in N \Leftrightarrow a$ is the niece of b. Note that aNb does not imply bUa, nor does aUb imply aNb. However, if we had $S \subset A \times A$ given by $(a, b) \in T \Leftrightarrow a$ is the sibling of b, then $aSb \Leftrightarrow bSa$.

Normally, relations are denoted by symbols other than letters. Thus we adopt the convention that the symbol $\bowtie$ will denote a generic relation. Keep in mind that if $\bowtie$ is a relation on a set A, this means $\bowtie$ is a subset of $A \times A$.

2. Properties of Relations

Definition 4.2. Let $\bowtie$ be a relation on a set A.
The relation is *reflexive* if $a \bowtie a$ for all $a \in A$.
The relation is *symmetric* if $a \bowtie b$ implies $b \bowtie a$.
The relation is *transitive* if $a \bowtie b$ and $b \bowtie c$ implies $a \bowtie c$.
The relation is *antisymmetric* if $a \bowtie b$ and $b \bowtie a$ implies $a = b$.
The relation is *definite* if $a \bowtie b$ or $b \bowtie a$ for all $a, b \in A$.

Example 4.4. The relation "is the same person as" is reflexive, symmetric, and transitive; so is the relation "is the same height as". The relation "is the parent of" has none of these properties (except antisymmetry; think about why). The relation "is the ancestor of" is transitive, and if we allow that one is one's own ancestor, it is also reflexive and antisymmetric.

Proposition 4.3. *Let $\bowtie$ be a relation on a set A.*
If $\bowtie$ is reflexive, then $\mathrm{dom}(\bowtie) = A$.

Proof. Let $a \in A$. Since $\bowtie$ is reflexive, $a \bowtie a$. This means that $(a, a) \in \bowtie$, so $a \in \mathrm{dom}(\bowtie)$. □

Proposition 4.4. *Let $\bowtie$ be a relation on a set A.*
If $\bowtie$ is definite, then $\bowtie$ is reflexive.

Proof. Let $a \in A$, and set $b = a$. Since $\bowtie$ is definite, either $a \bowtie b$ or $b \bowtie a$. But $b = a$, so $a \bowtie a$. □

Definition 4.5. Let $\bowtie$ be a relation on a set A. Let $B \subset A$. The *restriction* of $\bowtie$ to B is

$$\bowtie|_B = \bowtie \cap (B \times B).$$

For $b, c \in B$, we still write $b \bowtie c$ to mean $(b, c) \in R \cap (B \times B)$.

Proposition 4.6. *Let $\bowtie$ be a relation on a set A, and let $B \subset A$. Then the restriction of $\bowtie$ to B is a relation on B. Moreover, if $\bowtie$ is reflexive, symmetric, transitive, antisymmetric, or definite on A, then it still has this property when restricted to B.*

The bulk of what we need to say in this chapter describes a certain type of relations known as an equivalence relation. The notion of equivalence relation may be the most fundamental abstract concept in mathematics, and mastering it is a prerequisite for defining numbers and studying abstract algebra and topology, or anything dependent on these topics.

However, we will also have need for certain types of order relations, so we discuss those first.

3. Order Relations

Definition 4.7. Let $\leq$ be a relation on a set A. We say that $\leq$ is a *partial order* if for all $a, b, c \in A$ we have

- **(O1)** $a \leq a$ (reflexivity);
- **(O2)** if $a \leq b$ and $b \leq a$, then $a = b$ (antisymmetry);
- **(O3)** if $a \leq b$ and $b \leq c$, then $a \leq c$ (transitivity).

A partial order $\leq$ is called a *total order* if additionally it satisfies

- **(O4)** either $a \leq b$ or $b \leq a$ for all $a, b \in A$ (definiteness).

We note that **(O1)** is included by **(O4)**, so it is unnecessary to address **(O1)** to show that a relation is a total order.

Proposition 4.8. *Let X be a set. The containment relation $\subset$ is a partial order on the power set $\mathcal{P}(X)$.*

Proof. This is an application of Proposition 1.10. □

Example 4.5. The containment relation on the power set is not a total order relation. For example, if $X = \{1, 2, 3, 4, 5\}$, then the subsets $\{1, 3, 5\}$ and $\{1, 2, 3\}$ are not related by inclusion.

Example 4.6. Familiar examples of totally ordered sets are the natural number $\mathbb{N}$, the integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, and the real numbers $\mathbb{R}$. The complex number $\mathbb{C}$ have no total ordering which is compatible with their algebraic structure. We do, however, have a several partial orderings on $\mathbb{C}$ which arise from their algebraic structure (think about what these could be).

Example 4.7. Let $X = \mathbb{Z} \times \mathbb{Z}$, and let $\leq$ be the standard total order on $\mathbb{Z}$. Define a relation $\prec$ on X by

$$(a, b) \prec (c, d) \;\Leftrightarrow\; (a \leq c) \wedge (b \leq d).$$

Show that $\prec$ is a partial order.

Solution. We wish to show that $\prec$ is reflexive, antisymmetric, and transitive.

(Reflexivity) Let $(a, b) \in X$. Then since $\leq$ is a total order, it is reflexive, so $a \leq a$ and $b \leq b$. Thus $(a, b) \prec (a, b)$, and R is reflexive.

(Antisymmetry) Let $(a, b), (c, d) \in X$ such that $(a, b)R(c, d)$ and $(c, d) \prec (a, b)$. Then $a \leq c$ and $c \leq a$. Since $\leq$ is antisymmetric, we have $a = c$. Similarly, $b = d$. Thus $(a, b) = (c, d)$, and R is antisymmetric.

(Transitivity) Let $(a, b), (c, d), (e, f) \in X$ and suppose that $(a, b) \prec (c, d)$ and $(c, d) \prec (e, f)$. Then $a \leq c$ and $c \leq e$. Since $\leq$ is transitive, we have $a \leq e$. Similarly, $b \leq f$. Thus $(a, b) \leq (e, f)$, and R is transitive. □

Remark. Graph the set $X = \mathbb{Z} \times \mathbb{Z}$, so that we may visualize the set X as a set of discrete points in the plane $\mathbb{R}^2$. If we graph the point (a, b), the set of points in X greater than (a, b) are those lying to the right and above the position of (a, b). □

Definition 4.9. When the symbol $\leq$ is used for a partial order on a set X, the following symbols are assumed to have the given meanings:

- $a < b$ means $a \leq b$ and $a \neq b$;
- $a \geq b$ means $b \leq a$;
- $a > b$ means $b < a$.

Definition 4.10. Let $\leq$ be a total order on a set X, and let $m \in X$.

We say that m is a *maximum* element of X if $x \leq m$ for every $x \in X$.

We say that m is a *minimum* element of X if $m \leq x$ for every $x \in X$.

If m is a maximum or a minimum, then we say that m is an *extremum*.

Proposition 4.11. *Let $\leq$ be a total order on a set X.*

If X has a maximum, it is unique, and is denoted by $\max X$.

If X has a minimum, it is unique, and is denoted by $\min X$.

Proof. Let $m_1, m_2 \in X$. Suppose m_1 and m_2 are maxima for X. Then $x \leq m_1$ and $x \leq m_2$ for every $x \in X$. Since m_1 and m_2 are both in X, this implies that $m_2 \leq m_1$ and $m_1 \leq m_2$. Thus, by antisymmetry, $m_1 = m_2$. The demonstration if m_1 and m_2 are minima is analogous. □

4. Equivalence Relations

Definition 4.12. Let A be a set and let $\sim$ be a relation on A. We say that $\sim$ is an *equivalence relation* if for all $a, b, c \in A$ we have

- **(E1)** $a \sim a$ (reflexivity);
- **(E2)** $a \sim b$ if and only if $b \sim a$ (symmetry);
- **(E3)** if $a \sim b$ and $b \sim c$, then $a \sim c$ (transitivity).

If $a, b \in A$ and $a \sim b$, we say that a and b are *equivalent*.

Example 4.8. Let A be a set and let

$$E = \{(a, b) \in A \times A \mid a = b\}.$$

The set E is sometimes called the *diagonal* of $A \times A$; it is simply the relation of equality. This is an equivalence relation.

Example 4.9. Let A be the set of all animals in the world. Define a relation $\sim$ on A by

$$a \sim b \Leftrightarrow a \text{ and } b \text{ are of the same species.}$$

Then $\sim$ is an equivalence relation on the set A. For certainly if an animal a is a pig, then it is a pig (reflexivity); if a and b are both pigs, then b and a are both pigs (symmetry); and if a and b are both pigs, and b and c are both pigs, then a and c are both pigs (transitivity). And so forth.

Example 4.10. Let $X = \mathbb{N} \times \mathbb{N}$. Define a relation $\sim$ on X by

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.$$

This is an equivalence relation.

Example 4.11. Let $\mathbb{Z}^\bullet = \mathbb{Z} \setminus \{0\}$ be the set of nonzero integers (we will develop the arithmetic properties of $\mathbb{Z}$ later). Let $X = \mathbb{Z} \times \mathbb{Z}^\bullet$. Define a relation $\sim$ on X by

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Show that this is an equivalence relation.

Solution. We wish to show that $\sim$ is reflexive, symmetric, and transitive.

(Reflexivity) Let $(a, b) \in X$. Then $ab = ba$ by commutativity of multiplication. This says that $(a, b) \sim (a, b)$, so $\sim$ is reflexive.

(Symmetry) Let $(a, b), (c, d) \in X$. Then

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow (c, d) \sim (a, b),$$

so $\sim$ is symmetric.

(Transitivity) Let $(a, b), (c, d), (e, f) \in X$. Suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad = bc$ and $ce = df$. Multiply the first equation by e and the second by b and apply commutativity of multiplication in the integers to obtain $ade = bce$ and $bce = bdf$. Then by transitivity of equality, we have $ade = bdf$. By cancellation, we have $ae = bf$. Thus $(a, b) \sim (e, f)$, and $\sim$ is transitive. □

5. Equivalence Classes

Definition 4.13. Let A be a set and let $\sim$ be an equivalence relation on A. Let $a \in A$. The *equivalence class* of a is

$$[a]_\sim = \{b \in A \mid a \sim b\}.$$

Proposition 4.14. *Let A be a set and let $\sim$ be an equivalence relation on A. Let $a \in A$. Then $a \in [a]_\sim$.*

Proposition 4.15. *Let A be a set and let $\sim$ be an equivalence relation on A. Let $a, b \in A$. The following conditions are equivalent:*

(i) $a \sim b$;
(ii) $a \in [b]_\sim$;
(ii) $[a]_\sim = [b]_\sim$.

Proof. Since implication is a transitive logical operator, it suffices to show that

$$\textbf{(i)} \Rightarrow \textbf{(ii)} \Rightarrow \textbf{(iii)} \Rightarrow \textbf{(i)}.$$

(**(i)** $\Rightarrow$ **(ii)**) Suppose $a \sim b$. Then by definition of equivalence class, $b \in [a]_\sim$.

(**(ii)** $\Rightarrow$ **(ii)**) Suppose that $a \in [b]_\sim$. Then $b \sim a$, and by symmetry, $a \sim b$.

To show that two sets are equal, we show that each is contained in the other. To show that a set is contained in another set, we select and arbitrary element of the first set, and show that it is in the second.

Let $x \in [a]_\sim$. Then $a \sim x$. Since $b \sim a$ and $a \sim x$, transitivity of $\sim$ implies that $b \sim x$. Thus $x \in [b]_\sim$.

Let $y \in [b]_\sim$. Then $b \sim y$. Since $a \sim b$ and $b \sim y$, transitivity of $\sim$ implies that $a \sim y$. Thus $y \in [a]_\sim$.

This completes the proof that $[a]_\sim = [b]_\sim$.

(**(iii)** $\Rightarrow$ **(i)**) Suppose that $[a]_\sim = [b]_\sim$. Now $b \in [b]_\sim$ by Proposition 4.14, so $b \in [a]_\sim$ because these sets are equal, so $a \sim b$ by definition of equivalence class. □

Example 4.12. Suppose A is the set of all animals in the world, and $\sim$ is the relation of being in the same species. Let p be a pig. Then $[p]_\sim$ is the set of all pigs in the world. One can see that if q is also a pig, then $[p]_\sim = [q]_\sim$. Also it is clear that if a is an anteater, then $[p]_\sim \cap [a]_\sim = \varnothing$. Note there is exactly one equivalence class $[x]_\sim$ for each species of animal on earth such that x is an animal of that species.

6. Equivalence Relations and Partitions

Equivalence relations are particularly important in mathematics, because they group the elements of a set into blocks such that the members of one of the blocks, although not exactly equal, are similar in some sense in which one may be interested. More precisely, equivalence relations induce partitions on sets.

Proposition 4.16. *Let A be a set and let $\sim$ be an equivalence relation on A. The collection of equivalence classes*

$$[A]_\sim = \{[a]_\sim \mid a \in A\}$$

is a partition of A, referred to as the partition induced by the equivalence relation.

Proof. First we note that $[A]_\sim$ is a set, because

$$[A]_\sim = \{B \in \mathcal{P}(A) \mid B = [a]_\sim \text{ for some } a \in A\},$$

which is a set by Axiom 8. We must shows that this collection satisfies conditions **(P0)**, **(P1)**, and **(P2)** of being a partition, according to Definition 3.26.

(P0) Let $B \in [A]_\sim$. Then $B = [a]_\sim$ for some $a \in A$, and $a \in B$. Thus $B \neq \varnothing$.

(P1) We wish to show that the equivalence classes cover A; that is, that A equals the union of the equivalence classes. Since each equivalence class is a subset of A, the union of the equivalence classes is a subset of A. So it remains to see that A is a subset of the union of the equivalence classes.

Let $a \in A$. By Proposition 4.14, $a \in [a]_\sim$, so $a \in \cup_{a\in A}[a]_\sim$. Since a was arbitrary, $A \subset \cup_{a\in A}[a]_\sim$.

(P2) We wish to show that the equivalence classes are pairwise disjoint. Thus let $a, b \in A$, so that $[a]_\sim$ and $[b]_\sim$ are arbitrarily chosen equivalence classes. We wish to show that either $[a]_\sim = [b]_\sim$, or that $[a]_\sim \cap [b]_\sim = \varnothing$. To do this, it suffices to assume that the intersection is nonempty, and show that the classes are equal.

Let $c \in [a]_\sim \cap [b]_\sim$. Then $a \sim c$ and $b \sim c$. By symmetry, $c \sim b$. By transitivity, since $a \sim c$ and $c \sim b$, we have $a \sim b$. Thus $[a]_\sim = [b]_\sim$ by Proposition 4.15. □

Proposition 4.17. *Let A be a set and let $\mathcal{R}$ be a partition of A.*
Define a relation $\ni$ on A by

$$a \ni b \Leftrightarrow b \in [a]_\mathcal{R},$$

where $[a]_\mathcal{R}$ denotes the unique member of $\mathcal{R}$ which contains a.
Then $\ni$ is an equivalence relation, referred to as the equivalence relation induced by the partition.

Proof. First we note that since $\mathcal{R}$ is a partition, Proposition 3.27 tells us that every element $a \in A$ is in exactly one member of $\mathcal{R}$, so there is no ambiguity in the notation $[a]_\mathcal{R}$.

Next we claim that or $a, b \in A$, $a \in [b]_\mathcal{R}$ if and only if $[a]_\mathcal{R} = [b]_\mathcal{R}$.
To see this, suppose that $a \in [b]_\mathcal{R}$. Then $[b]_\mathcal{R}$ is the unique member of the partition $\mathcal{R}$ which contains a. Since we are calling this member $[a]_\mathcal{R}$, we have $[a]_\mathcal{R} = [b]_\mathcal{R}$. On the other hand, we know that $a \in [a]_\mathcal{R}$, so if $[a]_\mathcal{R} = [b]_\mathcal{R}$, we have $a \in [b]_\mathcal{R}$.

Now we show that $\ni$ is reflexive, symmetric, and transitive.

We have $a \in [a]_\mathcal{R}$, so $a \ni a$. Thus $\ni$ is reflexive.

Suppose $a \ni b$. We wish to show that $b \ni a$. Now $a \ni b$ means that $b \in [a]_\mathcal{R}$, so $[a]_\mathcal{R} = [b]_\mathcal{R}$ by our claim. Thus $a \in [b]_\mathcal{R}$, whence $b \ni a$. Thus $\ni$ is symmetric.

Suppose that $a \ni b$ and $b \ni c$. Then $b \in [a]_\mathcal{R}$ and $c \in [b]_\mathcal{R}$. By the claim, $[b]_\mathcal{R} = [a]_\mathcal{R}$, so $c \in [a]_\mathcal{R}$, which is the meaning of $a \ni c$. Thus $\ni$ is transitive. □

We see that equivalence relations and partitions on a set A are essentially the same idea. Yet, they are not exactly the same; they are in one to one correspondence with each other. The next proposition formalizes this statement.

Proposition 4.18. *Let A be a nonempty set. Let $\mathfrak{E}$ be the set of all equivalence relations on A, and let $\mathfrak{R}$ be the set of all partitions of A. If $\sim$ is an equivalence relation on A, let $\mathcal{R}_\sim$ denote the partition induced by $\sim$. If $\mathcal{R}$ is a partition of A, let $\ni_\mathcal{R}$ denote the equivalence relation induced by $\mathcal{R}$. Define a function*

$$\Omega : \mathfrak{E} \to \mathfrak{R} \quad \text{by} \quad \sim \mapsto \mathcal{R}_\sim.$$

Then Ω is bijective, with inverse $\mathcal{R} \mapsto \ni_\mathcal{R}$.

Proof. Let $L = \mathcal{P}(A \times A)$; then L is the set of all relations on A. Thus $\mathfrak{E} = \{\sim \in L \mid \sim$ is an equivalence relation$\}$ is a set. Also $\mathfrak{R} = \{\mathcal{R} \in \mathcal{P}(\mathcal{P}(A)) \mid \mathcal{R}$ is a partition$\}$ is a set.

That $\Omega : \sim \mapsto \mathcal{R}_\sim$ is a meaningful function is clear from Proposition 4.16. We only have to show that $\mathcal{R} \mapsto \ni_\mathcal{R}$ is an inverse.

Thus let $\sim$ be an equivalence relation on A and let $\mathcal{R} = \mathcal{R}_\sim$ be the induced partition, whose blocks are the equivalence classes of $\sim$. If $[a]_\mathcal{R}$ denotes the unique block containing a, then $[a]_\sim = [a]_\mathcal{R}$.

Let $\ni$ be the equivalence relation induced by $\mathcal{R}$. We only have to show that $\sim$ equals $\ni$.

Refer to Proposition 2.2. Since $\sim$ and $\ni$ are both relations on A, it suffices to show that $\mathrm{grf}(\sim) = \mathrm{grf}(\ni)$. This amounts to showing, for every $a, b \in A$,

$$a \sim b \Leftrightarrow a \ni b.$$

Using the definition of $\sim$, $\mathcal{R}$, and $\ni$, we have

$$a \sim b \;\Leftrightarrow\; b \in [a]_\sim \;\Leftrightarrow\; b \in [a]_\mathcal{R} \;\Leftrightarrow\; a \ni b.$$

□

7. Equivalence Relations and Functions

Proposition 4.19. *Let $f : A \to B$ be a function. Define a relation $\approx$ on A by*

$$a \approx b \;\Leftrightarrow\; f(a) = f(b).$$

Then $\approx$ is an equivalence relation, referred to as the equivalence relation induced by the function.

Proof. We wish to show that $\approx$ is reflexive, symmetric, and transitive.

It is reflexive because $f(a) = f(a)$.

It is symmetric because $f(a) = f(b)$ implies $f(b) = f(a)$.

It is transitive because $f(a) = f(b)$ and $f(b) = f(c)$ implies $f(a) = f(c)$. □

Proposition 4.20. *Let $f : A \to B$ be a function. Let*

$$\mathcal{R} = \{f^{-1}(b) \mid b \in B\}.$$

Then $\mathcal{R}$ is a partition of A, referred to as the partition induced by the function f.

Proof. We point out that $\mathcal{R}$ is indeed a set by Axiom 8, because

$$\mathcal{R} = \{C \in \mathcal{P}(A) \mid C = f^{-1}(b) \text{ for some } b \in B\}.$$

Now Proposition 4.19 states that f induces an equivalence relation $\approx$, and Proposition 4.16 states that $\approx$ induces a partition. We see that $\mathcal{R}$ is the partition induced by $\approx$. □

Proposition 4.21. *Let $f : A \to B$ be a function. Define a relation $\approx$ on A by*

$$a_1 \approx a_2 \;\Leftrightarrow\; f(a_1) = f(a_2).$$

Then $\approx$ is an equivalence relation, referred by as the kernel equivalence induced by the function f.

Proof. Let $a_1, a_2, a_3 \in A$. Then $f(a_1) = f(a_1)$, so $a_1 \approx a_1$. Also if $a_1 \approx a_2$, then $f(a_1) = f(a_2)$, so $f(a_2) = f(a_1)$, and $a_2 \approx a_1$. Finally if $a_1 \approx a_2$ and $a_2 \approx a_3$, then $f(a_1) = f(a_2)$ and $f(a_2) = f(a_3)$. It follows that $f(a_1) = f(a_3)$, so $a_1 \approx a_3$. Thus the reflexivity, symmetry, and transitivity of $\approx$ follows from the corresponding property of equality. □

We summarize our last six propositions.

Let A be any nonempty set. An equivalence relation $\sim$ on A induces a partition $\mathcal{R}_\sim$ of A, whose blocks are the equivalence classes. Conversely, a partition $\mathcal{R}$ of A induces an equivalence relation $\ni_{\mathcal{R}}$ on A. This creates a bijective correspondence

$$\{\text{equivalence relations on } A\} \leftrightarrow \{\text{partitions of } A\}$$

given by

$$\sim \mapsto \mathcal{R}_\sim \quad \text{with inverse} \quad \mathcal{R} \mapsto \ni_{\mathcal{R}} .$$

A function $f : A \to B$ induces a partition on A, and it also induces an equivalence relation on A. The blocks of this partition, or the equivalence classes of this equivalence relation, are precisely the preimages of points in B under the map A.

Example 4.13. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = \sin x$. Then f induces an equivalence relation on $\mathbb{R}$ which is given by

$$x_1 \approx x_2 \;\Leftrightarrow\; x_2 - x_1 = k\pi \text{ for some } k \in \mathbb{Z}.$$

The blocks of the corresponding partition are the equivalence classes of this equivalence relation. Such a block consists of points scattered on the real line at a distance of π from each other. The set of all such blocks covers the real line.

Example 4.14. Let A be the set of animals on earth and let S be the set of species. Define a function $f : A \to S$ by sending an animal to the species of which it is a member. Then the partition of A induced by f is the collection of subsets of A consisting of blocks such that all the animals in one block are of the same species, and any two animals of the same species are in the same block.

8. Functions defined on Partitions

Definition 4.22. Let A be a set and let $\mathcal{R}$ be a partition of A. Let $C \in \mathcal{R}$. A *representative* of C is an element $a \in C$. We say that a *represents* C, or that a is a *choice of representative* for C.

A *parliament* for $\mathcal{R}$ is a set $R \subset A$ such that R contains exactly one representative of each block of $\mathcal{R}$.

It is frequently convenient to shorten our notation when the equivalence class or partition is understood. Thus we write for $a \in A$, we write $\overline{a}$ instead of $[a]_\sim$ or $[a]_{\mathcal{R}}$, and we write $\overline{A}$ instead of $[A]_\sim$ or $[A]_{\mathcal{R}}$ (note that $[A]_{\mathcal{R}}$ just means $\mathcal{R}$). This is referred to as BAR notation.

Let A be a set and let $\overline{A}$ be a partition of A. If $a \in A$, we denote the unique block which contains a by $\overline{a}$. Clearly a represents $\overline{a}$, but it is also true that if b is equivalent to a under the induced equivalence relation, then b also represent $\overline{a}$. Sometimes were call a parliament a "preferred set of representatives"

Suppose B is another set and we wish to define a function $\alpha : \overline{A} \to B$, and we do so by saying where each block $\overline{a} \in \overline{a}$ should be sent in B. Perhaps we use some formula or algorithm which depends on the choice of representative $a_1 \in \overline{a}$.

Then we better be certain that, if a_2 is another element representing $\overline{a}$, then the algorithm gives the same value for a_2 as it did for a_1.

Example 4.15. Let $X = \mathbb{R} \setminus \{0\}$ be the set of nonzero real numbers. Let $Y = \{x \in X \mid x > 0\}$ be the set of positive real numbers and let $Z = X \setminus Y$ be the set of negative real numbers. Then $\mathcal{X} = \{Y, Z\}$ is a partition of X.

If we attempt to define a function $f : \mathcal{X} \to \mathbb{Z}$ by $[x] \mapsto x^2$, this doesn't make sense, since $\overline{1} = \overline{2}$, but $f(\overline{1}) = 1$ and $f(\overline{2}) = 4$.

However, if we attempt to define a function $g : \mathcal{X} \to \mathbb{Z}$ by $\overline{x} \mapsto \frac{x}{|x|}$, this function does make sense, since the entire block of positive numbers is sent to 1 and the entire block of negative number is sent to -1.

Definition 4.23. Let A be a set and let $\overline{A}$ be a partition of A. Let $f : A \to B$ be a function. Suppose we define $\overline{f} : \overline{A} \to B$ by specifying $\overline{f}(\overline{a}) = f(a) \in B$. We say that $\overline{f}$ is *well-defined* if $f(a_1) = f(a_2)$ whenever $\overline{a_1} = \overline{a_2}$.

Example 4.16. Let V be the set of vertebrate animals in the world and let $\overline{V}$ be the set of equivalence classes of vertebrates of the same species.

Let $T = \{\text{fish}, \text{amph}, \text{rept}, \text{bird}, \text{mamm}\}$ be the set of types of vertebrates. Attempt to define $f : \overline{V} \to B$ by

$$f(\overline{v}) = \begin{cases} \text{fish} & \text{if } v \text{ is a fish;} \\ \text{amph} & \text{if } v \text{ is an amphibian;} \\ \text{rept} & \text{if } v \text{ is a reptile;} \\ \text{bird} & \text{if } v \text{ is a bird;} \\ \text{mamm} & \text{if } v \text{ is a mammal.} \end{cases}$$

Then f is well-defined, since all the vertebrates of the same species are of the same type. However, if we attempt to define $g : \overline{V} \to \mathbb{R}$ by

$$g(\overline{v}) = \text{ the mass of } v \text{ in grams ,}$$

then g is not well-defined, because not every vertebrate of the same species has the same mass.

9. Canonical Functions

Definition 4.24. Let A be a set and let $\overline{A}$ be a partition of A. Let $\overline{a}$ denote the block containing $a \in A$. The *canonical function* is

$$\widehat{f} : A \to \overline{A} \quad \text{given by} \quad \widehat{f}(a) = \overline{a}.$$

The canonical function simply sends each element of A to the block containing it. That is, each element is sent to its equivalence class in the equivalence relation corresponding to the partition.

The next proposition is a prototype for some of the most powerful basic theorems in group theory, ring theory, topology, and category theory in general.

Theorem 4.25. (Isomorphism Theorem in the Category of Sets) *Let $f : A \to B$ be a surjective function. Let $\overline{A}$ denote the set of equivalence classes induced by f, and let $\overline{a}$ denote the equivalence class of $a \in A$. Define functions*

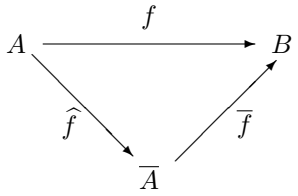
$$\widehat{f} : A \to \overline{A} \quad \textit{given by} \quad a \mapsto \overline{a}.$$

and

$$\overline{f} : \overline{A} \to B \quad \textit{given by} \quad \overline{a} \mapsto f(a).$$

Then

(a) $\widehat{f}$ *is surjective;*
(b) $\overline{f}$ *is well-defined and bijective;*
(c) $f = \overline{f} \circ \widehat{f}$.



Proof. Let $C \in \overline{A}$. Since $\overline{A}$ is a partition, C is nonempty. Let $a \in C$; then $\widehat{f}(a) = C$. Thus $\widehat{f}$ is surjective.

By definition of $\overline{A}$, $\overline{a_1} = \overline{a_2}$ if and only if $f(a_1) = f(a_2)$. This shows that $\overline{f}$ is well-defined and injective. Now if $b \in B$, then since f is surjective, $b = f(a)$ for some $a \in A$. Then $\overline{f}(\overline{a}) = b$. Thus $\overline{f}$ is surjective.

Finally, for $a \in A$, we have $\overline{f}(\widehat{f}(a)) = \overline{f}(\overline{a}) = f(a)$ by definition of $\overline{f}$. It follows that $\overline{f} \circ \widehat{f} = f$. □

Example 4.17. Let A be the set of animals on earth and let S be the set of species. Let $f : A \to S$ be given by sending an animal to its species. Let $\overline{A}$ be the partition of A into subsets of A which contain all of the animals of a given species. Then $\overline{A}$ is the partition of A induced by f. Let $\widehat{f} : A \to \overline{A}$ be the canonical function which sends an animal to the block which contains it. One can easily see that such blocks naturally correspond to the set of species. The bijective function $\overline{f}$, whose existence is guaranteed by the above theorem, sends each block to the species to which the animals in the block belong.

10. Problems and Exercises

Problem 4.1. Let $f : A \to B$ be an injective function. Let $\leq$ be a total order on B, and define a relation $\preccurlyeq$ on A by

$$a_1 \preccurlyeq a_2 \Leftrightarrow f(a_1) \leq f(a_2).$$

Show that $\preccurlyeq$ is a total order on A.

Exercise 4.1. Let $f : A \to B$ be a function. Let $\leq$ be a total order on B, and define a relation $\preccurlyeq$ on A by

$$a_1 \preccurlyeq a_2 \Leftrightarrow f(a_1) \leq f(a_2).$$

In reference to Problem 4.1, give an example where f is not injective and $\preccurlyeq$ is not a partial order on A.

Exercise 4.2. Let X be a set and let $\mathcal{C} \subset \mathcal{P}(X)$. Define a relation $\preccurlyeq$ on $\mathcal{C}$ by

$$A \preccurlyeq B \Leftrightarrow \exists \text{ injective } f : A \to B.$$

Is $\preccurlyeq$ a partial order on $\mathcal{C}$?

Exercise 4.3. Let X be a set and let $\mathcal{C} \subset \mathcal{P}(X)$. Define a relation $\sim$ on $\mathcal{C}$ by

$$A \sim B \Leftrightarrow \exists \text{ bijective } f : A \to B.$$

Show that $\sim$ is an equivalence relation.

Exercise 4.4. Let $\mathcal{C} \subset \mathcal{P}(\mathbb{R}^2)$ be the collection of all circles in the cartesian plane. Define a relation $\preccurlyeq$ on $\mathcal{C}$ by

$$C_1 \preccurlyeq C_2 \Leftrightarrow C_1 \text{ is inside } C_2.$$

Is $\preccurlyeq$ a partial order on $\mathcal{C}$?

Exercise 4.5. A *circle in the cartesian plane* is a subset of $\mathbb{R}^2$ which is the set of all points equidistant from a given point, called its *center*; the common distance is called the *radius* of the circle. If $C \subset \mathbb{R}^2$ is a circle and $A \subset \mathbb{R}^2$, we say that A is *inside* C if for each $a \in A$, the distance from a to the center of C is less than or equal to the radius of the circle.

Let $\mathcal{C} \subset \mathcal{P}(\mathbb{R}^2)$ be the collection of all circles in the cartesian plane. Define a relation $\preccurlyeq$ on $\mathcal{C}$ by

$$C_1 \preccurlyeq C_2 \Leftrightarrow \text{ the center of } C_1 \text{ is inside } C_2.$$

Is $\preccurlyeq$ a partial order on $\mathcal{C}$?

Exercise 4.6. Let $\mathcal{C} \subset \mathcal{P}(\mathbb{R}^2)$ be the collection of all circles in the cartesian plane. Define a relation $\sim$ on $\mathcal{C}$ by

$$C_1 \sim C_2 \Leftrightarrow C_1 \text{ and } C_2 \text{ have the same center .}$$

Is $\sim$ an equivalence relation?

Exercise 4.7. Define a function $|\cdot| : \mathbb{R}^2 \to \mathbb{R}$ by

$$|(x, y)| = \sqrt{x^2 + y^2}.$$

Let $\mathcal{C}$ be the partition of $\mathbb{R}^2$ induced by this function.
Describe the members of $\mathcal{C}$.

Exercise 4.8. Let $X = \{1, 2, 3\}$. Define a function $f : \mathcal{P}(X) \setminus \{\varnothing\} \to X$ by

$$f(A) = \text{ the smallest member of A.}$$

Compute the partition of $\mathcal{P}(X)$ induced by the function f.

Exercise 4.9. Let $X = \mathbb{N} \times \mathbb{N}$. Define a relation on X by

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.$$

(a) Show that this is an equivalence relation.
(b) Describe the equivalence classes.
(c) Let $\mathcal{C}$ be the set of equivalence classes. Denote the equivalence class of (a, b) by $[a, b]$. Determine which of the following functions $f : \mathcal{C} \to \mathbb{R}$ are well-defined:

- $f([a, b]) = a^2 + b^2$;
- $f([a, b]) = a^2 - 2ab + b^2$;
- $f([a, b]) = \frac{a}{b}$;
- $f([a, b]) = \sin(a - b)$.

Exercise 4.10. Define a relation $\sim$ on $\mathbb{Z}$ by

$$a \sim b \Leftrightarrow (a-b) = 6k \text{ for some } k \in \mathbb{Z}.$$

(a) Show that $\sim$ is an equivalence relation.
(b) Describe the equivalence classes.
(c) Count the equivalence classes.
(d) Let $\mathcal{C}$ be the set of equivalence classes. Denote the equivalence class of a by $[a]$. Determine which of the following functions $f : \mathcal{C} \to \mathbb{Z}$ are well-defined:

- $f([a]) = 3a$;
- $f([a]) = 3r$, where r is the remainder when a is divided by 6;
- $f([a]) = x$, where x is the remainder when $3a$ is divided by 6;
- $f([a]) = x$, where x is the remainder when a is divided by 3;
- $f([a]) = x$, where x is the remainder when a is divided by 5.

Exercise 4.11. Let X be a set and let $\mathcal{C} = \{C_1, \ldots, C_m\}$ and $\mathcal{D} = \{D_1, \ldots, D_n\}$ be partitions of X. Define

$$\mathcal{E} = \{C_i \cap D_j \mid C_i \in \mathcal{C}, D_j \in \mathcal{D}\}.$$

(a) Show that $\mathcal{E}$ is a partition of X.
(b) Describe the equivalence relation induced by $\mathcal{E}$ in terms of the equivalence relations induced by $\mathcal{C}$ and $\mathcal{D}$.

Exercise 4.12. Let X and Y be sets. Let $\sim$ be an equivalence relation on X and let $\approx$ be an equivalence relation on Y. Let $[X]$ and $[Y]$ denote the respective sets of equivalence classes. Show that there is an induced equivalence relation $\sim$ on $X \times Y$. Denote the set of equivalence classes by $[X \times Y]$, and for $(x, y) \in X \times Y$, denote its equivalence class by $[x, y]$. Define a function

$$\phi : [X \times Y] \to [X] \times [Y]$$

by $[x, y] \mapsto ([x], [y])$. Show that ϕ is well-defined and bijective.

CHAPTER 5

Binary Operators

1. Binary Operators

Definition 5.1. Let A be a set. A *binary operator* on A is a function

$$\circledast : A \times A \to A.$$

We often write $a \circledast b$ to mean $\circledast(a, b)$.

A binary operator is simply something that takes two elements of a set and gives back a third element of the same set. Even though it is customary to write $a \circledast b$ instead of $\circledast(a, b)$, where $a, b \in A$, we keep in mind that $\circledast$ is a function and that $a \circledast b \in A$.

Example 5.1. Let $\mathbb{R}$ be the set of real numbers. Then $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, given by $+(x, y) = x + y$, is a binary operator. Also $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, given by $\cdot(x, y) = xy$, is a binary operator.

More generally, in the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, addition and multiplication are binary operators.

Example 5.2. Let X be a set and let $\mathcal{P}(X)$ be the power set of X. Then union and intersection are binary operators on $\mathcal{P}(X)$; for example

$$\cap : \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$$

is defined by $\cap(A, B) = A \cap B$, where $A, B \subset X$.

Example 5.3. Let X be a set and let $\mathcal{F}(X, X)$ be the set of all functions from X to X. Then function composition $\circ$ is a binary operation on $\mathcal{F}(X, X)$.

Example 5.4. Let X be a set and let $\mathrm{Sym}(X)$ be the set of all permutations of X. Then $\circ$ is a binary operator on $\mathrm{Sym}(X)$:

$$\circ : \mathrm{Sym}(X) \times \mathrm{Sym}(X) \to \mathrm{Sym}(X)$$

is defined by $\circ(\phi, \psi) = \phi \circ \psi$.

2. Closure

Definition 5.2. Let $\circledast : A \times A \to A$ be a binary operator on a set A and let $B \subset A$. We say that B is *closed* under the operation of $\circledast$ if for every $b_1, b_2 \in B$, we have $b_1 \circledast b_2 \in B$.

Example 5.5. Let E be the set of even integers. Then E is closed under the operations of addition and multiplication of integers. Indeed, the sum of even integers is even, and the product of even integers is even.

Let O be the set of odd integers. Then O is closed under multiplication. However, O is not closed under addition, because the sum of two odd integers is even.

Example 5.6. Let $B = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$. Then B is closed under addition and multiplication of real numbers. For example, if $a_1 + b_1\sqrt{2}$ and $a_2 + b_2\sqrt{2}$ are two element of B, then

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in B$$

and

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in B.$$

Note that these results are in B because $\mathbb{Q}$ itself is closed under addition and multiplication. Therefore $a_1a_2 + 2b_1b_2 \in \mathbb{Q}$, and so forth.

Example 5.7. Let X be a set and let $Y \subset X$. Then $\mathcal{P}(Y) \subset \mathcal{P}(X)$, and the subset $\mathcal{P}(Y)$ is closed under the operations of intersection and union of subset of X.

3. Properties of Binary Operations

Definition 5.3. Let $\circledast$ be a binary operation on a set A.

We say that $\circledast$ is *commutative* if for every $a, b \in A$, we have

$$a \circledast b = b \circledast a.$$

We say that $\circledast$ is *associative* if for every $a, b, c \in A$, we have

$$(a \circledast b) \circledast c = a \circledast (b \circledast c).$$

Definition 5.4. Let $\circledast$ be a binary operation on a set A.

An element $e \in A$ is called an *identity* with respect to $\circledast$ if $a \circledast e = e \circledast a = a$ for every $a \in A$.

Proposition 5.5. *Let $\circledast$ be a binary operation on a set A. If $e, f \in A$ are identities with respect to $\circledast$, then $e = f$.*

Proof. Since f is an identity, $e * f = e$, so since equality is symmetric, $e = e * f$. Since e is an identity, $e * f = f$. Since equality is transitive, $e = e * f$ and $e * f = f$ implies that $e = f$. □

Definition 5.6. Let $\circledast$ be a binary operation on a set A with an identity e.

Let $a \in A$. An element $b \in A$ is called an *inverse of a* with respect to $\circledast$ if $ab = ba = e$. If a has an inverse, we say that a is *invertible*.

If every element of A has an inverse with respect to $\circledast$, we say that $\circledast$ is *invertible*.

Proposition 5.7. *Let $\circledast$ be an associative binary operation on a set A with an identity e. Let $a \in A$. If $b, c \in A$ are inverses for a with respect to $\circledast$, then $b = c$.*

Proof. Note $e = a \circledast c$ and $e = b \circledast a$. Using symmetry and transitivity of equality as well as associativity of $\circledast$, we have

$$b = b \circledast e = b \circledast (a \circledast c) = (b \circledast a) \circledast c = e \circledast c = c.$$

□

Definition 5.8. Let $\circledast$ be a binary operation on a set A.

An element $z \in A$ is called a *pit* with respect to $\circledast$ if $z \circledast a = a \circledast z = z$ for every $a \in A$.

Proposition 5.9. *Let $\circledast$ be a binary operation on a set A. If $y, z \in A$ are pits with respect to $\circledast$, then $y = z$.*

Proof. We have $z = y \circledast z = y$. □

Definition 5.10. Let $\circledast$ be a binary operation on a set A with a pit z.

An element $a \in A$ is *irregular* if there exists $b, c \in A \setminus \{z\}$ such that $a \circledast b = c \circledast a = z$. Otherwise we say that a is *regular*.

Definition 5.11. Let $\circledast$ be a binary operation on a set A.

An element $a \in A$ is *cancellable* if $ac = bc \Rightarrow a = b$ and $ca = cb \Rightarrow a = b$. Let $\circledast$ be a commutative, associative binary operation on a set A with a pit z.

Problem 5.1. Let $\circledast$ be a binary operation on a set A, and let $a \in A$. Show that if a is cancellable, then a is regular.

Example 5.8. The real numbers have two binary operations, addition and multiplication. Each is commutative and associative. The additive identity is 0, and the multiplicative identity is 1. Every element a has an additive inverse $-a$, and if $a \neq 0$, it has a multiplicative inverse $a^{-1} = \frac{1}{a}$.

The subset $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{N}$ of $\mathbb{R}$ each contain 0 and 1, and these act as additive and multiplicative identities in these sets. Every nonzero rational number has an additive and multiplicative inverse. The integers have additive inverses but not multiplicative inverses. The natural numbers do not contain additive inverses.

Example 5.9. Let X be a set and consider intersection and union of subsets of X. These are operations on $\mathcal{P}(X)$ which are commutative and associative. Intersection has an identity element, which is the entire set X, since for $A \subset X$, we have $A \cap X = A$. Union also has an identity element, which is $\varnothing$. Neither of these operations supports inverses.

However, the operation of symmetric difference on $\mathcal{P}(X)$, defined by

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

is commutative, associative, and invertible. The identity element is $\varnothing$, and the inverse of $A \in \mathcal{P}(X)$ is itself.

Example 5.10. Let X be a set and consider composition of permutations of X. This operation on $\mathrm{Sym}(X)$ is associative, because composition of functions is always associative. It is also invertible. The identity element for this operation is the identity function id_X. The inverse of a permutation exists because bijective functions are always invertible.

However, composition of permutations is not commutative. For example, let $X = \{1, 2, 3\}$. Let $\phi \in \mathrm{Sym}(X)$ be given by $(1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1)$ and let $\psi \in \mathrm{Sym}(X)$ be given by $(1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3)$. Then $\phi \circ \psi = (1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1)$ but $\psi \circ \phi = (1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2)$. Thus $\phi \circ \psi \neq \psi \circ \psi$.

Example 5.11. The standard *dot product* on $\mathbb{R}^n$ is defined by

$$\vec{v} \cdot \vec{w} = v_1 w_1 + \cdots + v_n v_w,$$

where $\vec{v} = (v_1, \ldots, v_n)$ and $\vec{w} = (w_1, \ldots, w_n)$. Note that for $n > 1$, this is NOT a binary operator, since it is a function

$$\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R};$$

to be a binary operator on $\mathbb{R}^n$, the target has to be $\mathbb{R}^n$.

Example 5.12. Let X be a set and let $\mathcal{F}(X, X)$ be the set of all functions, not necessarily bijective, from X into itself. Composition is a binary operator on $\mathcal{F}(X, X)$, and $\mathrm{Sym}(X)$ is a closed under this operation. The same identity element id_X exists in this set. However, not every element is invertible; in fact, $\mathrm{Sym}(X)$ is the subset of invertible elements.

Let $h \in \mathcal{F}(X, X)$. This is the same as saying $h : X \to X$. For each $n \in \mathbb{N}$, define the function $h^n : X \to X$ in the natural way. For $n = 0$, $h^0 = \mathrm{id}_X$. For $n = 1$, $h^1 = h$. However, $h^2 = h \circ h$, $h^3 = h \circ h \circ h$, and in general,

$$h^n = h \circ \cdots \circ h \ (n \text{ times}).$$

Example 5.13. An $m \times n$ *matrix* with entries in $\mathbb{R}$ is an array of elements of $\mathbb{R}$ with m rows and n columns. The entries of a matrix are often labelled a_{ij}, where this is the entry in the i^{th} row and j^{th} column. We may write such a matrix with the notation (a_{ij}).

An $m \times n$ matrix $A = (a_{ij})$ may be added to an $m \times n$ matrix $B = (b_{ij})$ to give an $m \times n$ matrix $AB = C = (c_{ij})$ by the formula

$$c_{ij} = a_{ij} + b_{ij}.$$

An $m \times n$ matrix $A = (a_{ij})$ may be multiplied by an $n \times p$ matrix $B = (b_{jk})$ to give an $m \times p$ matrix $AB = C = (c_{ik})$ by the formula

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk};$$

thus the ik^{th} entry of C is the dot product of the i^{th} row of A with the k^{th} column of B.

Let $\mathbb{M}_n(\mathbb{R})$ be the set all $n \times n$ matrices over $\mathbb{R}$. Then addition of matrices is a binary operation on $\mathbb{M}_n(\mathbb{R})$ which is commutative, associative, and invertible. Also, multiplication of matrices is a binary operation on $\mathbb{M}_n(\mathbb{R})$ which is associative and has an identity. The identity is simply the matrix given by $a_{ij} = 1$ if $i = j$ and $a_{ij} = 0$ otherwise. However, this operation is not commutative, and there are many elements which do not have inverses.

4. Exercises

Exercise 5.1. In each case, we define a binary operation $\circledast$ on $\mathbb{R}$. Determine if $\circledast$ is commutative and/or associative, find an identity if it exists, and find any invertible elements.

(a) $x \circledast y = xy + 1$;
(b) $x \circledast y = \frac{1}{2}xy$;
(c) $x \circledast y = |x|^y$.

Exercise 5.2. Consider the plane $\mathbb{R}^2$. Define a binary operation $\circledast$ on $\mathbb{R}^2$ by

$$(x_1, y_1) \circledast (x_2, y_2) = \left(\frac{x_1 + x_2}{2}, \frac{y_1 + y_2}{2}\right).$$

Thus the "product" of two points under this operation is the point which is midway between them. Determine if $\circledast$ is commutative and/or associative, find an identity if it exists, and find any invertible elements.

Exercise 5.3. Let $\mathcal{I}$ be the collection of all open intervals of real numbers. We consider the empty set to be an open interval.
(a) Show that $\mathcal{I}$ is closed under the operation of $\cap$ on $\mathcal{P}(\mathbb{R})$.
(b) Show that $\mathcal{I}$ is not closed under the operation of $\cup$ on $\mathcal{P}(\mathbb{R})$.

Exercise 5.4. Let X and Y be sets and let $\circledast : Y \times Y \to Y$ be a binary operation on Y which is commutative, associative, and invertible. Let $f : X \to Y$ be a bijective function. Define an operation $\boxdot$ on X by

$$x_1 \boxdot x_2 = f^{-1}(f(x_1) \circledast f(x_2)).$$

Show that $\boxdot$ is commutative, associative, and invertible.

Exercise 5.5. Let X and Y be sets and let $\circledast : Y \times Y \to Y$ be a binary operation on Y. Let $\mathcal{F}(X, Y)$ be the set of all functions from X to Y. Show that $\circledast$ induces a binary operation, which may also be called $\circledast$, on $\mathcal{F}(X, Y)$.

Exercise 5.6. Let X be a set and let $\circledast : X \times X \to X$ be a binary operation on X which is associative and invertible. Show that $\circledast$ induces a binary operation, which may also be called $\circledast$, on $\mathcal{P}(X)$. Is it associative? Does it have an identity? Is it invertible?

CHAPTER 6

The Natural Numbers

1. Peano/von Neumann Construction

Definition 6.1. Let n be a set. The *successor* of n is

$$n^+ = n \cup \{n\}.$$

Proposition 6.2. *Let n be a set. Then n^+ is a set.*

Proof. We are given that n is a set. By Proposition 1.3, $\{n\}$ is a set. Thus by Proposition 1.13, $n \cup \{n\}$ is a set. Thus $n^+ = n \cup \{n\}$ is a set. □

Definition 6.3. Let N be a set. We say that N is *supernatural* if

(N1) $\varnothing \in N$;
(N2) if $n \in N$, then $n^+ \in N$.

Proposition 6.4. *Let $\mathcal{N}$ be a nonempty collection of supernatural sets. Then $\cap\mathcal{N}$ is supernatural.*

Proof. Since $\mathcal{N}$ is nonempty, there is at least one set in $\mathcal{N}$, and since every set in $\mathcal{N}$ is supernatural, $\varnothing \in N$ for every $N \in \mathcal{N}$. Thus $\varnothing \in \cap\mathcal{N}$, and $\cap\mathcal{N}$ satisfies **(N1)**.

Let $n \in \cap\mathcal{N}$. Then $n \in N$ for every $N \in \mathcal{N}$. By **(N2)**, $n^+ \in N$ for every $N \in \mathcal{N}$. Thus $n^+ \in \cap\mathcal{N}$, and $\cap\mathcal{N}$ satisfies **(N2)**. □

Definition 6.5. Let N be a supernatural set. We say that N is *natural* if

(N3) if $S \subset N$ is supernatural, then $S = N$.

Theorem 6.6. (Peano/von Neumann Theorem)
There exists a unique natural set.

Proof. By Axiom 5, there exists a supernatural set X. Let

$$\mathcal{N} = \{N \in \mathcal{P}(X) \mid N \text{ is supernatural}\}.$$

Now $\mathcal{N}$ is a set by Axiom 8, and $\mathcal{N}$ is nonempty, because $X \in \mathcal{N}$.

Set $M = \cap\mathcal{N}$. By Proposition 6.4, M is supernatural. Let $S \subset M$ be supernatural. Then $S \subset X$, so $S \in \mathcal{N}$. Thus $M = \cap\mathcal{N} \subset S$, whence $S = M$. Thus M is natural, so a natural set exists; it remains to show that it is unique.

Let M and N be natural sets. We wish to show that $M = N$.

Let $S = M \cap N$. Since S is the intersection of supernatural sets, S is also supernatural. Now $S \subset M$ and $S \subset N$, so by **(N3)**, which is satisfied by both M and N, we have $S = M$ and $S = N$. Therefore $M = N$. □

2. Natural Numbers

Definition 6.7. The *natural numbers* are the elements of the unique natural set. Let $\mathbb{N}$ denote the set of natural numbers.

To see how this definition produces with our conventional counting scheme,

$$\mathbb{N} = \{0, 1, 2, 3, \dots\},$$

we must first realize that n^+ will become $n + 1$ (once we have defined addition). It is "natural" to let $\varnothing$ be zero, and proceed from there:

- $0 = \varnothing$;
- $1 = 0^+ = \{\varnothing\}$;
- $2 = 1^+ = \{\varnothing, \{\varnothing\}\}$;
- $3 = 2^+ = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$;

as so forth. We could have written this as

- $0 = \varnothing$;
- $1 = \{0\}$;
- $2 = \{0, 1\}$;
- $3 = \{0, 1, 2\}$;

and in general, $n^+ = \{m \in \mathbb{N} \mid m \leq n\}$. Conveniently, the number n is a set containing n elements.

Peano's postulates contain the core idea of Property **(N3)**, and von Neumann applied Definition 6.1 to obtain the construction presented here. Hence the name of the theorem, which is nonstandard but appropriate.

Proposition 6.8. *Let $n \in \mathbb{N}$. Then $n \subset \mathbb{N}$.*

Proof. Let

$$S = \{n \in \mathbb{N} \mid n \subset \mathbb{N}\};$$

it suffices to show that $S = \mathbb{N}$.

Let $n = \varnothing$. Then $n \subset \mathbb{N}$, so $\varnothing \in S$.

Let $n \in S$ and let $x \in n^+$. Since $n^+ = n \cup \{n\}$, either $x \in n$ or $x = n$.

Case 1: If $x \in n$, then $x \in \mathbb{N}$ because $n \subset \mathbb{N}$.

Case 2: If $x = n$, then $x \in \mathbb{N}$ because $n \in \mathbb{N}$.

In either case, $x \in \mathbb{N}$, so $n^+ \subset \mathbb{N}$, and $n^+ \in S$. By Property **(N3)**, $S = \mathbb{N}$. □

3. Ordering of Natural Numbers

Definition 6.9. Define a relation $\leq$ on $\mathbb{N}$ by

$$m \leq n \;\Leftrightarrow\; m \subset n,$$

where $m, n \in \mathbb{N}$.

Lemma 6.10. *If $n \in \mathbb{N}$ and $x \in n$, then $x \subset n$.*

Proof. Let

$$S = \{n \in \mathbb{N} \mid x \in n \text{ implies } x \subset n\}.$$

Let $n = \varnothing$. Then the condition $x \in n \Rightarrow x \subset n$ is vacuously true, so $\varnothing \in S$.

Let $n \in S$ and let $x \in n^+$. By definition of successor, either $x \in n$ or $x = n$.

Case 1: If $x \in n$, then $x \subset n$ because $n \in S$, so $x \subset n^+$ because $n \subset n^+$.

Case 2: If $x = n$, then $x \subset n^+$ by definition of successor.

Thus $n^+ \in S$, so $S = \mathbb{N}$ by Property **(N3)**. □

Lemma 6.11. *If $n \in \mathbb{N}$ and $x \in n$, then $x^+ \subset n$.*

Proof. By hypothesis, $x \in n$, so by Lemma 6.10, $x \subset n$. Let $a \in x^+ = x \cup \{x\}$. Then $a \in x$ or $a = x$. If $a \in x$, then $a \in n$ because $x \subset n$. If $a = x$, then $a \in n$ because $x \in n$. In either case, $a \in n$, so $x^+ \subset n$. □

Lemma 6.12. *If $n, x \in \mathbb{N}$ and $x \subset n$, then $x \in n$ or $x = n$.*

Proof. Let

$$S = \{n \in \mathbb{N} \mid x \in \mathbb{N} \text{ and } x \subset n \text{ implies } x \in n \text{ or } x = n\}.$$

Let $n = \varnothing$. If $x \subset n$, then x must be empty, so $x = n$. Thus $\varnothing \in S$.

Let $n \in S$ and $x \in \mathbb{N}$ with $x \subset n^+$. Then $x \subset n \cup \{n\}$, so either $x \subset n$ or $n \in x$.
Case 1: If $x \subset n$, then $x \in n$ or $x = n$, because $n \in S$; either way, $x \in n^+$.
Case 2: Suppose $n \in x$. Apply Lemma 6.11 (with the roles of n and x reversed) to obtain $n^+ \subset x$. We also have $x \subset n^+$, so $x = n^+$

Thus $n^+ \in S$, so $S = \mathbb{N}$ by Property **(N3)**. □

Theorem 6.13. (Natural Ordering Principle)
The relation $\leq$ on $\mathbb{N}$ is a total order relation.

Proof. Since $m \subset m$ for any set m, the relation is reflexive.

If $m \subset n$ and $n \subset m$, then $m = n$, so the relation is antisymmetric.

If $m \subset n$ and $n \subset p$, then $m \subset p$, so the relation is transitive.

It remains to show that the relation is a total order; this requires that we show that for $m, n \in \mathbb{N}$, either $m \leq n$ or $n \leq m$, that is, either $m \subset n$ or $n \subset m$. Let

$$S = \{x \in \mathbb{N} \mid x \subset n \text{ or } n \subset x\};$$

we wish to show that $m \in S$, and it suffices to show that $S = \mathbb{N}$.

Clearly $\varnothing \subset n$, so $\varnothing \in S$. Now assume that $x \in S$; we wish to show that $x^+ \in S$. Since $x \in S$, either $n \subset x$ or $x \subset n$.

Case 1: Suppose that $n \subset x$. Then $n \subset x^+ = x \cup \{x\}$, so $x^+ \in S$.

Case 2: Suppose that $x \subset n$. By Lemma 6.12, $x \in n$ or $x = n$.
Case 2a: Suppose $x \in n$. Then $x \subset n$ and $x \in n$. Since $x^+ = x \cup \{x\}$, $x^+ \in n$.
Case 2b: Suppose $x = n$. Then $x^+ = x \cup \{n\}$, so $n \subset x^+$.
So if $x \subset n$, either $x^+ \subset n$ or $n \subset x^+$. In either case, $x^+ \in S$.

Therefore $S = \mathbb{N}$ by Property **(N3)**. □

4. Well Ordering Principle

Lemma 6.14. *Let $n, x \in \mathbb{N}$. If $n < x$, then $n^+ \leq x$.*

Proof. Suppose $n < x$, which means $n \leq x$ and $n \neq x$. Now $n \leq x$ means that $n \subset x$, and Lemma 6.12 states that this implies $n \in x$ or $n = x$. Thus $n \in x$, and Lemma 6.10 concludes from this that $n^+ \subset x$. It follows from the definition that $n^+ \leq x$. □

Theorem 6.15. (Well Ordering Principle)
Let $A \subset \mathbb{N}$ be nonempty. Then A has a minimum element.

Proof. Let $A \subset \mathbb{N}$ and suppose that A has no minimum element. Let

$$S = \{n \in \mathbb{N} \mid n < a \text{ for every } a \in A\}.$$

It is clear that $S \cap A = \varnothing$.

Let $a \in A$. Now a is a natural number, and a cannot be zero, because A has no minimum element. Thus $0 < a$, so $0 \in S$.

Now suppose that $n \in S$; then $n < a$ for every $a \in A$. By Lemma 6.14, $n^+ \leq a$ for every $a \in A$. But since A has no minimum element, $n^+ \notin A$, so $n^+ < a$ for every $a \in A$, so $n^+ \in S$. This shows that $S = \mathbb{N}$. Therefore A is empty. □

Problem 6.1. Let $A \subset \mathbb{N}$ be nonempty. Show that $\cap A \in A$, and that $\cap A$ is the minimum element of A.

5. Induction Principle

Theorem 6.16. (Induction Principle)
Let $p(n)$ be a proposition for each $n \in \mathbb{N}$. If

(a) *$p(0)$ is true;*
(b) *$p(n) \Rightarrow p(n^+)$;*

then $p(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let

$$S = \{n \in \mathbb{N} \mid p(n) \text{ is true}\}.$$

By **(a)**, $0 \in S$. If $n \in S$, then **(b)** implies that $n^+ \in S$. Therefore, $S = \mathbb{N}$, and the principle follows. □

We don't have to start the induction at zero; we may start at any natural number.

Theorem 6.17. (Induction Principle Initial Form)
Let $p(n)$ be a proposition for each $n \in \mathbb{N}$, and let $k \in \mathbb{N}$. If

(a) *$p(k)$ is true;*
(b) *if $n \geq k$, then $p(n) \Rightarrow p(n^+)$;*

then $p(n)$ is true for all $n \in \mathbb{N}$ with $n \geq k$.

Proof. Let

$$S = \{n \in \mathbb{N} \mid n < k \text{ or } p(n) \text{ is true}\}.$$

If $k = 0$, we are done; otherwise, $0 \in S$ since $0 < k$.

Let $n \in S$; either $n^+ < k$, $n^+ = k$, or $n^+ > k$. If $n^+ < k$, then $n^+ \in S$ by the specification of S. If $n^+ = k$, then $n^+ \in S$ by **(a)**. If $n > k$, then $n^+ \in S$ by **(b)**. Therefore, $S = \mathbb{N}$, and the principle follows. □

The induction theorem can be made stronger by weakening the hypothesis. The resulting theorem gives a proof technique which is known as strong induction.

Theorem 6.18. (Strong Induction Principle)
Let $p(n)$ be a proposition for each $n \in \mathbb{N}$. If

(1) *$p(0)$ is true;*
(2) *If $p(m)$ is true for all $m \leq n$, then $p(n^+)$ is true;*

then $p(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let $t(n)$ be the statement that "p(m) is true for all $m \leq n$".

Our first assumption is that $p(0)$ is true, and since the only natural number less than or equal to 0 is zero (because the only subset of the empty set is itself), this means that $t(0)$ is true.

Our second assumption is that if $t(n)$ is true, then $p(n+1)$ is true. Thus assume that $t(n)$ is true so that $p(n+1)$ is also true. Then $p(i)$ is true for all $i \leq n+1$. Thus $t(n+1)$ is true.

By our original Induction Theorem, we conclude that $t(n)$ is true for all $n \in \mathbb{N}$. This implies that $p(n)$ is true for all $n \in \mathbb{N}$. □

6. Successor Map

Definition 6.19. Let $\mathbb{N}^+ = \{n \in \mathbb{N} \mid n \geq 1\}$ denote the positive natural numbers.

The *successor map* is the function

$$\sigma : \mathbb{N} \to \mathbb{N} \quad \text{given by} \quad \sigma(n) = n^+.$$

Proposition 6.20. *Let $\sigma : \mathbb{N} \to \mathbb{N}$ be the successor map. The constriction of σ to $\mathbb{N}^+$ is bijective.*

Proof. Note that for every $n \in \mathbb{N}$, $n \in \sigma(n) = n^+$; thus $\sigma(n)$ is nonempty. This shows that 0 is not the successor of any natural number, so the range of σ is a subset of $\mathbb{N}^+$.

Let $S = \sigma(\mathbb{N}) \cup \{0\}$. Then S satisfies **(N1)** and **(N2)**; by **(N3)**, $S = \mathbb{N}$; that is, $\mathbb{N} = \sigma(\mathbb{N}) \cup \{0\}$, so

$$\mathbb{N}^+ = \mathbb{N} \setminus \{0\} = (\sigma(\mathbb{N}) \cup \{0\}) \setminus \{0\} = \sigma(\mathbb{N}).$$

Thus σ is surjective onto $\mathbb{N}^+$.

Suppose $\sigma(m) = \sigma(n)$. We have $m^+ = n^+$, so $m \cup \{m\} = n \cup \{n\}$. From this, $m \in n \cup \{n\}$ and $n \in m \cup \{m\}$. Thus $m \in n$ or $m = n$, and $n \in m$ or $m = n$. If $m = n$ we are done, so assume $m \in n$ and $n \in m$. From Lemma 6.10, $m \subset n$ and $m \subset n$. This implies $m = n$, and show that σ is injective. □

Proposition 6.21. *If $n \in \mathbb{N}^+$, then there exists a unique element $n^- \in \mathbb{N}$ such that $(n^-)^+ = n$.*

Proof. Let $\sigma : \mathbb{N} \to \mathbb{N}^+$ be the constriction of the successor map, with inverse $\sigma^{-1} : \mathbb{N}^+ \to \mathbb{N}$. Set $n^- = \sigma^{-1}(n)$. Then $(n^-)^+ = s(s^{-1}(n)) = n$. □

The Induction Principle may be restated in the following form, which has the advantage that a proof using it ends when the desired statement is attained.

Theorem 6.22. (Induction Principle Predecessor Form)
Let $p(n)$ be a proposition for each $n \in \mathbb{N}$. If

- **(a)** *$p(0)$ is true;*
- **(b)** *if $n > 0$, then $p(n^-) \Rightarrow p(n)$;*

then $p(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let

$$S = \{n \in \mathbb{N} \mid p(n) \text{ is true}\}.$$

By **(a)**, $0 \in S$. Suppose $n > 0$, and let $m = n^-$. If $m \in S$, then $p(m)$ is true, so $p(n^-)$ is true, and **(b)** implies that $p(n)$ is true. Since $p(n) = p(m^+)$, $m^+ \in S$. Therefore, $S = \mathbb{N}$ by **(N3)**, and the principle follows. □

7. Recursion Theorem

The Recursion Theorem tells us that inductively defined sequences exist. That is, if we have a function $f : X \to X$ and we pick any point in X, and we follows where f sends it as f is repeatedly applied, we can capture the entire path of the point with a single function.

Theorem 6.23. (Recursion Theorem)
Let X be a set, $f : X \to X$, and $a \in X$. Then there exists a unique function $\phi : \mathbb{N} \to X$ such that $\phi(0) = a$ and $\phi(n^+) = f(\phi(n))$ for all $n \in \mathbb{N}$.

Proof. Recall that a function from $\mathbb{N}$ to X is a set of the form $((\mathbb{N}, X), F)$, where $F \subset \mathbb{N} \times X$ satisfies

$$\forall n \in \mathbb{N}\ \exists! x \in X \mid (n, x) \in F.$$

Let

$$\mathcal{G} = \{G \in \mathcal{P}(\mathbb{N} \times X) \mid (0, a) \in G \text{ and } (n, x) \in G \Rightarrow (n^+, f(x)) \in G\}.$$

Since $\mathbb{N} \times X$ itself has the specified property, $\mathcal{G}$ is nonempty. Let $F = \cap\mathcal{G}$ and consider the mapping $\phi = ((\mathbb{N}, X), F)$.

We claim that $F \in \mathcal{G}$. Indeed, $(0, a)$ is in G for every $G \in \mathcal{G}$, so $(0, a) \in \cap\mathcal{G} = F$. Now let $(n, x) \in F$. Then $(n, x) \in G$ for every $G \in \mathcal{G}$, so $(n^+, f(x)) \in G$ for every $G \in \mathcal{G}$. Then $(n^+, f(x)) \in F$. This shows that F meets the specification of $\mathcal{G}$.

We discuss why $\phi : \mathbb{N} \to X$.

Set $S = \{n \in \mathbb{N} \mid (n, x) \in F \text{ for some } x \in X\}$; that is, S is the domain of the mapping ϕ. Then $0 \in S$ because $(0, a) \in F$. Also, $n \in S$, then $(n, x) \in F$ for some $x \in X$, so $(n^+, f(x)) \in F$. Thus $n^+ \in S$, and by **(N3)**, $S = \mathbb{N}$. Thus $\mathrm{dom}(\phi) = \mathbb{N}$.

Set $T = \{n \in \mathbb{N} \mid (n, x_1), (n, x_2) \in F \Rightarrow x_1 = x_2\}$; that is, T is the set of all $n \in \mathbb{N}$ which are mapped to a unique element in X by ϕ.

If $0 \neq T$, then $(0, a)$ and $(0, x_2) \in S$ for some $x_2 \in X$. Then $F \setminus \{(0, x_2)\} \in \mathcal{G}$, and this set is smaller that $F = \mathcal{G}$, a contradiction. Thus $0 \in T$.

Suppose $n \in T$. Then $(n, x) \in F$ for some unique $x \in X$. Now if $n^+ \neq S$, there are distinct $x_1, x_2 \in X$ such that $(n^+, x_1), (n^+, x_2) \in F$. Only one of these can be $f(x)$; without loss of generality, $x_2 \neq f(x)$. Then $F \setminus \{(n^+, x_2)\} \in \mathcal{G}$, and this set is smaller than $F = \mathcal{G}$, again a contradiction. Thus $n^+ \in T$. By **(N3)**, $T = \mathbb{N}$. This shows that ϕ is a function.

Finally, ϕ is clearly unique by construction. □

The Recursion Theorem and the successor map and intimately intertwined with the theory of powers of a function and the arithmetic of the natural numbers. So for the next few sections, these theories will be developed side by side.

8. Powers

Definition 6.24. Let $\circledast$ be a binary operation on a set A with identity element $e \in A$, and let $b \in A$. Define a function $\mu_b : A \to A$ by $\mu_b(a) = b \circledast a$. By the Recursion Theorem, there exists as unique function $\phi_b : \mathbb{N} \to A$ such that $\phi_b(0) = e$ and $\phi_b(m^+) = \mu_b(\phi_b(m))$.

Define the n^{th} *power of b with respect to* $\circledast$ to be $\phi_b(n)$.

Example 6.1. Let X be a set and let $A = \mathcal{F}(X, X)$. Then composition is a binary operator on A, and if $f \in A$, the n^{th} power of f with respect to $\circ$ is the composition of f with itself n times, and is denoted f^n. In this case, $f^0 = \mathrm{id}_X$.

Example 6.2. Let $\cdot$ be a binary operator on a set A, which we call multiplication. with an identity element $1_A \in A$. In this case, if $b \in A$, the n^{th} power of b is respect to $\cdot$ is denoted b^n. Note that $b^0 = 1_A$.

Example 6.3. Let $+$ be a binary operator on a set A, which we call addition, with an identity element $0_A \in A$. In this case, if $b \in A$, the n^{th} power of b with respect to $+$ is normally called the n^{th} multiple of b, and is denoted nb. Note that $0b = 0_A$.

9. Powers of a Function

Definition 6.25. Let $f : X \to X$ be a function, and let $n \in \mathbb{N}$. Let $x \in X$. By the Recursion Theorem, there exists as unique function $\phi_x : X \to X$ such that $\phi_x(0) = x$ and $\phi_x(m^+) = f(\phi_x(m))$.

Define the n^{th} *power of* f to be the function

$$f^n : X \to X \quad \text{given by} \quad f^n(x) = \phi_x(n).$$

The next few propositions position us to show analogous properties with σ playing the role of f. This sets us up to prove properties of addition.

Proposition 6.26. *Let $f : X \to X$ be a function, and let $n \in \mathbb{N}$. Then*

(a) *$f^0(x) = x$ and $f^1(x) = f(x)$;*
(b) *$f^{n^+}(x) = f(f^n(x))$;*
(c) *$f^{n^+}(x) = f^n(f(x))$.*

Proof. We use the notation of Definition 6.25.

Now $f^0(x) = \phi_x(0) = x$, and $f^1(x) = \phi_x(1) = \phi_x(0^+) = f(\phi_x(0)) = f(x)$, proving **(a)**.

Also, $f^{n^+}(x) = \phi_x(n^+) = f(\phi_x(n)) = f(f^n(x))$, which proves **(b)**.

To prove **(c)**, proceed by induction on n. For $n = 0$, we have

$$f^{0^+}(x) = f^1(x) = f(x) = f^0(f(x))$$

by **(a)**, so **(c)** is true in this case.

Let $n > 0$ and assume that $f^n(x) = f^{n^-}(f(x))$. Applying f to both sides given $f(f^n(x)) = f(f^{n^-}(f(x)))$. Now **(b)** implies that

$$f(f^n(x)) = f^{n^+}(x) \quad \text{and} \quad f(f^{n^-}(f(x))) = f^{(n^-)^+}(f(x)) = f^n(f(x));$$

thus $f^{n^+}(x) = f^n(f(x))$, which proves **(c)**. □

Proposition 6.27. *Let $f : X \to X$ be an injective function, and let $n \in \mathbb{N}$. Then $f^n : X \to X$ is injective.*

Proof. Proceed by induction on n. For $n = 0$, $f^0(x) = x$, which is the identity function, and is clearly injective.

Let $n > 0$ and assume that f^{n^-} is injective. Let $m = n^-$, so that f^m is injective. Then

$$f^n(x) = f^{m^+}(x) = f(f^m(x)) = (f \circ f^m)(x).$$

This shows that f^n is the composition of injective functions, so f^n is injective by Proposition 2.19. □

Problem 6.2. Let $f : X \to X$ be a surjective function, and let $n \in \mathbb{N}$. Show that f^n is surjective.

10. Powers of Succession

Proposition 6.28. *Let $\sigma : \mathbb{N} \to \mathbb{N}$ be the successor map. Let $m, n \in \mathbb{N}$. Then*

(a) $\sigma^0(n) = \sigma^n(0) = n$;
(b) $(\sigma^m(n))^+ = \sigma^{m^+}(n)$;
(c) $(\sigma^m(n))^+ = \sigma^m(n^+)$.

Proof. From Definition 6.25, $\sigma^0(n) = \phi_n(0) = n$. To see that $\sigma^n(0) = n$, proceed by induction on n. For $n = 0$, we already have $\sigma^0(0) = 0$.

Assume that $n > 0$ and that $\sigma^{n^-}(0) = n^-$. Now from Proposition 6.26 and the definition of σ,

$$\sigma^n(0) = \sigma(\sigma^{n^-}(0)) = \sigma(n^-) = (n^-)^+ = n.$$

This proves **(a)**.

The definition of σ and Proposition 6.26 gives

$$(\sigma^m(n))^+ = \sigma(\sigma^m(n)) = \sigma^{m^+}(n).$$

This proves **(b)**.

Similarly, combining Proposition 6.26 parts **(b)** and **(c)**,

$$(\sigma^m(n))^+ = \sigma(\sigma^m(n)) = \sigma^m(\sigma(n)) = \sigma^m(n^+).$$

This proves **(c)**. □

The next proposition will produce the commutativity of addition as a corollary.

Proposition 6.29. *Let $\sigma : \mathbb{N} \to \mathbb{N}$ be the successor map. Let $m, n \in \mathbb{N}$. Then*

$$\sigma^m(n) = \sigma^n(m).$$

Proof. Fix n and proceed by induction on m. For $m = 0$, the statement is $\sigma^0(n) = \sigma^n(0)$, which is true by Proposition 6.28 part **(a)**.

Let $m > 0$ and assume that $\sigma^{m^-}(n) = \sigma^n(m^-)$. Apply σ to both sides to get

$$\sigma(\sigma^{m^-}(n)) = \sigma(\sigma^n(m^-)).$$

Use Proposition 6.26 part **(b)** to see that the left hand side simplifies as

$$\sigma(\sigma^{m^-}(n)) = \sigma^m(n).$$

Use Proposition 6.28 parts **(b)** and **(c)** to see that the right hand side simplifies as

$$\sigma(\sigma^n(m^-)) = \sigma(\sigma^{n^-}(m)) = \sigma^n(m).$$

Thus $\sigma^m(n) = \sigma^n(m)$. □

11. Addition of Natural Numbers

Definition 6.30. Define a binary operation called *addition* on $\mathbb{N}$ as

$$+ : \mathbb{N} \to \mathbb{N} \quad \text{given by} \quad m + n = \sigma^m(n).$$

Proposition 6.31. $1 + 1 = 2$.

Proof. Recall that $0 = \varnothing$, $1 = \{\varnothing\}$, and $2 = \{\varnothing, \{\varnothing\}\}$; thus

$$0^+ = \varnothing^+ = \varnothing \cup \{\varnothing\} = \{\varnothing\} = 1$$

and

$$1^+ = \{\varnothing\}^+ = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\} = 2.$$

Applying the notation of Definition 6.25 with $f = \sigma$, recall that ϕ_1 is the unique function such that $\phi_1(0) = 1$ and $\phi_1(m^+) = \sigma(\phi_1(m))$. We compute

$$1 + 1 = \sigma^1(1) = \phi_1(1) = \phi_1(0^+) = \sigma(\phi_1(0)) = \sigma(1) = 1^+ = 2.$$

□

Problem 6.3. Show that $2 + 3 = 5$.

The next proposition will produce associativity of addition as a corollary. We needed the definition of addition just to state this proposition.

Proposition 6.32. *Let $f : X \to X$. Then*

$$f^{m+n}(x) = f^m(f^n(x)) \text{ for every } x \in X.$$

Proof. Proceed by induction on m. For $m = 0$, the statement is $f^{0+n}(x) = f^0(f^n(x))$. Now Proposition 6.26 part **(a)** says that for any function f, $f^0(x) = x$, so $0 + n = \sigma^0(n) = n$, so both sides of the equation equal $f^n(x)$, and the statement is true in this case.

Let $m > 0$ and assume $f^{m^- + n}(x) = f^{m^-}(f^n(x))$. Applying f to both sides produces $f(f^{m^- + n}(x)) = f(f^{m^-}(f^n(x)))$. By Proposition 6.26 part **(b)**, this equations simplifies to

$$f^{(m^- + n)^+}(x) = f^{(m^-)^+}(f(x)).$$

Now apply Proposition 6.28 part **(b)** to the exponent on the left to get

$$(m^- + n)^+ = (\sigma^{m^-}(n))^+ = \sigma^{(m^-)^+}(n) = \sigma^m(n) = m + n;$$

also, we know that $(m^-)^+ = m$. Thus the equation further simplifies to

$$f^{m+n}(x) = f^m(f^n(x)).$$

□

12. Properties of Addition

Proposition 6.33. (Properties of Addition)
Let $a, b, c \in \mathbb{N}$. Then

- **(a)** *$a + b = b + a$ (commutative property of addition);*
- **(b)** *$(a + b) + c = a + (b + c)$ (associative property of addition);*
- **(c)** *$0 + a = a$ (existence of an additive identity);*
- **(d)** *$a + c = b + c$ implies $a = b$ (cancellation law of addition).*

Proof. We prove each part.

(a) *Commutativity:* by Proposition 6.29,

$$a + b = \sigma^a(b) = \sigma^b(a) = b + a.$$

(b) *Associativity:* by Proposition 6.32,

$$(a + b) + c = \sigma^{a+b}(c) = \sigma^a(\sigma^b(c)) = \sigma^a(b + c) = a + (b + c).$$

(c) *Identity:* by Proposition 6.28 part **(a)**, $0 + a = \sigma^0(a) = a$.

(d) *Cancellation:* suppose that $a+c = b+c$. Then $c+a = c+b$, so $\sigma^c(a) = \sigma^c(b)$. Since σ is injective, so is σ^c by Proposition 6.27. Thus $a = b$. □

It behooves us to point out the following.

Proposition 6.34. *Let $n \in \mathbb{N}$. Then $n + 1 = n^+$.*

Proof. We have $n + 1 = \sigma^n(1) = \sigma^1(n) = \sigma(n) = n^+$. □

Proposition 6.35. *Let $m, n \in \mathbb{N}$. $(m + n)^+ = m^+ + n = m + n^+$.*

Proof. In light of definition 6.30, this is a restatement of 6.28. □

13. Addition and Ordering

Proposition 6.36. *Let $m, n, s \in \mathbb{N}$. Then*

$$m \leq n \;\Leftrightarrow\; m + s \leq n + s.$$

Proof. Proceed by induction on s. Since 0 is an additive identity, the statement is obvious for $s = 0$.

Let $s > 0$ and assume that $m \leq n \Leftrightarrow m + s^- \leq n + s^-$. By injectivity of the successor map, $m+s^- \leq n+s^- \Leftrightarrow (m+s^-)^+ \leq (n+s^-)^+$. Now by Proposition 6.34 and associativity of addition, $(m+s^-)^+ = (m+s^-)+1 = m+(s^-+1) = m+(s^-)^+ = m + s$. Similarly, $(n_s^-)^+ = n + s$, so we have $m + s^- \leq n + s^- \Leftrightarrow m + s \leq n + s$. Combined with the induction hypothesis and transitivity of order, this implies $m \leq n \Leftrightarrow m + s \leq n + s$. □

Proposition 6.37. *Let $m, n, s, t \in \mathbb{N}$. If $m \leq n$ and $s \leq t$, then $m + s \leq n + t$.*

Proof. Since $m \leq n$, Proposition 6.36 implies $m + s \leq n + s$. Since $s \leq t$, again 6.36 implies $s + n \leq t + n$, so commutativity of addition produces $n + s \leq n + t$. By transitivity of inequality, we conclude that $m + s \leq n + t$. □

Proposition 6.38. *Let $m, n \in \mathbb{N}$. Then*

$$m \leq n \;\Leftrightarrow\; n = m + s \text{ for some } s \in \mathbb{N}.$$

Moreover, $m = n$ if and only if $s = 0$.

Proof. We prove each direction.

($\Rightarrow$) Fix m and show that for every $n \geq m$ there exists $s \in \mathbb{N}$ such that $n = m+s$; proceed by induction on n. For $n = m$, set $s = 0$ to see that $m+s = m \leq n$.

Suppose that $m \leq n$ and $n = m + t$ for some $t \in \mathbb{N}$. Then $n^+ = (m + t)^+ = m + t^+$. So with $s = t^+$, then result follows, by Theorem 6.17.

($\Leftarrow$) Proceed by induction on s. Let $s = 0$ and suppose $n = m + s$. Then $m = m + 0 = n$, so $m \leq n$.

Assume that $p = q + s \Rightarrow q \leq p$ for all $p, q \in \mathbb{N}$. Suppose $n = m + s^+$. Then $n = m^+ + s$, so with $p = n$ and $q = m^+$, we have $m^+ \leq n$. Since $m \leq m^+$, transitivity of inequality gives $m \leq n$.

As for that last statement, suppose $n = m$ and $n = m + s$. Then $n = n + s$, so $0 + n = s + n$, so $s = 0$ by the cancellation law of addition. □

14. Powers of Powers of a Function

Proposition 6.39. *Let $f : X \to X$. Then $f^0 = \mathrm{id}_X$.*

Proof. This is just a restatement of the fact that $f^0(x) = x$ from Proposition 6.26 part **(a)**. □

Proposition 6.40. *Let $\mathrm{id}_X : X \to X$ be the identity function, and let $n \in \mathbb{N}$. Then $\mathrm{id}_X^n = \mathrm{id}_X$.*

Proof. For $n = 0$, this is Proposition 6.39.

Let $n > 0$ and assume that $\mathrm{id}_X^{n^-} = \mathrm{id}_X$ So $\mathrm{id}_X^{n^-}(x) = x$. Applying id_X to both sides, $\mathrm{id}_X^n(x) = \mathrm{id}_X(x) = x$. So, id_X^n is the identity function. □

The next two propositions will allow us to prove that multiplication is commutative.

Proposition 6.41. *Let $f, g : X \to X$ such that $f \circ g = g \circ f$. Let $n \in \mathbb{N}$. Then*

(a) $f^n \circ g = g \circ f^n$;
(b) $f^n \circ g^n = (f \circ g)^n$.

Proof. Proceed by induction on n.

Let $n = 0$.

We have $f^0 \circ g = \mathrm{id}_X \circ g = g$, and $g \circ f^0 = g \circ \mathrm{id}_X = g$, so **(a)** is true in this case.

We also have $f^0 \circ g^0 = \mathrm{id}_X \circ \mathrm{id}_x = \mathrm{id}_x$, and $(f \circ g)^0 = \mathrm{id}_X$. So **(b)** is true in this case.

Let $n > 0$. Assume that $f^{n^-} \circ g = g \circ f^{n^-}$, and that $f^{n^-} \circ g^{n^-} = (f \circ g)^{n^-}$.

Apply f to both sides of the first equation to get $f^n \circ g = f \circ g \circ f^{n^-} = g \circ f^n$, so **(a)** is true.

Apply $(f \circ g)$ to both sides of the second equation to get $f \circ g \circ f^{n^-} \circ g^{n^-} = (f \circ g)^n$. By **(a)**, g and f^{n^-} commute, so the left hand sides simplifies as

$$f \circ g \circ f^{n^-} \circ g^{n^-} = f \circ f^{n^-} \circ g \circ g^{n^-} = f^n \circ g^n.$$

This proves **(b)**. □

Proposition 6.42. *Let $f : X \to X$ and let $m, n \in \mathbb{N}$. Then*

$$(f^m)^n(x) = (f^n)^m(x).$$

Proof. Proceed by induction on m. For $m = 0$, we have $(f^0)^n = \mathrm{id}_X^n = \mathrm{id}_X$, and $(f^n)^0 = \mathrm{id}_X$. So the proposition is true in this case.

Let $m > 0$ and assume that $(f^{m^-})^n = (f^n)^{m^-}$. Apply f^n to both sides to obtain $f^n \circ (f^{m^-})^n = (f^n)^m$. Certainly f commutes with itself under composition, so f commutes with $g = f^{m^-}$ by Proposition 6.41 part **(a)**, allowing us to apply part Proposition 6.41 part **(b)** to simplify the left hand side as

$$f^n \circ (f^{m^-})^n = (f \circ f^{m^-})^n = (f^m)^n.$$

Thus $(f^m)^n = (f^n)^m$. □

15. Multiplication of Natural Numbers

Definition 6.43. Define a binary operation called *multiplication* on $\mathbb{N}$ as

$$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad \text{given by } mn = (\sigma^m)^n(0).$$

As in Definition 6.52, we drop the dot and denote multiplication by juxtaposition.

The next propositions will produce associativity of multiplication and the distributive property as corollaries. Note that we need the definition of multiplication just to state this proposition, so we will need the definition to prove it.

Proposition 6.44. *Let $m, n \in \mathbb{N}$. Then $m + mn^- = mn$.*

Proof. By the definitions of addition and multiplication and Proposition 6.26 part **(b)** applied to the function $f = \sigma^m$, we have

$$m + mn^- = \sigma^m(mn^-) = \sigma^m((\sigma^m)^{n^-}(0)) = (\sigma^m)^{(n^-)^+}(0) = (\sigma^m)^n(0) = mn.$$

□

Proposition 6.45. *Let $f : X \to X$ be a function, and let $m, n \in \mathbb{N}$. Then*

$$f^{mn}(x) = (f^m)^n(x).$$

Proof. Proceed by induction on n. First note that $m \cdot 0 = (\sigma^m)^0(0) = \mathrm{id}_X(0) = 0$. Now for $n = 0$, we have $f^{m\cdot 0}(x) = f^0(x) = x$, and $(f^m)^0(x) = x$, so the proposition is true in this case.

Let $n > 0$ and assume that $f^{mn^-} = (f^m)^{n^-}$. Applying f^m to both sides gives $f^m \circ f^{mn^-} = f^m \circ (f^m)^{n^-}$. The right hand side simplifies as

$$f^m \circ f^{mn^-} = f^{m+mn^-} = f^{mn}.$$

The left hand side simplifies as

$$f^m \circ (f^m)^{n^-} = (f^m)^{(n^-)^+} = (f^m)^n.$$

Thus $f^m n = (f^m)^n$. □

16. Properties of Multiplication

Proposition 6.46. (Properties of Multiplication)
Let $a, b, c \in \mathbb{N}$. Then

- **(a)** *$ab = ba$ (commutative property of multiplication);*
- **(b)** *$(ab)c = a(bc)$ (associative property of multiplication);*
- **(c)** *$1 \cdot a = a$ (existence of a multiplicative identity);*
- **(d)** *$0 \cdot a = 0$ (existence of a multiplicative pit);*
- **(e)** *$(a + b)c = ac + bc$ (distributivity of multiplication over addition);*
- **(f)** *$ab = 0$ implies $a = 0$ or $b = 0$ (regularity);*
- **(g)** *$ac = bc$ and $c \neq 0$ implies $a = b$ (cancellation law of multiplication).*

Proof. We prove each part.

(a) *Commutativity:* from Proposition 6.42,

$$ab = (\sigma^a)^b(0) = (\sigma^b)^a(0) = ba.$$

(b) *Associativity:* using Proposition 6.45, we have

$$(ab)c = (\sigma^{ab})^c(0) = ((\sigma^a)^b)^c(0) = (\sigma^a)^{bc}(0) = a(bc).$$

(c) *Identity:* since $\sigma^1 = \sigma$, we have

$$1 \cdot a = (\sigma^1)^a(0) = \sigma^a(0) = a.$$

(d) *Pit:*

$$0 \cdot a = (\sigma^0)^a(0) = \mathrm{id}_X^a(0) = \mathrm{id}_X(0) = 0.$$

(e) *Distributivity:* proceed by induction on c.

For $c = 0$, $(a+b)\cdot 0 = 0$ and $a \cdot 0 + b \cdot 0 = 0 + 0 = 0$. So the proposition is true in this case.

Let $c > 0$ and assume that $(a+b)c^- = ac^- + bc^-$. Adding $(a+b)$ to both side gives

$$(a+b) + (a+b)c^- = (a+b) + ac^- + bc^-.$$

Applying Proposition 6.44 to the left hand side, we see that

$$(a+b) + (a+b)c^- = (a+b)c.$$

Using commutativity and associativity of addition and Proposition 6.44 on the right hand side, we see that

$$a + b + ac^- + bc^- = (a + ac^-) + (b + bc^-) = ac + bc.$$

Thus $(a+b)c = ac + bc$.

(f) *Regularity:* suppose $ab = 0$ and $b > 0$; we show that $a = 0$. Since $b > 0$, b^- exists, so $ab^- \in \mathbb{N}$, and $0 \leq ab^-$. Adding a to both sides gives $a \leq ab^- + a = ab$. Clearly $0 \leq a$, so $ab \leq a$ and $a \leq ab$; thus $a = ab = 0$.

(g) *Cancellation:* suppose $ac = bc$. Either $a \leq b$ or $b \leq a$. Without loss of generality, assume $a \leq b$. Then $b = a + s$ for some $s \in \mathbb{N}$. Thus $ac = bc = (a+s)c = ac + sc$. By the cancellation law of addition, $sc = 0$. Since $c \neq 0$, we have $s = 0$, by regularity. Thus $b = a + 0 = a$. □

17. Multiplication and Ordering

Proposition 6.47. *Let $m, n, k \in \mathbb{N}$ with $k > 0$.*

$$m \leq n \;\Leftrightarrow\; mk \leq nk.$$

Proof. We apply the characterization of Proposition 6.38

If $m \leq n$, then $n = m + s$ for some $s \in \mathbb{N}$. Thus $(m+s)k = nk$, so $mk + sk = nk$, so $mk \leq nk$.

On the other hand, suppose that $n < m$ and $mk \leq nk$; we show that $k = 0$. Since $n < m$, then $m = n + s$ for some $s \in \mathbb{N}$ with $s > 0$. Thus $(n+s)k \leq nk$, so $nk + sk \leq nk$, whence $sk \leq 0$, so $sk = 0$. Since $s \neq 0$, we must have $k = 0$. □

Proposition 6.48. *Let $m, n \in \mathbb{N}$. If $mn = 1$, then $m = 1$ and $n = 1$. [RETURN - want PropNaturalUnits as a separate Prop? it seems silly. It is also in next chapter in PropEucI]*

Proof. Suppose that $mn = 1$. By Proposition 6.46 part **(d)**, $m \neq 0$ and $n \neq 0$; thus $1 \leq m$ and $1 \leq n$. By Proposition 6.47, $m \leq mn$ and $n \leq mn$, that is, $m \leq 1$ and $n \leq 1$ By antisymmetry of inequality, $m = 1$ and $n = 1$. □

18. Additive and Multiplicative Notation

Sets containing the first few natural numbers, or the first few nonzero natural numbers, are ubiquitous in mathematics, so we allocate permanent notation for them.

Definition 6.49. Let $n \in \mathbb{N}$. Define

$$\mathbb{N}_n = \{m \in \mathbb{N} \mid m < n\} \quad \text{and} \quad \mathbb{N}_n^+ = \{m \in \mathbb{N} \mid 1 \leq m \leq n\}.$$

According to this notation,

$$\mathbb{N}_5 = \{0, 1, 2, 3, 4\} \quad \text{and} \quad \mathbb{N}_7^+ = \{1, 2, 3, 4, 5, 6, 7\}.$$

If the n is large or arbitrary, it may be impractical or impossible to list all of the elements. In this case, we may see something like

$$\mathbb{N}_{29} = \{0, 1, \ldots, 28\} \quad \text{or} \quad \mathbb{N}_n^+ = \{1, 2, \ldots, n\}.$$

The ellipsis notation $(\ldots)$ is usually read "dot dot dot"; it means "continue in this way", where the "way" is left to the reader to infer. We cannot get around this requirement that the reader make an inference in the case of the ellipsis notation.

However, we have justified, from the axioms of set theory, that if we are given a clearly defined way to move one step at a time, then the entire journey is determined; the basis for this is the Recursion Theorem (Theorem 6.23).

Definition 6.50. Let A and I be a sets. A *family of elements in A indexed by I* is a a function $a : I \to A$.

We often use $\mathbb{N}_n^+$ as an indexing set. If we say that $a_1, \ldots, a_n \in A$, we mean that there exists a family $a : \mathbb{N}_n^+ \to A$ such that $a(i) = a_i$.

Definition 6.51. Let A be set with a binary operation $+ : A \times A \to A$. Since the operation is denoted with $+$, conventions regarding *additive notation* are in effect:

- $+$ has an identity and inverses, and is associative and commutative;
- 0 denotes the identity element;
- the inverse of a is denoted by $-a$;
- na means $a + \cdots + a$ (n times), where $n \in \mathbb{N}$, and $na = 0$ if $n = 0$;
- $\sum_{i=1}^n a_i$ means $a_1 + a_2 + \cdots + a_n$, where $n \in \mathbb{N}$ and $a_i \in A$.

Definition 6.52. Let A be a set with a binary operation $\cdot : A \times A \to A$. Since the operation is denoted with a dot, conventions regarding *multiplicative notation* are in effect:

- the dot may be suppressed, and the operation denoted by juxtaposition;
- $\cdot$ has an identity, and is associative (but not necessarily commutative);
- 1 denotes the identity element;
- the inverse of a is denoted by a^{-1}, if it exists;
- a^n means $a \cdots a$ (n times), where $n \in \mathbb{N}$, and $a^n = 1$ if $n = 0$.
- $\prod_{i=1}^n a_i$ means $a_1 a_2 \ldots a_n$, where $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in \mathbb{N}$.

CHAPTER 7

The Integers

1. Integral Equivalence

The goal is to create the integers from the natural numbers. This will give us a formal number system in which subtraction is possible. We know where we want to go with this; we just wish to formalize it in a manner that makes proving things about the integers possible. Thus it is allowable and desirable to use our intuitive understanding of the number system we wish to devise as a beacon.

The plan is two take ordered pairs of natural numbers, and think of them as integers. The pair (m, n) is to be thought of as the integer $m - n$. Thus $(5, 0)$ should represent 5, and $(0, 5)$ should represent -5. Unfortunately, $(3, 8)$ should also represent -5. Thus there are too many pairs.

This situation is alleviated via the use of equivalence relations. We take the set of ordered pairs of natural numbers and partition it into blocks of pairs which represent the same integer. Here, two integers represent the same integer if they differ by the same amount. Since we do not yet have the operation of subtraction, instead of defining "differing by the same amount" as $a - b = c - d$, instead we say that (a, b) and (c, d) differ by the same amount if $a + d = b + c$.

Then we define an integer to be a block in the partition of $\mathbb{N} \times \mathbb{N}$ induced by this equivalence relation.

Proposition 7.1. *Define a relation on* $\mathbb{N} \times \mathbb{N}$ *by*

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.$$

Then $\sim$ *is an equivalence relation, called* integral equivalence.

Proof. We wish to show that $\sim$ is reflexive, symmetric, and transitive.

(Reflexivity) Let $(a, b) \in \mathbb{N} \times \mathbb{N}$. Then $a + b = b + a$ because addition of natural numbers is commutative. Thus $(a, b) \sim (a, b)$, and $\sim$ is reflexive.

(Symmetry) Let $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. Then by symmetry of equality and commutativity of addition of natural numbers,

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c \Leftrightarrow c + b = d + a \Leftrightarrow (c, d) \sim (a, b).$$

Thus $\sim$ is symmetric.

(Transitivity) Let $(a, b), (c, d), (e, f) \in \mathbb{N} \times \mathbb{N}$. Suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $a + d = b + c$ and $c + f = d + e$. Add f to both sides of the first equation and add b to both sides of the second to obtain $a + d + f = b + c + f$ and $b + c + f = b + d + e$. Thus $a + d + f = b + d + e$. By the commutativity of addition and cancellation, we obtain $a + f = b + e$. Thus $(a, b) \sim (e, f)$, and $\sim$ is transitive. $\square$

2. Integers

Definition 7.2. The *integers* are equivalence classes induced by the integral equivalence relation. Let $\mathbb{Z}$ denote the set of integers:

$$\mathbb{Z} = \{[a, b] \mid a \in \mathbb{N}, b \in \mathbb{N}\},$$

where $[a, b]$ denotes the equivalence class of (a, b).

3. Addition of Integers

Definition 7.3. Define a binary operation called *addition* on $\mathbb{Z}$ as

$$+ : \mathbb{Z} \to \mathbb{Z} \quad \text{given by} \quad [a, b] + [c, d] = [a + c, b + d].$$

To define addition, we select members from two different equivalence classes and define their sum in terms of the selected members. What if we had selected different members? For example, is $[3, 5] + [2, 1] = [6, 8] + [9, 8]$? We need to reassure ourselves that the defined operation makes sense in this regard. If it does, it is called *well-defined*.

Proposition 7.4. *Addition of integers is well-defined.*

Proof. To show that addition is well-defined, we select two arbitrary representatives from each equivalence class and show that they produce the same equivalence class upon being added.

Let $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{N}$ such that

$$[a_1, b_1] = [a_2, b_2] \text{ and } [c_1, d_1] = [c_2, d_2].$$

This means that $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$, so

$$a_1 + b_2 = b_1 + a_2; \tag{1}$$

$$c_1 + d_2 = d_1 + c_2 \tag{2}$$

by our definition of equivalence.

Our definition of addition of equivalence classes gives that

$$[a_1, b_1] + [c_1, d_1] = [a_1 + c_1, b_1 + d_1]$$

and

$$[a_2, b_2] + [c_2, d_2] = [a_2 + c_2, b_2 + d_2].$$

We wish to show that $[a_1 + c_1, b_1 + d_1] = [a_2 + c_2, b_2 + d_2]$.

Adding equations (1) and (2) yields:

$$(a_1 + b_2) + (c_1 + d_2) = (b_1 + a_2) + (d_1 + c_2).$$

Since addition of natural numbers is commutative and associative,

$$(a_1 + c_1) + (b_2 + d_2) = (b_1 + d_1) + (a_2 + c_2).$$

Thus $(a_1+c_1, b_1+d_1) \sim (a_2+c_2, b_2+d_2)$. Therefore $[a_1+c_1, b_1+d_1] = [a_2+c_2, b_2+d_2]$, and addition is well-defined. □

4. Properties of Addition

Definition 7.5. Let $z = [0, 0]$ until section 8.

Let $a = [m, n] \in \mathbb{Z}$. We define the *negative* of a to be $-a = [n, m]$.

Proposition 7.6. *Let $a = [m, n] \in \mathbb{Z}$. Then $a = z \Leftrightarrow m = n$.*

Proposition 7.7. (Properties of Addition)
Let $a, b, c \in \mathbb{Z}$.

- **(a)** *$a + b = b + a$ (commutative property of addition);*
- **(b)** *$(a + b) + c = a + (b + c)$ (associative property of addition);*
- **(c)** *$z + a = a$ (existence of an addition identity);*
- **(d)** *$a + (-a) = z$ (existence of additive inverses);*
- **(e)** *$a + c = b + c$ implies $a = b$ (cancellation law of addition).*

Proof. Since a, b, c are integers, they are represents by pairs of natural numbers. Let $a = [m, n]$, $b = [s, t]$, and $[u, v]$. As we prove each part, we see that all of the work was done in showing that addition is well-defined.

(a) *Commutativity:* since addition is commutative in $\mathbb{N}$,

$$a + b = [m, n] + [s, t] = [m + s, n + t] = [s + m, t + n] = [s, t] + [m, n] = b + a.$$

(b) *Associativity:* since addition is associative in $\mathbb{N}$,

$$\begin{aligned}(a + b) + c &= ([m, n] + ([s, t]) + [u, v] \\ &= [m + s, n + t] + [u, v] \\ &= [(m + s) + u, (n + t), v)] \\ &= [m + (s + u), n + (t + v)] \\ &= [m, n] + [s + u, t + v] \\ &= [m, n] + ([s, t] + [u, v]) \\ &= a + (b + c).\end{aligned}$$

(c) *Identity:* since 0 is an additive identity in $\mathbb{N}$,

$$z + a = [0, 0] + [m, n] = [0 + m, 0 + n] = [m, n] = a.$$

(d) *Inverses:* if $p \in \mathbb{N}$, then $(0, 0) \sim (p, p)$, because $0 + p = 0 + p$. Thus

$$a + (-a) = [m, n] + [n, m] = [m + n, n + m] = [m + n, m + n] = [0, 0].$$

(e) *Cancellation:* suppose that $a + c = b + c$. Adding $-c$ to both sides gives $a = b$. □

Definition 7.8. Define a binary operation called *subtraction* on $\mathbb{Z}$ as

$$- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \quad \text{given by} \quad a - b = a + (-b).$$

Clearly subtraction in not commutative or associative.

5. Multiplication of Integers

Definition 7.9. Define a binary operation called *multiplication* on $\mathbb{Z}$ as

$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \quad \text{given by} \quad [a, b] \cdot [c, d] = [ac + bd, ad + bc].$$

Proposition 7.10. *Multiplication of integers is well-defined.*

Proof. To show that multiplication is well-defined, we select two arbitrary representatives from each equivalence class and show that they produce the same equivalence class upon being multiplied.

Let $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{N}$ such that

$$[a_1, b_1] = [a_2, b_2] \text{ and } [c_1, d_1] = [c_2, d_2].$$

This means that $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$, so

$$a_1 + b_2 = b_1 + a_2 \text{ and } c_1 + d_2 = d_1 + c_2$$

by our definition of equivalence.

Our definition of multiplication of equivalence classes gives that

$$[a_1, b_1][c_1, d_1] = [a_1c_1 + b_1d_1, a_1d_1 + b_1c_1]$$

and

$$[a_2, b_2][c_2, d_2] = [a_2c_2 + b_2d_2, a_2d_2 + b_2c_2].$$

We wish to show that $[a_1c_1 + b_1d_1, a_1d_1 + b_1c_1] = [a_2c_2 + b_2d_2, a_2d_2 + b_2c_2]$. This is a little tricky, so we introduce some additional notation to shorten things. Define

$$x = a_1c_1 + b_1d_1 + a_2d_2 + b_2c_2;$$

$$y = a_1d_1 + b_1c_1 + a_2c_2 + b_2d_2.$$

Now if we show that $x = y$, we will be done by definition of equivalence. Let

$$w = a_1d_2 + b_2d_1 + b_1c_2 + a_2c_1.$$

By the cancellation law of addition of natural numbers, it suffices to show that $x + w = y + w$. This is accomplished by showing that each side is equal to $2(a_1b_2)(c_1d_2)$.

First add w to both sides of the definition of x, expand w on the right side, and use commutativity of addition to shuffle the terms of w into the expression, achieving

$$a_1c_1 + a_1d_2 + b_2c_2 + b_2d_1 + b_1d_1 + b_1c_2 + a_2d_2 + a_2c_1 = x + z.$$

Distributivity in $\mathbb{N}$ converts this into

$$a_1(c_1 + d_2) + b_2(c_2 + d_1) + b_1(d_1 + c_2) + a_2(d_2 + c_1) = x + z.$$

Now use the fact that $c_1 + d_2 = c_2 + d_1$ to obtain

$$(a_1 + b_2 + b_1 + a_2)(c_1 + d_2) = x + w.$$

Since $a_1 + b_2 = a_2 + b_1$, we have

$$2(a_1 + b_2)(c_1 + d_2) = x + w.$$

Perform the same manner of computation on the equation defining y, and you will find that

$$2(a_1 + b_2)(c_1 + d_2) = y + w.$$

Thus $x + w = y + w$, and by cancellation of addition in $\mathbb{N}$, we have $x = y$. $\square$

6. Properties of Multiplication

Definition 7.11. Let $e = [1, 0]$ until section 8.

Proposition 7.12. (Properties of Multiplication)
Let $a, b, c \in \mathbb{N}$. Then

- **(a)** *$ab = ba$ (commutative property of multiplication);*
- **(b)** *$(ab)c = a(bc)$ (associative property of multiplication);*
- **(c)** *$e \cdot a = a$ (existence of a multiplicative identity);*
- **(d)** *$z \cdot a = z$ (existence of a multiplicative pit);*
- **(e)** *$(a + b)c = ac + bc$ (distributivity of multiplication over addition;*
- **(f)** *$ab = z$ implies either $a = z$ or $b = z$ (regularity);*
- **(g)** *$ac = bc$ and $c \neq 0$ implies $a = b$ (cancellation law of multiplication).*

Proof. Since a, b, c are integers, they are represented by pairs of natural numbers. Let $a = [m, n]$, $b = [s, t]$, and $[u, v]$. We prove each part.

(a) *Commutativity:* using commutativity of addition and multiplication in $\mathbb{N}$, we have

$$ab = [m, n][s, t] = [ms + nt, mt + ns] = [sm + tn, sn + tm] = [s, t][m, n] = ba.$$

(b) *Associativity:* this requires commutativity and associativity of addition and multiplication in $\mathbb{N}$, as well as distributivity of multiplication over addition in $\mathbb{N}$. This is longer, so here we go:

$$\begin{aligned}
(ab)c &= ([m, n][s, t])[u, v] \\
&= [ms + nt, mt + ns][u, v] \\
&= [(ms + nt)u + (mt + ns)v, (ms + nt)v + (mt + ns)u] \\
&= [(msu + ntu) + (mtv + nsv), (msv + ntv) + (mtu + nsu)] \\
&= [(msu + mtv) + (ntu + nsv), (ntv + nsu) + (msv + mtu)] \\
&= [m(su + tv) + n(tu + sv), n(tv + su) + m(sv + tu)] \\
&= [m(su + tv) + n(sv + tu), n(su + tv) + m(sv + tu)] \\
&= [m, n][su + tv, sv + tu] \\
&= [m, n]([s, t][u, v]) \\
&= a(bc).
\end{aligned}$$

(c) *Identity:* $e \cdot a = [1, 0][m, n] = [1 \cdot m + 0 \cdot n, 1 \cdot n + 0 \cdot m] = [m, n] = a$.
(d) *Pit:* $z \cdot a = [0, 0][m, n] = [0 \cdot m + 0 \cdot n, 0 \cdot n + 0 \cdot m] = [0, 0] = z$.
(e) *Distributivity:*

$$\begin{aligned}
(a + b)c &= ([m, n] + [s, t])[u, v] \\
&= [m + s, n + t][u, v] \\
&= [(m + s)u + (n + t)v, (m + s)v + (n + t)u] \\
&= [mu + su + nv + tv, mv + sv + nu + tu] \\
&= [mu + nv, mv + nu] + [su + tv, sv + tu] \\
&= [m, n][u, v] + [m, n][u, v] \\
&= ac + bc.
\end{aligned}$$

(f) *Regularity:* suppose that $ab = z$. Then $[m, n][s, t] = [0, 0]$, so $[ms+nt, mt+ns] = [0, 0]$, which gives $ms + nt = mt + ns$. Assume $n \leq m$; the other case can be handled similarly. Then $n = m + k$ for some $k \in \mathbb{N}$, and we have $ms + mt + kt = mt + ms + ks$; the cancellation of addition in $\mathbb{N}$ now gives $kt = ks$, so either $s = t$ or $k = 0$. If $k = 0$, then $m = n$, and $[m, n] = z$. If $s = t$, then $[s, t] = [s, s] = z$.

(g) *Cancellation:* suppose that $ac = bc$. Then $ac - bc = z$, so $(a - b)c = z$. Since $c \neq z$, **(f)** dictates that $a - b = z$, so $a = b$. □

7. Ordering of Integers

Definition 7.13. Define a relation $\leq$ on $\mathbb{Z}$ by

$$[m, n] \leq [s, t] \Leftrightarrow m + t \leq n + s.$$

Proposition 7.14. *The relation $\leq$ on $\mathbb{Z}$ is well-defined.*

Proof. Let $[m_1, n_1] = [m_2, n_2]$ and $[s_1, t_1] = [s_2, t_2]$. where $m_i, n_i, s_i, t_i \in \mathbb{N}$ for $i = 1, 2$. Then $m_1 + n_2 = n_1 + m_2$ and $s_1 + t_2 = t_1 + s_2$. Suppose $m_1 + t_1 \leq n_1 + s_1$; we wish to show that $m_2 + t_2 \leq n_2 + s_2$.

Apply Proposition 6.47 to add $n_2 + s_2$ to both sides of $m_1 + t_1 \leq n_1 + s_1$, and use commutativity and associativity of addition in $\mathbb{N}$ to obtain

$$m_1 + n_2 + t_1 + s_2 \leq n_1 + s_1 + n_2 + s_2.$$

Apply the definition of integral equivalence to convert this to

$$m_2 + n_1 + t_2 + s_1 \leq n_1 + s_1 + n_2 + s_2.$$

Again by Proposition 6.47, we may cancel $n_1 + s_1$ from both sides and have

$$m_2 + t_2 \leq n_2 + s_2.$$

Thus inequality is a well-defined relation on $\mathbb{Z}$. □

Proposition 7.15. *The relation $\leq$ on $\mathbb{Z}$ is a total order relation.*

Proof. Let $a, b, c \in \mathbb{Z}$ such that $a = [m, n]$, $b = [s, t]$, and $[u, v]$. We prove that $\leq$ is definite, antisymmetric, and transitive.

Definiteness: Suppose that a is not less than or equal to b. Then it is false that $m+t \leq n+s$, so $n+s < m+t$, which implies $s+n \leq t+m$. Thus $[s, t] \leq [m, n]$, so $b \leq a$.

Antisymmetry: Suppose $a \leq b$ and $b \leq a$. Then $[m, n] \leq [s, t]$, so $m+t \leq n+s$, and $[s, t] \leq [m, n]$, so $s + n \leq t + m$, and $n + s \leq m + t$. Thus $m + t = n + s$, so $[m, n] = [s, t]$, and $a = b$.

Transitivity: Suppose that $a \leq b$ and $b \leq c$. Then $[m, n] \leq [s, t]$ and $[s, t] \leq [u, v]$, so $m + t \leq n + s$ and $s + v \leq t + u$. Adding these inequalities together using Proposition 6.37 part **(a)**, we have $m + t + s + v \leq n + s + tu$, so $m + v + s + t \leq n + u + s + t$; by Proposition 6.37 part **(b)**, we obtain $m + v \leq n + u$. Thus $[m, n] \leq [u, v]$, that is, $a \leq c$. □

Proposition 7.16. *Let $a \in \mathbb{Z}$ with $z \leq a$. Then there exists $s \in \mathbb{N}$ such that $a = [s, 0]$.*

Proof. By definition, $a = [m, n]$ for some $m, n \in \mathbb{Z}$. Since $z \leq a$, $[0, 0] \leq [m, n]$, so $0 + n \leq 0 + m$, so $n \leq m$. Then $m = n + s$ for some $s \in \mathbb{N}$, and $a = [n + s, n] = [s, 0]$. □

Proposition 7.17. (Properties of Inequality)
Let $a, b, c \in \mathbb{Z}$. Then

(a) *$a \leq b$ implies $a + c \leq b + c$;*
(b) *$a \leq b$ and $z \leq c$ implies $ac \leq bc$;*
(c) *$ac \leq bc$ and $z < c$ implies $a \leq b$.*

Proof. Since a, b, c are integers, they are represents by pairs of natural numbers. Let $a = [m, n]$, $b = [s, t]$, and $[u, v]$. We prove each part.

(a) Suppose that $a \leq b$. Then $[m, n] \leq [s, t]$, so $m + t \leq n + s$. Thus $(m + t) + (u + v) \leq (n + s) + (u + v)$, so $(m + u) + (t + v) \leq (n + v) + (s + u)$. Thus $[m + u, n + v] \leq [s + u, t + v]$, that is, $a + c \leq b + c$.

(b) Suppose that $a \leq b$ and $z \leq c$. Then $m + t \leq n + s$ and $c = [w, 0]$ for some $w \in \mathbb{N}$. Multiplying the first inequality by w gives $mw + tw \leq nw + sw$. Thus $[mw, nw] \leq [sw, tw]$. Since $ac = [mw, nw]$ and $bc = [sw, tw]$, the result follows.

(c) Suppose that $ac \leq bc$ and $z < c$. Now $c = [w, 0]$ for some $w \in \mathbb{N}^+$. Then $[m, n][w, 0] \leq [s, t][w, 0]$, so $[mw, nw] \leq [sw, tw]$. Thus $mw + tw \leq nw + sw$, so $(m+t)w \leq (n+s)w$, and $m+t \leq n+s$ by Proposition 6.47. Therefore $[m, n] \leq [s, t]$, that is, $a \leq b$. □

Proposition 7.18.

Problem 7.1. Let $a, b, c \in \mathbb{Z}$ with $c < z$. Show that

$$a \leq b \;\Leftrightarrow\; bc \leq ac.$$

Definition 7.19. Let $a \in \mathbb{Z}$. We say that a is *positive* if $a > z$, and we say that a is *negative* if $a < z$.

Problem 7.2. Let $a, b, c \in \mathbb{Z}$ with $c = ab$. Show that if any two of these are positive, then so is the third.

Definition 7.20. We define a function $|\cdot| : \mathbb{Z} \to \mathbb{Z}$ by

$$|a| = \begin{cases} a \text{ if } a \geq z; \\ -a \text{ otherwise .} \end{cases}$$

We call $|a|$ the *absolute value* of a.

8. Embedding

We wish to show that, in a very meaningful sense, the natural numbers can be regarded as integers. To do this, we create an injective function $\mathbb{N} \hookrightarrow \mathbb{Z}$ which preserves all of the properties of the natural numbers with which we are concerned. That is, what matters to us about the natural numbers is not how they were defined, but how they behave. Specifically, they can be added and multiplied, and they have a total order. Thus we want our injective function to preserve these properties.

Definition 7.21. The *canonical embedding* of $\mathbb{N}$ into $\mathbb{Z}$ is the function

$$\xi_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z} \quad \text{given by} \quad \xi_{\mathbb{N}}(n) = [n, 0].$$

Theorem 7.22. (Natural Embedding Theorem)
The function $\xi_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}$ is the unique nonzero function from $\mathbb{N}$ to $\mathbb{Z}$ which satisfies

(a) *$\xi_{\mathbb{N}}(m + n) = \xi_{\mathbb{N}}(m) + \xi_{\mathbb{N}}(n)$;*
(b) *$\xi_{\mathbb{N}}(mn) = \xi_{\mathbb{N}}(m)\xi_{\mathbb{N}}(n)$.*

Moreover, $\xi_{\mathbb{N}}$ is injective, and satisfies

(c) $\xi_{\mathbb{N}}(0) = z$*;*
(d) $\xi_{\mathbb{N}}(1) = e$*;*
(e) $m \leq n$ *if and only if* $\xi_{\mathbb{N}}(m) \leq \xi_{\mathbb{N}}(n)$*;*
(f) *for every* $n \in \mathbb{N}$ *there exists* $b \in \mathbb{Z}$ *such that* $\xi_{\mathbb{N}}(n) + b = \xi_{\mathbb{N}}(0)$*;*
(g) *for every* $a \in \mathbb{Z}$ *there exists* $n \in \mathbb{N}$ *such that* $a = \xi_{\mathbb{N}}(n)$ *or* $a = -\xi_{\mathbb{N}}(n)$*.*

Proof. First, let's show that $\xi_{\mathbb{N}}$ satisfies **(a)** and **(b)**, so that $\xi_{\mathbb{N}}$ preserves the arithmetic of $\mathbb{N}$.

(a) Let $m, n \in \mathbb{N}$. Then

$$\xi_{\mathbb{N}}(m+n) = [m+n, 0] = [m, 0] + [n, 0] = \xi_{\mathbb{N}}(m) + \xi_{\mathbb{N}}(n).$$

(b) Let $m, n \in \mathbb{N}$. Then

$$\xi_{\mathbb{N}}(mn) = [mn, 0] = [mn + 0 \cdot 0, 0 \cdot n + m \cdot 0] = [m, 0][n, 0] = \xi_{\mathbb{N}}(m)\xi_{\mathbb{N}}(n).$$

To show that $\xi_{\mathbb{N}}$ is unique with these properties, suppose that $\psi : \mathbb{N} \to \mathbb{Z}$ is nonzero and satisfies **(a)** and **(b)**. Being nonzero means that ψ is not defined by $\psi(n) = z$ for all n. If $\psi(1) = z$, then $\psi(n) = \psi(1 \cdot n) = \psi(1)\psi(n) = z \cdot \psi(n) = z$. Thus $\psi(1) \neq z$.

By **(a)**, $\psi(0) = \psi(0 + 0) = \psi(0) + \psi(0)$; thus the cancellation law of addition in $\mathbb{Z}$ implies $z = \psi(0)$.

By **(b)**, $\psi(1) = \psi(1 \cdot 1) = \psi(1)\psi(1)$; since $\psi(1) \neq z$, the cancellation of multiplication in $\mathbb{Z}$ implies $e = \psi(1)$.

So, $\psi(0) = [0, 0]$ and $\psi(1) = [1, 0]$. To compute $\psi(m)$, proceed by induction on m. Assume that $\psi(m-1) = [m-1, 0]$. Then $\psi((m-1)+1) = \psi(m-1) + \psi(1) = [m-1, 0] + [1, 0] = [m, 0]$. Thus $\psi = \xi_{\mathbb{N}}$.

Next we show that $\xi_{\mathbb{N}}$ is injective. Thus let $m, n \in \mathbb{N}$ such that $\xi_{\mathbb{N}}(m) = \xi_{\mathbb{N}}(n)$. Then $[m, 0] = [n, 0]$, so $m + 0 = n + 0$, so $m = n$. Thus $\xi_{\mathbb{N}}$ is injective.

(c) We have already seen this.

(d) We have already seen this.

(e) Let $m, n \in \mathbb{N}$. Then

$$m \leq n \Leftrightarrow m + 0 \leq n + 0 \Leftrightarrow [m, 0] \leq [n, 0] \Leftrightarrow \xi_{\mathbb{N}}(m) \leq \xi_{\mathbb{N}}(n).$$

(f) Let $n \in \mathbb{N}$. Set $b = [0, n]$. Then

$$\xi_{\mathbb{N}}(n) + b = [n, 0] + [0, n] = [n, n] = [0, 0] = \xi_{\mathbb{N}}(0).$$

(g) Let $a \in \mathbb{Z}$. Then $a = [m, n]$ for some $m, n \in \mathbb{Z}$. Either $m \leq n$ or $n \leq m$. If $m \leq n$, then $n = m + s$ for some $s \in \mathbb{N}$, by Proposition 6.38. Thus $a = [m, m + s] = [0, s] = -[s, 0] = -\xi_{\mathbb{N}}(s)$. On the other hand but similarly, if $n \leq m$, then $m = n + t$ for some $t \in \mathbb{N}$, and $a = [n + t, n] = [t, 0] = \xi_{\mathbb{N}}(t)$. □

In Theorem 7.22, **(f)** says that $\mathbb{Z}$ contains the additive inverses of the natural numbers, and **(g)** says that $\mathbb{Z}$ is, in some sense, the smallest set that does so.

Thus from now on, whenever it is convenient, we view $\mathbb{N}$ as a subset of $\mathbb{Z}$. Then to say that $a \in \mathbb{N} \cap \mathbb{Z}$ we mean that $a \in \xi_{\mathbb{N}}(\mathbb{N}) \subset \mathbb{Z}$. The meaning should be clear from the context.

In particular, $\xi_{\mathbb{N}}(1) = e$ by definition and $\xi_{\mathbb{N}}(0) = z$ because the additive identity of $\mathbb{Z}$ is unique. Thus we identify 1 with e and 0 with z, and may drop these temporary names.

CHAPTER 8

The Rational Numbers

1. Rational Equivalence

Proposition 8.1. *Let $\mathbb{Z}^\bullet = \mathbb{Z} \setminus \{0\}$. Define a relation on $\mathbb{Z} \times \mathbb{Z}^\bullet$ by*

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Then $\sim$ is an equivalence relation, called rational equivalence.

Proof. We wish to show that $\sim$ is reflexive, symmetric, and transitive.

(Reflexivity) Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\bullet$. Then $ab = ba$ because multiplication of integers numbers is commutative. Thus $(a, b) \sim (a, b)$, and $\sim$ is reflexive.

(Symmetry) Let $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^\bullet$. Then by symmetry of equality and commutativity of multiplication of integers,

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow (c, d) \sim (a, b).$$

Thus $\sim$ is symmetric.

(Transitivity) Let $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}^\bullet$. Suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad = bc$ and $cf = de$. Multiply the first equation by f and multiply the second equation by b to obtain $adf = bcf$ and $bcf = bde$. By transitivity of equality, $adf = bde$. By the commutativity of multiplication and cancellation, we obtain $af = be$. Thus $(a, b) \sim (e, f)$, and $\sim$ is transitive. □

2. Rational Numbers

Definition 8.2. The *rational numbers* are equivalence classes induced by the rational equivalence relation. Let $\mathbb{Q}$ denote the set of rational numbers:

$$\mathbb{Q} = \{[a, b] \mid a \in \mathbb{Z}, b \in \mathbb{Z}^\bullet\},$$

where $[a, b]$ denote the equivalence class of (a, b).

Proposition 8.3. *Let $x \in \mathbb{Q}$. Then there exist integer $a, b \in \mathbb{Z}$ with $b > 0$ such that $x = [a, b]$.*

Proof. Let $x = [c, d]$. We know that $d \neq 0$, and one sees that $[c, d] = [-c, -d]$; thus if $d > 0$, set $a = c$ and $b = d$. Otherwise, set $a = -c$ and $b = -d$. □

3. Addition of Rational Numbers

Definition 8.4. Define a binary operation called *addition* on $\mathbb{Q}$ as

$$+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \quad \text{given by} \quad [a, b][c, d] = [ad + bc, bd].$$

Proposition 8.5. *Addition of rational numbers is well-defined.*

Proof. Let $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{Z}$ such that

$$[a_1, b_1] = [a_2, b_2] \text{ and } [c_1, d_1] = [c_2, d_2].$$

This means that $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$, so

$$a_1 b_2 = b_1 a_2 \text{ and } c_1 d_2 = d_1 c_2$$

by our definition of equivalence.

Multiply the first equation by $d_1 d_2$ and the section by $b_1 b_2$ to obtain

$$a_1 b_2 d_1 d_2 = b_1 a_2 d_1 d_2 \text{ and } c_1 d_2 b_1 b_2 = d_1 c_2 b_1 b_2.$$

Add these equations to obtain

$$a_1 b_2 d_1 d_2 + c_1 d_2 b_1 b_2 = b_1 a_2 d_1 d_2 + d_1 c_2 b_1 b_2,$$

which is equivalent to

$$a_1 d_1 b_2 d_2 + b_1 c_1 b_2 d_2 = a_2 d_2 b_1 d_1 + b_2 c_2 b_1 d_1.$$

By the distributive property, we have

$$(a_1 d_1 + b_1 c_1)(b_2 d_2) = (a_2 d_2 + b_2 c_2)(b_1 d_1),$$

which, by our definition of equivalence, implies that

$$[a_1 d_1 + b_1 c_1, b_1 d_1] = [a_2 d_2 + b_2 c_2, b_2 d_2].$$

This is what we wished to show. □

4. Properties of Addition

Definition 8.6. Let $z = [0, 1]$ until section 8.

Let $x = [a, b] \in \mathbb{Q}$. We define the *negative* of x to be $-x = [-a, b]$.

Proposition 8.7. *Let $x = [a, b] \in \mathbb{Q}$. Then $x = z$ if and only if $a = 0$.*

Proof. If $x = z$, then $[a, b] = [0, 1]$, so $a \cdot 1 = b \cdot 0$, which implies that $a = 0$. If $a = 0$, then $x = [0, b]$ which is equivalent to $[0, 1]$ because $0 \cdot 1 = 0 \cdot b$. □

Proposition 8.8. (Properties of Addition)
Let $x, y, w \in \mathbb{Q}$. Then

- **(a)** *$x + y = y + x$ (commutative property of addition);*
- **(b)** *$(x + y) + w = x + (y + w)$ (associative property of addition);*
- **(c)** *$z + x = x$ (existence of an additive identity);*
- **(d)** *$x + (-x) = z$ (existence of additive inverses);*
- **(e)** *$x + w = y + w$ implies $x = y$ (cancellation law of addition).*

Proof. We prove each part. Let $x = [a, b]$, $y = [c, d]$, and $w = [f, g]$.

(a) *Commutativity:*

$$\begin{aligned} x + y &= [a, b] + [c, d] \\ &= [ad + bc, bd] \\ &= [bc + ad, bd] \\ &= [cb + da, db] \\ &= [c, d] + [a, b] \\ &= y + x. \end{aligned}$$

(b) *Associativity:*

$$\begin{aligned}(x+y)+w &= ([a,b]+[c,d])+[f,g]\\ &= [ad+bc,bd]+[f,g]\\ &= [(ad+bc)g+bdf,bdg]\\ &= [adg+bcg+bdf,bdg]\\ &= [adg+b(cg+df),bdg]\\ &= [a,b]+[cg+df,dg]\\ &= [a,b]+([c,d]+[f,g])\\ &= x+(y+w).\end{aligned}$$

(c) *Identity:*

$$z+x=[0,1]+[a,b]=[0\cdot b+1\cdot a,1\cdot b]=[a,b]=x.$$

(d) *Inverses:* [RETURN $b(-a)=-ab$ and $bb=b^2$?]

$$x+(-x)=[a,b]+[-a,b]=[ab+b(-a),bb]=[ab-ab,bb]=[0,bb]=z.$$

(e) *Cancellation:* add $-w$ to both sides. □

Definition 8.9. Define a binary operation called *subtraction* on $\mathbb{Q}$ as

$$-:\mathbb{Q}\times\mathbb{Q}\to\mathbb{Q} \quad \text{given by} \quad a-b=a+(-b).$$

5. Multiplication of Rational Numbers

Definition 8.10. Define a binary operation called *multiplication* on $\mathbb{Q}$ by

$$\cdot:\mathbb{Q}\times\mathbb{Q}\to\mathbb{Q} \quad \text{given by} \quad [a,b][c,d]=[ac,bd].$$

Proposition 8.11. *Multiplication of rational numbers is well-defined.*

Proof. Let $a_1,a_2,b_1,b_2,c_1,c_2,d_1,d_2\in\mathbb{Z}$ such that

$$[a_1,b_1]=[a_2,b_2] \text{ and } [c_1,d_1]=[c_2,d_2].$$

This means that $(a_1,b_1)\sim(a_2,b_2)$ and $(c_1,d_1)\sim(c_2,d_2)$, so

$$a_1b_2=b_1a_2 \text{ and } c_1d_2=d_1c_2$$

by our definition of equivalence.

Multiply these equations to get

$$a_1b_2c_1d_2=b_1a_2d_1c_2,$$

which is equivalent to

$$a_1c_1b_2d_2=b_1d_1a_2c_2,$$

which implies that

$$[a_1c_1,b_1d_1]=[a_2c_2,b_2d_2].$$

This is all we wanted to show. □

6. Properties of Multiplication

Definition 8.12. Let $\mathbb{Q}^* = \mathbb{Q} \setminus \{z\}$.
Let $e = [1, 1]$ until section 8.
If $x = [a, b] \in \mathbb{Q}^*$, let $x^{-1} = [b, a]$.

Proposition 8.13. *Let $x, y, w \in \mathbb{Q}$. Then*

(a) *$xy = yx$ (commutative property of multiplication);*
(b) *$(xy)w = x(yw)$ (associative property of multiplication);*
(c) *$ex = x$ (existence of a multiplicative identity);*
(d) *$zx = z$ (existence of a multiplicative pit);*
(e) *$x \neq z$ implies $xx^{-1} = e$ (existence of multiplicative inverses);*
(f) *$(x+y)w = xw+yw$ (distributive property of multiplication over addition);*
(g) *$xy = z$ implies $x = z$ or $y = z$ (regularity);*
(h) *$xw = yw$ and $w \neq z$ implies $x = y$ (cancellation law of multiplication).*

Proof. We prove each part. Let $x = [a, b]$, $y = [c, d]$, and $w = [f, g]$.

(a) *Commutativity:*

$$xy = [a, b][c, d] = [ac, bd] = [ca, db] = [c, d][a, b] = yx.$$

(b) *Associativity:*

$$(xy)w = [ac, bd][f, g] = [(ac)f, (bd)g] = [a(cf), b(dg)] = [a, b][cf, dg] = x(yw).$$

(c) *Identity:*

$$ex = [1, 1][a, b] = [1 \cdot a, 1 \cdot b] = [a, b] = x.$$

(d) *Pit:*

$$zx = [0, 1][a, b] = [0 \cdot a, 1 \cdot b] = [0, b] = z.$$

(e) *Inverses:* assume $x \neq 0$, so that $a \neq 0$. Then

$$xx^{-1} = [a, b][b, a] = [ab, ba] = [ab, ab] = [1, 1] = e.$$

(f) *Distributivity:*

$$\begin{aligned}(x + y)w &= ([a, b] + [c, d])[f, g] \\ &= [ad + bc, bd][f, g] \\ &= [adf + bcf, bdg] \\ &= [adfg + bcfg, bdgg] \\ &= [afdg + bgcf, bgdg] \\ &= [af, bg] + [cf, dg] \\ &= [a, b][f, g] + [c, d][f, g] \\ &= xw + yw.\end{aligned}$$

(g) *Regularity:* suppose $xy = z$. Then $[a, b][c, d] = 0$, so $[ac, bd] = z$, so $ac = 0$. By regularity of the integers, either $a = 0$ or $c = 0$. Thus either $x = z$ or $y = z$.

(h) *Cancellation:* since $w \neq z$, w^{-1} exists. Multiply both sides of $xw = yw$ on the right by w^{-1} to obtain $x = y$. □

Definition 8.14. Define a binary operation called *division* on $\mathbb{Q}^*$ as

$$\div : \mathbb{Q}^* \times \mathbb{Q}^* \to \mathbb{Q}^* \quad \text{given by} \quad x \div y = xy^{-1}.$$

7. Ordering of Rational Numbers

Definition 8.15. Define a relation $\leq$ on $\mathbb{Q}$ by

$$[a,b] \leq [c,d] \;\Leftrightarrow\; ad \leq bc, \text{ where } b,d > 0.$$

Proposition 8.16. *The relation $\leq$ on $\mathbb{Q}$ is well-defined.*

Proof. Suppose that $[a_1,b_1] = [a_2,b_2]$ and $[c_1,d_1] = [c_2,d_2]$, where $b_1,b_2,d_1,d_2 > 0$. By definition of equivalence, $a_1b_2 = b_1a_2$ and $c_1d_2 = d_1c_2$.

Suppose $a_1d_1 \leq b_1c_1$; we wish to show that $a_2d_2 \leq b_2c_2$.

Use 7.17 to multiply both sides of $a_1d_1 \leq b_1c_1$ by b_2d_2, and apply commutativity and associativity of multiplication in $\mathbb{Z}$ to obtain

$$a_1b_2d_1d_2 \leq b_1b_2c_1d_2.$$

Apply the definition of rational equivalence to obtain

$$a_2b_1d_1d_2 \leq b_1b_2d_1c_2.$$

Cancel b_1d_1 to obtain

$$a_2d_2 \leq b_2c_2.$$

This shows that inequality is a well-defined relation on $\mathbb{Q}$. □

Proposition 8.17. *The relation $\leq$ on $\mathbb{Q}$ is a total order relation.*

Proof. Let $x = [a,b]$, $y = [c,d]$, and $w = [f,g]$, where $b,d,g > 0$. We show that $\leq$ is definite, antisymmetric, and transitive.

Definiteness: Suppose that $y \leq x$ is false. Then $cb \leq da$ is false, so by definiteness of order in $\mathbb{Z}$, we have $da \leq cb$, so $ad \leq bc$ by commutativity of multiplication in $\mathbb{Z}$, so $[a,b] \leq [c,d]$, which means that $x \leq y$.

Antisymmetry: Suppose that $x \leq y$ and $y \leq y$. Then $ad \leq bc$ and $bc \leq ad$, so by antisymmetry in $\mathbb{Z}$, we have $ad = bc$, which means that $x = y$.

Transitivity: Suppose that $x \leq y$ and $y \leq w$. Then $ad \leq bc$ and $cg \leq df$. Multiplying the first inequality by g and the second by b and rearranging terms gives $adg \leq bcg$ and $bcg \leq bdf$. By transitivity in $\mathbb{Z}$, we have $adg \leq bdf$, and we may cancel d to get $ag \leq bf$. Thus $[a,b] \leq [f,g]$, so $x \leq w$. □

Proposition 8.18. (Properties of Inequality)
Let $x,y,w \in \mathbb{Q}$. Then

- **(a)** *$x \leq y$ implies $x + w \leq y + w$;*
- **(b)** *$x \leq y$ and $z \leq w$ implies $xw \leq yw$.*
- **(c)** *$x \leq y$ and $z \geq w$ implies $xw \geq yw$.*

Proof. Let $x = [a,b]$, $y = [c,d]$, and $w = [f,g]$, where $b,d,g > 0$.

(a) Suppose $x \leq y$; then $ad \leq bc$. Multiply by gg to get $adgg \leq bcgg$, and add $bfdg$ to get $adgg + bfdg \leq bcgg + bfdg$. Apply commutativity, associativity, and distributivity in $\mathbb{Z}$ to obtain $(ag + bf)dg \leq bg(cg + df)$. Then $[ag + bf, bg] \leq [cg + df, dg]$, so $[a,b] + [f,g] \leq [c,d] + [f,g]$. Therefore $x + w \leq y + w$.

(b) Suppose that $x \leq y$ and $z \leq w$. Now $0 \leq w$ means $[0,1] \leq [f,g]$, so $0 \leq f$, and $x \leq y$ means $ad \leq bc$. Multiply both sides of $ad \leq bc$ by fg and rearrange terms to obtain $afdg \leq bgcf$. Then $[af, bg] \leq [cf, dg]$. Therefore $xw \leq yw$.

(c) Suppose that $x \leq y$ and $z \geq w$. Now $0 \geq w$ means $w \leq z$, so $[f,g] \leq [0,1]$, whence $f \leq 0$; since $g > 0$, $fg \leq 0$. Since $x \leq y$, we have $ad \leq bc$, so $adfg \geq bcfg$

by Proposition 7.17 part XXX. Rearrange terms to obtain $bgcf \leq afdg$, whence $[cf, dg] \leq [af, bg]$, or $[af, bg] \geq [cf, dg]$. Therefore $yw \geq xw$. □

Problem 8.1. Let $x, y, w \in \mathbb{Q}$. Show that

(a) $x < y$ implies $x + w < y + w$;
(b) $x < y$ and $0 < w$ implies $xw < yw$.

Problem 8.2. [RETURN - prove this? used in cuts] Let $x, y, w \in \mathbb{Q}$ with $w < 0$. Show that

$$x \leq y \;\Leftrightarrow\; yw \leq xw.$$

8. Embedding

Definition 8.19. The *canonical embedding* of $\mathbb{Z}$ into $\mathbb{Q}$ is the function

$$\xi_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Q} \quad \text{given by} \quad \xi_{\mathbb{Z}}(a) = [a, 1].$$

Theorem 8.20. (Integral Embedding Theorem)
The function $\xi_{\mathbb{Z}} : \mathbb{N} \to \mathbb{Z}$ is the unique nonzero function from $\mathbb{Z}$ to $\mathbb{Q}$ which satisfies

(a) $\xi_{\mathbb{Z}}(a + b) = \xi_{\mathbb{Z}}(a) + \xi_{\mathbb{Z}}(b)$;
(b) $\xi_{\mathbb{Z}}(ab) = \xi_{\mathbb{Z}}(a)\xi_{\mathbb{Z}}(b)$.

Moreover, $\xi_{\mathbb{Z}}$ is injective, and satisfies

(c) $\xi_{\mathbb{Z}}(0) = z$;
(d) $\xi_{\mathbb{Z}}(1) = e$;
(e) $a \leq b$ *if and only if* $\xi_{\mathbb{Z}}(a) \leq \xi_{\mathbb{Z}}(b)$;
(f) *for every* $a \in \mathbb{Z} \setminus \{0\}$ *there exists* $y \in \mathbb{Q}$ *such that* $\xi_{\mathbb{Z}}(a)y = \xi_{\mathbb{Z}}(1)$;

Proof. We prove each part.

(a) $\xi_{\mathbb{Z}}(a + b) = [a + b, 1] = [a \cdot 1 + b \cdot 1, 1 \cdot 1] = [a, 1] + [b, 1] = \xi_{\mathbb{Z}}(a) + \xi_{\mathbb{Z}}(b)$.
(b) $\xi_{\mathbb{Z}}(ab) = [ab, 1] = [a, 1][b, 1] = \xi_{\mathbb{Z}}(a)\xi_{\mathbb{Z}}(b)$.
(c) $\xi_{\mathbb{Z}}(0) = [0, 1] = z$.
(d) $\xi_{\mathbb{Z}}(1) = [1, 1] = e$.
(e) $a \leq b \Leftrightarrow a \cdot 1 \leq b \cdot 1 \Leftrightarrow [a, 1] \leq [b, 1] \Leftrightarrow \xi_{\mathbb{Z}}(a) \leq \xi_{\mathbb{Z}}(b)$.
(f) Let $y = [1, a]$. Then $\xi_{\mathbb{Z}}(a)y = [a, 1][1, a] = [a, a] = e = \xi_{\mathbb{Z}}(1)$. □

Henceforth, we view $\mathbb{Z}$ as a subset of $\mathbb{Q}$, identified with the image of $\xi_{\mathbb{Z}}$, whenever it is convenient. In this way, we also view $\mathbb{N}$ as a subset of $\mathbb{Q}$.

The reader should ascertain from the context whether the original version of $\mathbb{Z}$, or the image of $\xi_{\mathbb{Z}}$, is meant. If only properties of $\mathbb{Z}$ which relate to addition, multiplication, and order are concerned, the difference is irrelevant.

We now denote z also by 0 and e also by 1, and we denote $[a, b]$ by $\frac{a}{b}$.

Proposition 8.21. (Archimedean Property for $\mathbb{Q}$)
Let $x, y \in \mathbb{Q}$ with $x > 0$. Then there exists $n \in \mathbb{N}$ such that $y < nx$.

Proof. If $y \leq 0$, take $n = 1$. Otherwise, we have $x, y > 0$, so there exist $a, b, c, d \in \mathbb{N}^+$ such that $x = \frac{a}{b}$ and $y = \frac{c}{d}$. Now $y < nx$ if and only if $\frac{c}{d} < \frac{na}{b}$, which is the case if and only if $bc < nad$. If $n = bc + 1$, then $n \in \mathbb{N}$ and $bc < nad$. □

CHAPTER 9

The Real Numbers

1. Dedekind Cuts

Definition 9.1. Let $\alpha \subset \mathbb{Q}$. We say that α is a *Dedekind cut* (or simply a *cut*) if

(C0) $\alpha \neq \varnothing$ and $\alpha \neq \mathbb{Q}$;
(C1) $x \in \alpha$ and $u \in \mathbb{Q} \setminus \alpha$ implies $x < u$;
(C2) α does not contain a maximal element.

Definition 9.2. Let $y \in \mathbb{Q}$. The *cut of* y is

$$\kappa_y = \{x \in \mathbb{Q} \mid x < y\}.$$

Proposition 9.3. *Let $y \in \mathbb{Q}$. Then κ_y is a Dedekind cut.*

Proof. Clear. □

Proposition 9.4. *Let $y \in \mathbb{Q}$ and let α be a Dedekind cut.*

(a) *If $y \in \alpha$, then $\kappa_y \subset \alpha$.*
(b) *If $y \notin \alpha$, then $\alpha \subset \kappa_y$.*

Proof. Both parts rely on Property **(C1)** of the definition of Dedekind cut.

Suppose $y \in \alpha$, and let $x \in \kappa_y$. Then $x < y$. If $x \in \mathbb{Q} \setminus \alpha$, then $y < x$, which is not the case. Thus $x \notin \mathbb{Q} \setminus \alpha$, so $x \in \alpha$. This proves **(a)**.

Suppose $y \notin \alpha$, and let $x \in \alpha$. Then $x < y$, so $x \in \kappa_y$. This proves **(b)**. □

2. Real Numbers

Definition 9.5. The *real numbers* are Dedekind cuts. Let $\mathbb{R}$ denote the set of real numbers:

$$\mathbb{R} = \{\alpha \in \mathcal{P}(\mathbb{Q}) \mid \alpha \text{ is a Dedekind cut}\}.$$

Definition 9.6. Let $\alpha \in \mathbb{R}$, and define *negative* α to be

$$-\alpha = \{z \in \mathbb{Q} \mid z = -u \text{ for some nonminimal } u \in \mathbb{Q} \setminus \alpha\}.$$

Proposition 9.7. *Let $\alpha \in \mathbb{R}$. Then $-\alpha \in \mathbb{R}$.*

Proof. We justify properties **(C0)**, **(C1)**, and **(C2)** of being a Dedekind cut.

(C0) Since α is a cut, $\alpha \neq \mathbb{Q}$, so there exists some $v \in \mathbb{Q} \setminus \alpha$. If $u = v + 1$, then $v < u$, so u is a nonminimal element of $\mathbb{Q} \setminus \alpha$, and $-u \in -\alpha$. Thus $-\alpha$ is nonempty. Also, since α is a cut, it is nonempty; let $x \in \alpha$. Then $x \notin \mathbb{Q} \setminus \alpha$, so $-x \notin -\alpha$. Thus $-\alpha \neq \mathbb{Q}$.

(C1) Let $z \in -\alpha$ and $c \in \mathbb{Q} \setminus (-\alpha)$. Then $z = -u$ for some $u \in \mathbb{Q} \setminus \alpha$, so $-z \in \mathbb{Q} \setminus \alpha$. Also $c \neq -v$ for any $v \in \mathbb{Q} \setminus \alpha$, so $-c \notin \mathbb{Q} \setminus \alpha$, so $-c \in \alpha$. Since α is a Dedekind cut, $-c < -z$, whence $z < c$ by Problem 8.2 [RETURN - is it a prop or a prob?].

(C2) Let $z \in -\alpha$. Then $z = -u$ for some nonminimal $u \in \mathbb{Q} \setminus \alpha$. Since u is nonminimal, there exists $v \in \mathbb{Q} \setminus \alpha$ such that $v < u$. Let $y = -v$; then $y \in \alpha$, and $-u < -v$, so $z < y$. Thus z is nonmaximal in α. □

Definition 9.8. Let $\mathbb{R}^* = \mathbb{R} \setminus \{\kappa_0\}$.

Let $\alpha \in \mathbb{R}^*$. Define α *inverse* as

$$\alpha^{-1} = \begin{cases} \{x \in \mathbb{Q} \mid x = y^{-1} \text{ for some nonminimal } y \in \mathbb{Q} \setminus \alpha\} \cup \kappa_0 & \text{if } \kappa_0 \subset \alpha \\ -((-\alpha)^{-1}) & \text{otherwise.} \end{cases}$$

Proposition 9.9. *Let $\alpha \in \mathbb{R}^*$. Then $\alpha^{-1} \in \mathbb{R}^*$.*

3. Addition of Real Numbers

Definition 9.10. Let $X, Y \subset \mathbb{Q}$. Define the *sum* of A and B as

$$X + Y = \{z \in \mathbb{Q} \mid z = x + y \text{ for some } x \in X, y \in Y\}.$$

Proposition 9.11. *Let $\alpha, \beta \in \mathbb{R}$. Then $\alpha + \beta \in \mathbb{R}$. This induces a binary operation*

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

called addition.

Proof. To show that $\alpha + \beta \in \mathbb{R}$, we need to show that $\alpha + \beta$ is a Dedekind cut by verifying Properties **(C0)**, **(C1)**, and **(C2)**.

(C0) Clearly $\gamma \subset \mathbb{Q}$ is nonempty. Suppose $u \in \mathbb{Q} \setminus \alpha$ and $v \in \mathbb{Q} \setminus \beta$; we wish to show that $u + v \in \mathbb{Q} \setminus \gamma$, so that $\gamma \neq \mathbb{Q}$. Since $\mathbb{Q}$ is closed under addition, $u + v \in \mathbb{Q}$. Let $z \in \gamma$; then $z = x + y$ for some $x \in \alpha$ and $y \in \beta$. Now $x < u$ and $y < v$, so $x + y < u + v$, so $z \neq u + v$, so $u + v \notin \gamma$.

(C1) Let $z \in \gamma$ and $u \in \mathbb{Q} \setminus \gamma$. Then $z = x + y$ for some $x \in \alpha$ and $y \in \beta$. Suppose that $u \leq z$; then $u - y \leq x$, which implies that $u - y \in \alpha$. But then $u = (u - y) + y \in \gamma$, a contradiction. Thus $z < u$.

(C2) Still with $z = x + y$, we show that z is not maximal in γ. Since α and β are cuts, x and y are not maximal elements in α and β, respectively. Thus there exists $x_1 \in \alpha$ and $y_1 \in \beta$ such that $x < x_1$ and $y < y_1$. Then $x_1 + y_1 \in \gamma$, and $z < x_1 + y_1$; thus z is not maximal in C.

This shows that $\alpha + \beta \in \mathbb{R}$, so $\mathbb{R}$ is closed under addition; thus addition is a binary operator on $\mathbb{R}$. □

Proposition 9.12. (Properties of Addition)
Let $\alpha, \beta, \gamma \in \mathbb{R}$. Then

- **(a)** *$\alpha + \beta = \beta + \alpha$ (commutative property of addition);*
- **(b)** *$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ (associative property of addition);*
- **(c)** *$\kappa_0 + \alpha = \alpha$ (existence of an additive identity);*
- **(d)** *$\alpha + (-\alpha) = \kappa_0$ (existence of additive inverses);*
- **(e)** *$\alpha + \gamma = \beta + \gamma$ implies $\alpha = \beta$ (cancellation law of addition).*

Proof. We prove each part.

(a) *Commutativity:*

$$\alpha + \beta = \{x + y \mid x \in \alpha, y \in \beta\} = \{y + x \mid x \in \alpha, y \in \beta\} = \beta + \alpha.$$

(b) *Associativity:*

$$\begin{aligned}(\alpha+\beta)+\gamma &= \{(x+y)+z \mid x\in\alpha, y\in\beta, z\in\gamma\}\\ &= \{x+(y+z) \mid x\in\alpha, y\in\beta, z\in\gamma\}\\ &= \alpha+(\beta+\gamma).\end{aligned}$$

(c) *Identity:* we show containment in both directions.
($\subset$) Let $z\in\kappa_0+\alpha$. Then $z=x+y$ for some $x\in\kappa_0$ and $y\in\alpha$. Since $x<0$, $x+y<y$, so $x+y\in\alpha$.
($\supset$) Let $z\in\alpha$. Then z is nonminimal, so there exists y such that $y\in\alpha$ and $z<y$. Let $x=z-y$; now $x<0$, so $x\in\kappa_0$, and $z=x+y\in(\kappa_0+\alpha)$.

(d) *Inverses:* we show containment in both directions.
($\subset$) Let $z\in\alpha+(-\alpha)$; then $z=x+y$ for some $x\in\alpha$ and $y\in(-\alpha)$. Now $y=-w$ for some $w\in\mathbb{Q}\setminus\alpha$. Thus $w>x$, so $z=x-w<0$. Thus $z\in\kappa_0$.
($\supset$) Let $x\in\kappa_0$. Then $x<0$, so $0<-x$. Let $A=\{n\in\mathbb{N} \mid n(-x)\notin\alpha\}$.

We wish to show that A is nonempty. Since α is a Dedekind cut, there exists $y\in\mathbb{Q}\setminus\alpha$, and by Proposition 8.21, there exists $n\in\mathbb{N}$ such that $y<n(-x)$; in this case, $n(-x)\notin\alpha$, so A is nonempty.

Let $m=\min A$, which exists by the Well-Ordering Principle. Clearly, $m>0$. Set

$$y=\begin{cases}\frac{2m-1}{2}(-x) & \text{if } m(-x) \text{ is minimal in } \mathbb{Q}\setminus\alpha;\\ (m-1)(-x) & \text{otherwise.}\end{cases}$$

Now $y\in\alpha$, $y-x\in\mathbb{Q}\setminus\alpha$, and $y-x$ is not a minimum element of $\mathbb{Q}\setminus\alpha$. Thus $-(y-x)=x-y\in-\alpha$. Therefore $x=y+(x-y)\in\alpha+(-\alpha)$.

(e) *Cancellation:* add $-\gamma$ to both sides. □

Definition 9.13. Define a binary operation called *subtraction* on $\mathbb{R}$ as

$$-:\mathbb{R}\times\mathbb{R}\to\mathbb{R} \quad \text{given by} \quad \alpha-\beta=\alpha+(-\beta).$$

4. Multiplication of Real Numbers

The product of two negative rational numbers is positive; this makes working with multiplication of sets more difficult than was the case for addition. The exploration is clearer if we begin by eliminating the negative rationals.

Definition 9.14. Let $X\subset\mathbb{Q}$. The *positive part* of X is

$$\widetilde{X}=\{x\in X \mid x>0\}.$$

Definition 9.15. Let $X,Y\subset\widetilde{\mathbb{Q}}$. Define the *product* of X and Y as

$$XY=\{z\in\mathbb{Q} \mid z=xy \text{ for some } x\in X, y\in Y\}.$$

Proposition 9.16. *Let $X,Y,Z\subset\widetilde{\mathbb{Q}}$. Then*

(a) $XY=YX$;
(b) $(XY)Z=X(YZ)$;
(c) $(X+Y)Z\subset XZ+YZ$;
(d) $\varnothing X=\varnothing$.

Proof. Part **(a)**:

$$XY=\{xy \mid x\in X, y\in Y\}=\{yx \mid x\in X, y\in Y\}=YX.$$

Part **(b)**:

$$(XY)Z = \{(xy)z \mid x \in X, y \in Y, z \in Z\} = \{x(yz) \mid x \in X, y \in Y, z \in Z\}.$$

Part **(c)**:

$$\begin{aligned}(X+Y)Z &= \{(x+y)z \mid x \in X, y \in Y, z \in Z\} \\ &= \{xz + yz \mid x \in X, y \in Y, z \in Z\} \\ &\subset \{xz_1 + yz_2 \mid x \in X, y \in Y, z_1, z_2 \in Z\} \\ &= XZ + YZ.\end{aligned}$$

Part **(d)** is vacuously true. □

Proposition 9.17. *Let $\alpha \in \mathbb{R}$.*

(a) $\widetilde{\kappa_0}\widetilde{\alpha} = \widetilde{\kappa_0}$*;*
(b) $\widetilde{\kappa_1}\widetilde{\alpha} = \widetilde{\alpha}$*;*
(c) $\widetilde{\alpha}\widetilde{\alpha^{-1}} = \widetilde{\kappa_1}$.

Proof. We prove each part.

(a) This is Proposition 9.16 part **(d)**.

(b) We prove both directions of inclusion. In light of **(a)**, we may assume that $\widetilde{\alpha}$ is nonempty, and therefore $\widetilde{\kappa_1}\widetilde{\alpha}$ is nonempty.

($\subset$) Let $z \in \widetilde{\kappa_1}\widetilde{\alpha}$; then $z = xy$ for some $x \in \widetilde{\kappa_1}$ and $y \in \widetilde{\alpha}$. Now $0 < x < 1$, so $0 < xy < y$; since α is a Dedekind cut, we see that $z \in \widetilde{\alpha}$.

($\supset$) Let $y \in \widetilde{\alpha}$. Since y is not maximal in $\widetilde{\alpha}$, there exists $y_1 \in \widetilde{\alpha}$ such that $0 < y < y_1$. Thus $0 < \frac{y}{y_1} < 1$; set $x_1 = \frac{y}{y_1}$. Then $y = x_1 y_1 \in \widetilde{\kappa_0}\widetilde{\alpha}$.

(c) We prove both directions of inclusion. In light of **(a)**, we may assume that $\widetilde{\alpha}$ is nonempty, and therefore $\widetilde{\alpha^{-1}}$ and $\widetilde{\alpha}\widetilde{\alpha^{-1}}$ are nonempty.

($\subset$) Let $z \in \widetilde{\alpha}\widetilde{\alpha^{-1}}$. Then $z = xy$ for some $x \in \widetilde{\alpha}$ and $y \in \widetilde{\alpha^{-1}}$. Then $y = u^{-1}$ for some nonminimal $u \in \mathbb{Q} \setminus \alpha$. Now $0 < x < u$, so $z = \frac{x}{u} < 1$. Thus $z \in \widetilde{\kappa_1}$.

($\supset$) Let $z \in \widetilde{\kappa_1}$. Then $0 < z < 1$. Either $1 \in \alpha$ or $1 \in \alpha^{-1}$ [RETURN]; since $(\alpha^{-1})^{-1} = \alpha$, we may assume without loss of generality that $1 \in \alpha$. by 9.16 part **(a)**.

Let $A = \{n \in \mathbb{N} \mid \frac{1}{z^n} \notin \alpha\}$. This set is nonempty [RETURN]; let $m = \min A$. By the previous paragraph, $n > 1$ [RETURN]. Let $x = \frac{1}{z^{n-1}}$ and $y = z^n$. Then $x \in \widetilde{\alpha}$, $y \in \widetilde{\alpha^{-1}}$, and $z = xy$. □

****

Definition 9.18. Let $\alpha, \beta \in \mathbb{R}$. Set

$$\alpha * \beta = \{x \in \mathbb{Q} \mid x = ab \text{ for some } a \in \alpha \setminus \kappa_0 \text{ and } b \in \beta \setminus \kappa_0\} \cup \kappa_0.$$

Define the *product* of α and β as

$$\alpha \cdot \beta = \begin{cases} \alpha * \beta & \text{if } \kappa_0 \subsetneq \alpha, \beta; \\ -((-\alpha) * \beta) & \text{if } \alpha \subsetneq \kappa_0 \text{ and } \kappa_0 \subsetneq \beta; \\ -(\alpha * (-\beta)) & \text{if } \kappa_0 \subsetneq \alpha \text{ and } \beta \subsetneq \kappa_0; \\ (-\alpha) * (-\beta) & \text{if } \alpha, \beta \subsetneq \kappa_0; \\ \kappa_0 & \text{if } \alpha = \kappa_0 \text{ or } \beta = \kappa_0. \end{cases}$$

Proposition 9.19. *Let $\alpha, \beta \in \mathbb{R}$. Then $\alpha \cdot \beta \in \mathbb{R}$. This induces a binary operation*

$$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

called multiplication.

Proof. Let $\gamma = \alpha \cdot \beta$; we wish to show that γ is a Dedekind cut by verifying the properties of Definition 9.1. By the nature of the case structure, it suffices to assume that $\kappa_0 \subsetneq \alpha, \beta$, so that $\gamma = \alpha * \beta$.

(C0) Clearly $\kappa_0 \subset \gamma$, so γ is nonempty. Also, if $u \in \mathbb{Q} \setminus \alpha$ and $v \in \mathbb{Q} \setminus \beta$, then $xy < uv$ for every $x \in \alpha \setminus \kappa_0$ and $y \in \beta \setminus \kappa_0$, so $uv \notin \gamma$; thus $\gamma \neq \mathbb{Q}$.

(C1) Let $z \in \gamma$ and $u \in \mathbb{Q} \setminus \gamma$. Since $\kappa_0 \subset \gamma$, we see that $u > 0$. If $z \leq 0$, then $z < u$. Otherwise, $z = xy$ for some $x \in \alpha$ and $b \in \beta$, with $x, y > 0$.

Suppose that $u \leq z$; then $u/y \leq x$, which implies that $u/y \in \alpha$. Set $u/y = x_1 \in \alpha$; then $u = x_1 y \in \alpha * \beta = \gamma$, a contradiction. Thus $z < u$.

(C2) Since α and β properly contain κ_0, each contains an element which is greater than 0, and the product of these elements is also greater than zero and is in γ. Thus 0 is not maximal in γ. Let $z \in \gamma$; we may assume that $z > 0$, so that $z = xy$ for some $x \in \alpha$ and $y \in \beta$ with $x, y > 0$. Now x and y are not maximal in α and β, respectively, so there exist $x_1 \in \alpha$ and $y_1 \in \beta$ such that $x < x_1$ and $y < y_1$. Then $z = xy < x_1 y_1$, and $x_1 y_1 \in \gamma$, so z is not a maximum element of γ.

This shows that $\alpha \cdot \beta \in \mathbb{R}$, so $\mathbb{R}$ is closed under multiplication; thus multiplication is a binary operator on $\mathbb{R}$. □

Proposition 9.20. (Properties of Multiplication)
Let $\alpha, \beta, \gamma \in \mathbb{R}$. Then

- **(a)** *$\alpha\beta = \beta\alpha$ (commutative property of multiplication);*
- **(b)** *$(\alpha\beta)\gamma = \alpha(\beta\gamma)$ (associative property of multiplication);*
- **(c)** *$\kappa_1\alpha = \alpha$ (existence of a multiplicative identity);*
- **(d)** *$\kappa_0\alpha = \kappa_0$ (existence of a multiplicative pit);*
- **(e)** *$\alpha \neq \kappa_0$ implies $\alpha\alpha^{-1} = \kappa_1$ (existence of multiplicative inverses);*
- **(f)** *$(\alpha+\beta)\gamma = \alpha\gamma+\beta\gamma$ (distributive property of multiplication over addition);*
- **(g)** *$\alpha\beta = \kappa_0$ implies $\alpha = \kappa_0$ or $\beta = \kappa_0$ (regularity);*
- **(h)** *$\alpha\gamma = \beta\gamma$ and $\gamma \neq \kappa_0$ implies $\alpha = \beta$ (cancellation law of multiplication).*

Proof. We prove each part, assuming that κ_0 is properly contained in α, β, and γ. The proof will actually be clearer if we ignore all rational numbers less than zero; assume all sets are subsets of $\mathbb{Q} \setminus \kappa_0$.

(a) *Commutativity:*

$$\alpha\beta = \{xy \mid x \in \alpha, y \in \beta\} = \{yx \mid x \in \alpha, y \in \beta\} = \beta\alpha.$$

(b) *Associativity:*

$$(\alpha\beta)\gamma = \{(xy)z \mid x \in \alpha, y \in \beta, z \in \gamma\} = \{x(yz) \mid x \in \alpha, y \in \beta, z \in \gamma\} = \alpha(\beta\gamma).$$

(c) *Identity:* we show containment in each direction.
($\subset$) Let $z \in (\kappa_1\alpha) \setminus \kappa_0$. Then $z = xy$ for some $x \in \kappa_1$ and $y \in \alpha$ with $0 < x < 1$ and $0 < y$.

□

Definition 9.21. Define a binary operation called *division* on $\mathbb{R}^*$ as

$$\div : \mathbb{R}^* \times \mathbb{R}^* \to \mathbb{R}^* \quad \text{given by} \quad \alpha \div \beta = \alpha\beta^{-1}.$$

5. Ordering of Real Numbers

Proposition 9.22. *Define a relation $\leq$ on $\mathbb{R}$ by*

$$\alpha \leq \beta \Leftrightarrow \alpha \subset \beta.$$

Then $\leq$ is a total order relation.

Proof. By Proposition 1.10, this is a partial order.

Let $\alpha, \beta \in \mathbb{R}$. To show that $\leq$ is a total order on $\mathbb{R}$, we wish to show that either $\alpha \leq \beta$ or $\beta \leq \alpha$. Thus suppose that β is not less than or equal to α. Then β is not contained in α, so there exists $b \in \beta$ such that $b \notin \alpha$. Then by Proposition 9.4,

$$\alpha \subset \kappa_b \subset \beta.$$

Thus $\alpha \leq \beta$. □

Proposition 9.23. *Let $\alpha, \beta, \gamma \in \mathbb{R}$. Then*

(a) *$\alpha \leq \beta$ implies $\alpha + \gamma \leq \beta + \gamma$;*
(b) *$\alpha \leq \beta$ and $\kappa_0 \leq \gamma$ implies $\alpha\gamma \leq \beta\gamma$.*

6. Embedding

Definition 9.24. The *canonical embedding* of $\mathbb{Q}$ into $\mathbb{R}$ is the function

$$\xi_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R} \quad \text{given by} \quad \xi_{\mathbb{Q}}(x) = \kappa_x.$$

Theorem 9.25. (Rational Embedding Theorem)
The function $\xi_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R}$ is the unique nonzero function from $\mathbb{Q}$ to $\mathbb{R}$ which satisfies

(a) *$\xi_{\mathbb{Q}}(a + b) = \xi_{\mathbb{Q}}(a) + \xi_{\mathbb{Q}}(b)$;*
(b) *$\xi_{\mathbb{Q}}(ab) = \xi_{\mathbb{Q}}(a)\xi_{\mathbb{Q}}(b)$.*

Moreover, $\xi_{\mathbb{Q}}$ is injective, and satisfies

(c) *$\xi_{\mathbb{Q}}(0) = \kappa_0$;*
(d) *$\xi_{\mathbb{Q}}(1) = \kappa_1$;*
(e) *$a \leq b$ if and only if $\xi_{\mathbb{Q}}(a) \leq \xi_{\mathbb{Q}}(b)$.*

Henceforth, we view $\mathbb{Q}$ as a subset of $\mathbb{R}$, identified with the image of $\xi_{\mathbb{Q}}$, whenever it is convenient. The reader should ascertain from the context whether the original version of $\mathbb{Q}$, or the image of $\xi_{\mathbb{Q}}$, is meant. If only properties of $\mathbb{Q}$ which relate to addition, multiplication, and order are concerned, the difference is irrelevant.

Moreover, we now denote κ_0 also by 0 and κ_1 also by 1.

7. Maxima and Minima

Definition 9.26. Let $\leq$ be a total order on a set X, and let $m \in X$.

We say that m is a *maximum* element of X if $x \leq m$ for every $x \in X$.

We say that m is a *minimum* element of X if $m \leq x$ for every $x \in X$.

If m is a maximum or a minimum, then we say that m is an *extremum*.

[RETURN - this definition is a copy of that in relations chapter (needed a few times between then and now)]

Proposition 9.27. *Let $\leq$ be a total order on a set X.*

If X has a maximum, it is unique, and is denoted by $\max X$.

If X has a minimum, it is unique, and is denoted by $\min X$.

Proof. Let $m_1, m_2 \in X$. Suppose m_1 and m_2 are maxima for X. Then $x \leq m_1$ and $x \leq m_2$ for every $x \in X$. Since m_1 and m_2 are both in X, this implies that $m_2 \leq m_1$ and $m_1 \leq m_2$. Thus, by antisymmetry, $m_1 = m_2$. The demonstration if m_1 and m_2 are minima is analogous. □

If $\leq$ is a total order on a set X and A is a subset of X, then $\leq$ (restricted to A) is a total order on A. Thus the definition of maximum and minimum do not need to reference subsets to attain their highest level of generality. This is not true of upper and lower bounds, which we define next.

Definition 9.28. Let $\leq$ be a total order on a set X. Let $A \subset X$ and let $b \in X$.

We say that b is an *upper bound* for A if $a \leq b$ for every $a \in A$. If A has an upper bound, we say that A is *bounded above*.

We say that b is a *lower bound* for A if $b \leq a$ for every $a \in A$. If A has a lower bound, we say that A is *bounded below*. We say that A is *bounded* if A is bounded above and A is bounded below.

It is clear that a maximum is an upper bound and a minimum is a lower bound.

Example 9.1. Let $X = \mathbb{Z}$ and $A = \{-25, -2, 6, 23, 32, 33\}$. Then A has a maximum, which is 33, and A has a minimum, which is -25. Thus A is bounded above, and some upper bounds (in $\mathbb{Z}$) are 33, 34, 100, and 2034. Also A is bounded below, and some lower bounds (in $\mathbb{Z}$) are -25, -50, -100, and so forth.

Proposition 9.29. *Let $A \subset \mathbb{Z}$ be nonempty.*

(a) *If A is bounded above, then A has a maximum element.*
(b) *If A is bounded below, then A has a minimum element.*

Proof. Suppose A is bounded above, and let b be an upper bound. Let $D = \{b - a \mid a \in A\}$. Then b is a set of nonnegative integers, which we view as a subset of $\mathbb{N}$. Since A is nonempty, it is clear that D is nonempty. Thus D has a minimum element, say $d \in D$ is a minimum. Then $d = b - a$ for some $a \in A$.

Now if $x \in A$, then $b - a \leq b - x$, so $-a \leq -x$, whence $x \leq a$. Thus a is a maximum element of A.

The argument for A bounded below is similar. □

No such proposition holds for the rational numbers.

Example 9.2. Let $X = \mathbb{Q}$ and $A = \{x \in \mathbb{Q} \mid 1 < x < 2\}$. Then A does not have a minimum or a maximum. However, A is bounded, and some upper bounds (in $\mathbb{Q}$) for A are 2, $\frac{3}{2}$, $\frac{100}{3}$, and so forth.

Of these upper bounds, we see that 2 is somehow "the best" upper bound; in fact, it is the least upper bound.

8. Suprema and Infima

Definition 9.30. Let $\leq$ be a total order on a set X. Let $A \subset X$ and let $b \in X$.

We say that b is a *supremum* (or *least upper bound*) for A in X if

(SUP1) $a \leq b$ for every $a \in A$;
(SUP2) $a \leq c$ for every $a \in A$ implies $b \leq c$.

We say that u is an *infimum* (or *greatest lower bound*) for A in X if

(INF1) $b \leq a$ for every $a \in A$;
(INF2) $c \leq a$ for every $a \in A$ implies $c \leq b$.

Proposition 9.31. *Let $\leq$ be a total order on a set X, and let $A \subset X$.*
If A has a supremum in X, it is unique, and is denoted by $\sup A$.
If A has an infimum in X, it is unique, and is denoted by $\inf A$.

Proof. Let $b_1, b_2 \in X$. Suppose b_1 and b_2 are suprema for A. Then $a \leq b_1$ and $a \leq b_2$ for every $a \in A$ by **(SUP1)** so $b_1 \leq b_2$ and $b_2 \leq b_1$ by **(SUP2)**. Thus $b_1 = b_2$ by antisymmetry. The demonstration if b_1 and b_2 are infima is analogous. □

Example 9.3. Let $X = \mathbb{Q}$ and $A = \{x \in \mathbb{Q} \mid 1 < x < 2\}$. Then A does not have a minimum or a maximum; however, $\sup A = 2$ and $\inf A = 1$.

9. Completeness

Theorem 9.32. *Let $\mathcal{A} \subset \mathbb{R}$ be a nonempty subset which is bounded above, and let $\sigma = \cup\mathcal{A}$. Then*

(a) $\sigma \in \mathbb{R}$;
(b) $\sup(\mathcal{A}) = \sigma$.

Proof. To show that $\sigma \in \mathbb{R}$, we demonstrate properties **(C0)**, **(C1)**, and **(C2)**.

(C0) Since $\mathcal{A}$ is nonempty, it contains a Dedekind cut, which is itself nonempty. An element of this cut is an element of σ, so σ is nonempty.

Since $\mathcal{A}$ is bounded above, there exists an upper bound $\beta \in \mathbb{R}$. By the definition of order on $\mathbb{R}$, $\alpha \subset \beta$ for every $\alpha \in \mathcal{A}$. Thus $\sigma \subset \beta$.

Now β is a Dedekind cut, so $\mathbb{Q} \setminus \beta$ is nonempty, and since $\sigma \subset \beta$, $\mathbb{Q} \setminus \beta \subset \mathbb{Q} \setminus \sigma$. Thus $\mathbb{Q} \setminus \sigma$ is nonempty; this proves **(C0)**.

(C1) Let $a \in \sigma$ and $u \in \mathbb{Q} \setminus \alpha$. Then $a \in \alpha$ for some $\alpha \in \mathcal{A}$, and u is not in any element of $\mathcal{A}$. In particular, $u \notin \alpha$, so $a < u$; this proves **(C1)**.

(C2) Suppose that σ contains a maximum; say $m \in \sigma$ is a maximum. Then $m \in \alpha$ for some $\alpha \in \mathcal{A}$. Clearly m is a maximum in α, since $\alpha \subset \sigma$. This contradicts that α is a Dedekind cut. Thus σ does not contain a maximum; this proves **(C2)**.

To show that $\sup \mathcal{A} = \sigma$, we verify properties **(SUP1)** and **(SUP2)**.

(SUP1) Let $\alpha \in \mathcal{A}$. Then $\alpha \subset \cup\mathcal{A} = \sigma$, so $\alpha \leq \sigma$; this proves **(SUP1)**.

(SUP2) Let τ be an upper bound for $\mathcal{A}$. Then $\alpha \leq \tau$ for every $\alpha \in \mathcal{A}$; that is, $\alpha \subset \tau$ for every $\alpha \in \mathcal{A}$, so $\cup\mathcal{A} \subset \tau$. Thus $\sigma \leq \tau$; this proves **(SUP2)**. □

Corollary 9.33. (Completeness of $\mathbb{R}$)
Every subset of the real numbers which is bounded above has a supremum.

Proposition 9.34. (Archimedean Property)
Let $a, b \in \mathbb{R}$ with $a > 0$ and $b > 0$. Then there exists $n \in \mathbb{N}$ such that $b \leq na$.

Proof. Suppose that the Archimedean property fails. Then there exists $a, b \in \mathbb{R}$ with $a > 0$ and $b > 0$ such that $na < b$ for every $n \in \mathbb{N}$. Set $A = \{na \mid n \in \mathbb{N}\}$. Now A is bounded above by b, so by the completeness property of $\mathbb{R}$, there exists $s \in \mathbb{R}$ such that $s = \sup(A)$. Since $a > 0$ we have $s < s + a$, so $s - a < s$. Since s is a least upper bound for A, $s - a$ is not an upper bound for A; thus there exists $na \in A$ such that $s - a < na$. This implies that $s < (n+1)a \in A$, which contradicts that $s = \sup(A)$. □

Proposition 9.35. (Density of $\mathbb{Q}$)
Let $a, b \in \mathbb{R}$ with $a < b$. Then there exists $q \in \mathbb{Q}$ such that $a < q < b$.

Proof. Set $c = b - a$, and note that $c > 0$. By the Archimedean property, there exists $n \in \mathbb{N}$ such that $1 \leq nc$, which shows that $1 \leq nb - na$, or $na + 1 \leq nb$.

Let $m = \min\{x \in \mathbb{N} \mid na < x\}$; this m exists by the Well-Ordering Principle of the natural numbers. Now $m \leq na+1$, for otherwise $na+1 < m$ and $na < m-1 < m$, contradicting the minimality of m. Therefore $na < m < na + 1 < nb$. Divide by n to achieve $a < \frac{m}{n} < b$. With $q = \frac{m}{n}$, the proof is complete. □

CHAPTER 10

Complex Numbers

1. Complex Numbers

Definition 10.1. The *complex numbers* are ordered pairs of real numbers. Let $\mathbb{C}$ denote the set of complex numbers:

$$\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}.$$

2. Addition of Complex Numbers

Definition 10.2. Define a binary operation called *addition* on $\mathbb{C}$ as

$$+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \quad \text{given by} \quad (x_1, y_1) + (x_2, y_2) = (x_1 + y_1, x_1, y_2).$$

3. Properties of Addition

Definition 10.3. Let $h \in \mathbb{C}$ be given by $h = (0, 0)$ until section 6.
Let $z = (x, y) \in \mathbb{C}$. We define the *negative* of x to be $-x = (-x, -y)$.

Proposition 10.4. (Properties of Addition)
Let $a, b, c \in \mathbb{C}$. Then

- **(a)** $a + b = b + a$ *(commutative property of addition);*
- **(b)** $(a + b) + c = a + (b + c)$ *(associative property of addition);*
- **(c)** $h + a = a$ *(existence of an additive identity);*
- **(d)** $a + (-a) = h$ *(existence of additive inverses);*
- **(e)** $a + c = b + c$ *implies* $a = b$ *(cancellation law of addition).*

4. Multiplication of Complex Numbers

Definition 10.5. Define a binary operation called *multiplication* on $\mathbb{C}$ as

$$\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \quad \text{given by} \quad (x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + y_1 x_2).$$

5. Properties of Multiplication

Definition 10.6. Let $\mathbb{C}^* = \mathbb{Q} \setminus \{h\}$.
Let $e = [1, 1]$ until section 6.
If $a = (x, y) \in \mathbb{C}^*$, let $a^{-1} = (\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2}$.

Proposition 10.7. *Let $a, b, c \in \mathbb{C}$. Then*

- **(a)** $ab = bc$ *(commutative property of multiplication);*
- **(b)** $(ab)c = a(bc)$ *(associative property of multiplication);*
- **(c)** $ea = a$ *(existence of a multiplicative identity);*
- **(d)** $ha = a$ *(existence of a multiplicative pit);*
- **(e)** $a \neq z$ *implies* $aa^{-1} = e$ *(existence of multiplicative inverses);*
- **(f)** $(a + b)c = ac + bc$ *(distributive property of multiplication over addition);*

(g) *$ab = h$ implies $a = h$ or $b = h$ (regularity);*
(h) *$ac = bc$ and $c \neq h$ implies $a = c$ (cancellation law of multiplication).*

6. Embedding

Definition 10.8. The *canonical embedding* of $\mathbb{R}$ into $\mathbb{C}$ is the function

$$\xi_{\mathbb{R}} : \mathbb{R} \to \mathbb{C} \quad \text{given by} \quad \xi_{\mathbb{R}}(x) = (x, 0).$$

Theorem 10.9. (Real Embedding Theorem)
The function $\xi_{\mathbb{R}} : \mathbb{R} \to \mathbb{C}$ is the unique nonzero function from $\mathbb{R}$ to $\mathbb{C}$ which satisfies

(a) $\xi_{\mathbb{Q}}(a + b) = \xi_{\mathbb{Q}}(a) + \xi_{\mathbb{Q}}(b)$;
(b) $\xi_{\mathbb{Q}}(ab) = \xi_{\mathbb{Q}}(a)\xi_{\mathbb{Q}}(b)$.

Moreover, $\xi_{\mathbb{Q}}$ is injective, and satisfies

(c) $\xi_{\mathbb{Q}}(0) = h$;
(d) $\xi_{\mathbb{Q}}(1) = e$;

Henceforth, we view $\mathbb{R}$ as a subset of $\mathbb{C}$, identified with the image of $\xi_{\mathbb{R}}$, whenever it is convenient. The reader should ascertain from the context whether the original version of $\mathbb{R}$, or the image of $\xi_{\mathbb{R}}$, is meant.

CHAPTER 11

Euclidean Space

1. Cartesian Space

The set of real numbers may be viewed geometrically as a line. We may also view the cartesian product of $\mathbb{R}$ with itself as a plane, and the cartesian product of three copies of $\mathbb{R}$ with itself as space. We generalize this.

Definition 11.1. Let A be a set and let $n \in \mathbb{N}$. Set $A_i = A$ for $i \in \mathbb{N}_n^+$. Define *n-dimensional cartesian A-space* be to

$$A^n = \begin{cases} \{\varnothing\} & \text{if } n = 0; \\ \times_{i=1}^n A_i & \text{if } n \geq 1. \end{cases}$$

Recall that $\times_{i=1}^n A_i$ is the product of a family of sets, indexed in this case by $\mathbb{N}_n^+$. An element of this set is a function from $\mathbb{N}_n^+$ to A, and is usually referred to as a *point* in n-dimensional cartesian A-space, or as an ordered n-tuple with entries from A. Thus $A^n = \mathcal{F}(\mathbb{N}_n^+, A)$. We adopt the convention of using a bold font to designate ordered n-tuples. Thus let $\boldsymbol{a} \in A^n$. Then $\boldsymbol{a} : \mathbb{N}_n^+ \to A$; we write $\boldsymbol{a} = (a_1, \ldots, a_n)$ to say that $\boldsymbol{a}(i) = a_i$.

We take the approach of defining geometric notions in terms of the number systems we have already developed; these number system, in turn, have been constructed from the axioms of set theory. Thus the axioms of set theory form the basic postulational foundation of our approach.

Euclid's *Elements* had its own set of postulates, from which he proved the basic facts of geometry. We now derive some of these facts from our development of the real numbers.

The motivation for the next definition is the Pythagorean Theorem; however, we cannot yet attempt to prove or even state this theorem yet, because we do not have a notion of angle.

Definition 11.2. We call $\mathbb{R}^n$ *n-dimensional euclidean space*. Let $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{R}^n$. We define the *distance* from $\boldsymbol{x}$ to $\boldsymbol{y}$ as

$$d(\boldsymbol{x}, \boldsymbol{y}) = \sqrt{\sum_{i=1}^n (y_i - x_i)^2}.$$

CHAPTER 12

Integer Theory and Justification for Real Numbers

1. Division Algorithm

We know how to divide integers to get a quotient and a remainder. The method we use to do this is an effective sequence of well-defined steps with no choices. Such an sequence of steps is known as an *algorithm*. Hence the name of the next proposition.

Proposition 12.1. (Division Algorithm for Integers)
Let $m, n \in \mathbb{Z}$ with $m \neq 0$. There exist unique integers $q, r \in \mathbb{Z}$ such that

$$n = qm + r \qquad \text{and} \qquad 0 \leq r < |m|.$$

Proof. Assume m is positive. Let $X = \{z \in \mathbb{Z} \mid z = n - km \text{ for some } k \in \mathbb{Z}\}$. The subset of X consisting of nonnegative integers is a subset of $\mathbb{N}$, and by the Well-Ordering Principle, contains a smallest member, say r. That is, $r = n - qm$ for some $q \in \mathbb{Z}$, so $n = qm + r$. We know $0 \leq r$. Also, $r < m$, for otherwise, $r - m$ is positive, less than r, and in X.

For uniqueness, assume $n = q_1m + r_1$ and $n = q_2m + r_2$, where $q_1, r_1, q_2, r_2 \in \mathbb{Z}$, $0 \leq r_1 < m$, and $0 \leq r_2 < m$. Then $m(q_1 - q_2) = r_1 - r_2$; also $-m < r_1 - r_2 < m$. Since $m \mid (r_1 - r_2)$, we must have $r_1 - r_2 = 0$. Thus $r_1 = r_2$, which forces $q_1 = q_2$. □

Exercise 12.1. Find where the proof above uses the assumption that $m > 0$, and prove the proposition for the case $m < 0$.

In the equation $n = mq + r$, we call n the *dividend*, m the *divisor*, q the *quotient*, and r the *remainder*. A proof of the division algorithm may be based on the method of division itself. The next exercise is similar to writing an essay on how to tie one's shoe; nevertheless, it forces one to consider precisely what needs to be done.

Exercise 12.2. Describe (in general terms) the method by which the quotient q and the remainder r are obtained from the dividend n and the divisor m.

The theory of the integers is dominated by the division algorithm, and in particular, the study of the remainders (as opposed to the quotients). We begin this study with the case where the remainder is zero.

Definition 12.2. Let $m, n \in \mathbb{Z}$. We say that m *divides* n, and write $m \mid n$, if there exists an integer k such that $n = km$. The following phrases are synonymous:

- m divides n;
- m is a *divisor* of n;
- m is a *factor* of n;

- n is a *multiple* of m;
- n is *divisible* by m.

Exercise 12.3. Let $a, b, c \in \mathbb{Z}$ be positive. Show that

(a) $a \mid a$ (Reflexivity);
(b) $a \mid b$ and $b \mid a$ implies $a = b$ (Antisymmetry);
(c) $a \mid b$ and $b \mid c$ implies $a \mid c$ (Transitivity).

Definition 12.3. Let $m, n \in \mathbb{Z}$. A *greatest common divisor* of m and n, denoted $\gcd(m, n)$, is a positive integer d such that

(a) $d \mid m$ and $d \mid n$;
(b) $e \mid m$ and $e \mid n$ implies $e \mid d$.

Exercise 12.4. Let $m, n \in \mathbb{Z}$. Show that there is exactly on positive integer d such that d is a greatest common divisor of m and n, thus justifying the notation $\gcd(m, n)$.

Exercise 12.5. Let $m, n \in \mathbb{Z}$ and let d, e be a positive integers. Show that d is a greatest common divisor of m and n if and only if

(a) $d \mid m$ and $d \mid n$;
(b) $e \mid m$ and $e \mid n$ implies $e < d$.

Exercise 12.6. Let $m, n \in \mathbb{Z}$ such that $m \mid n$. Show that $\gcd(m, n) = |m|$.

Definition 12.4. Let $m, n \in \mathbb{Z}$. A *least common multiple* of m and n, denoted $\operatorname{lcm}(m, n)$, is a positive integer s such that

(a) $m \mid s$ and $n \mid s$;
(b) $m \mid t$ and $n \mid t$ implies $s \mid t$.

Exercise 12.7. Let $m, n \in \mathbb{Z}$. Show that there is exactly one positive integer s such that s is a least common multiple of m and n, thus justifying the notation $\operatorname{lcm}(m, n)$.

Exercise 12.8. Let $m, n \in \mathbb{Z}$ and let s, t be a positive integers. Show that $s = \operatorname{lcm}(m, n)$ if and only if

(a) $m \mid s$ and $n \mid s$;
(b) $m \mid t$ and $n \mid t$ implies $s < t$.

Exercise 12.9. Let $m, n \in \mathbb{Z}$ such that $m \mid n$. Show that $\operatorname{lcm}(m, n) = |n|$.

Exercise 12.10. Let $m, n \in \mathbb{Z}$ be positive. Let $d = \gcd(m, n)$ and $s = \operatorname{lcm}(m, n)$.

(a) Show that $s \mid mn$.
(b) Show that $mn \mid ds$.
(c) Show that $ds \mid mn$.
(d) Conclude that $ds = mn$.

2. Euclidean Algorithm

There is an effective and efficient method to find the greatest common divisor of any two integers, which is known as the *Euclidean algorithm*, since it was originally published in Euclid's *The Elements*. This algorithm can be extended to produce $\gcd(a, b)$ as a linear combination of a and b. First we state and prove the theoretical result, then describe the method.

Proposition 12.5. (Euclidean Algorithm for Integers)
Let $m, n \in \mathbb{Z}$. Then there exists a unique $d \in \mathbb{Z}$ such that $d = \gcd(m, n)$, and there exist integers $x, y \in \mathbb{Z}$ such that

$$d = xm + yn.$$

Proof. Let $X = \{z \in \mathbb{Z} \mid z = xm + yn \text{ for some } x, y \in \mathbb{Z}\}$. Then the subset of X consisting of positive integers contains a smallest member, say d, where $d = xm+yn$ for some $x, y \in \mathbb{Z}$.

Now $m = qd + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$. Then $m = q(xm + yn) + r$, so $r = (1 - qxm)m + (qy)n \in X$. Since $r < d$ and d is the smallest positive integer in X, we have $r = 0$. Thus $d \mid m$. Similarly, $d \mid n$.

If $e \mid m$ and $e \mid n$, then $m = ke$ and $n = le$ for some $k, l \in \mathbb{Z}$. Then $d = xke + yle = (xk + yl)e$. Therefore $e \mid d$. This shows that $d = \gcd(m, n)$.

For uniqueness of a greatest common divisor, suppose that e also satisfies the conditions of a gcd. Then $d \mid e$ and $e \mid d$. Thus $d = ie$ and $e = jd$ for some $i, j \in \mathbb{Z}$. Then $d = ijd$, so $ij = 1$. Since i and j are integers, then $i = \pm 1$. Since d and e are both positive, we must have $i = 1$. Thus $d = e$. □

We say that $m, n \in \mathbb{Z}$ are *relatively prime* if $\gcd(m, n) = 1$. The next exercise provides a converse for the Euclidean algorithm for the case where $d = 1$.

Exercise 12.11. Let $m, n \in \mathbb{Z}$ and suppose that there exist integers $x, y \in \mathbb{Z}$ such that $xm + yn = 1$. Show that $\gcd(m, n) = 1$.

Exercise 12.12. Let $m, n \in \mathbb{N}$ and suppose that $m \mid n$. Show that $\gcd(m, n) = m$.

The procedure to find the greatest common divisor of two integers is based on the following fact.

Proposition 12.6. *Let $m, n \in \mathbb{Z}$, and let $q, r \in \mathbb{Z}$ be the unique integers such that $n = qm + r$ and $0 \leq r < m$. Then $\gcd(n, m) = \gcd(m, r)$.*

Proof. Let $d_1 = \gcd(n, m)$ and $d_2 = \gcd(m, r)$. Since "divides" is a partial order on the positive integers, it suffices to show that $d_1 \mid d_2$ and $d_2 \mid d_1$.

By definition of common divisor, we have integers $w, x, y, z \in \mathbb{Z}$ such that $d_1 w = n$, $d_1 x = m$, $d_2 y = m$, and $d_2 z = r$.

Then $d_1 w = q d_1 x + r$, so $r = d_1(w - qx)$, and $d_1 \mid r$. Also $d_1 \mid m$, so $d_1 \mid d_2$ by definition of gcd.

On the other hand, $n = q d_2 y + d_2 z = d_2(qy + z)$, so $d_2 \mid n$. Also $d_2 \mid m$, so $d_2 \mid d_1$ by definition of gcd. □

Now let $m, n \in \mathbb{Z}$ be arbitrary integers, and write $n = mq+r$, where $0 \leq r < m$. Let $r_0 = n$, $r_1 = m$, $r_2 = r$, and $q_1 = q$. Then the equation becomes $r_0 = r_1 q_1 + r_2$. Repeat the process by writing $m = rq_2+r_3$, which is the same as $r_1 = r_2 q_2+r_3$, with $0 \leq r_3 < r_2$. Continue in this manner, so in the i^{th} stage, we have $r_{i-1} = r_i q_i + r_{i+1}$, with $0 \leq r_{i+1} < r_i$. Since r_i keeps getting smaller, it must eventually reach zero.

Let k be the smallest integer such that $r_{k+1} = 0$. By the above proposition and induction,

$$\gcd(n, m) = \gcd(m, r) = \cdots = \gcd(r_{k-1}, r_k).$$

But $r_{k-1} = r_k q_k + r_{k+1} = r_k q_k$. Thus $r_k \mid r_{k-1}$, so $\gcd(r_{k-1}, r_k) = r_k$. Therefore $\gcd(n, m) = r_k$. This process for finding the gcd is known as the *Euclidean Algorithm*.

In order to find the unique integers x and y such that $xm+yn = \gcd(m,n)$, use the equations derived above and work backward. Start with $r_k = r_{k-2} - r_{k-1}q_{k-1}$. Substitute the previous equation $r_{k-1} = r_{k-3} - r_{k-2}q_{k-2}$ into this one to obtain

$$r_k = r_{k-2} - (r_{k-3} - r_{k-2}q_{k-2})q_{k-1}) = r_{k-2}(q_{k-2}q_{k-1} + 1) - r_{k-3}q_{k-1}.$$

Continuing in this way until you arrive back at the beginning.

For example, let $n = 210$ and $m = 165$. Work forward to find the gcd:

- $210 = 165 \cdot 1 + 45$;
- $165 = 45 \cdot 3 + 30$;
- $45 = 30 \cdot 1 + 15$;
- $30 = 15 \cdot 2 + 0$.

Therefore, $\gcd(210, 165) = 15$. Now work backwards to find the coefficients:

- $15 = 45 - 30 \cdot 1$;
- $15 = 45 - (165 - 45 \cdot 3) = 45 \cdot 4 - 165$;
- $15 = (210 - 165) \cdot 4 - 165 = 210 \cdot 4 - 165 \cdot 5$.

Therefore, $15 = 210 \cdot 4 + 165 \cdot (-5)$.

3. Fundamental Theorem of Arithmetic

The study of the integers is often referred to as number theory, and prime numbers take center stage in this discipline.

Definition 12.7. An integer $p \in \mathbb{Z}$ is called *prime* if

(1) $p \geq 2$;
(2) $p \mid ab$ implies $p \mid a$ or $p \mid b$, where $a, b \in \mathbb{N}$.

Definition 12.8. An integer $p \in \mathbb{Z}$ is called *irreducible* if

(1) $p \geq 2$;
(2) $p = ab$ implies $a = 1$ or $b = 1$, where $a, b \in \mathbb{N}$.

The definition of irreducible given above is often given as the definition of prime. However, standard practice in more general situations uses our definitions, so we show that, in the case of the integers, they are equivalent.

Proposition 12.9. *Let $p \in \mathbb{Z}$. Then p is prime if and only if p is irreducible.*

Proof. We prove both directions of the implication. We may assume that $p \geq 2$.

($\Rightarrow$) Suppose that p is prime, and that $p = ab$ for some $a, b \in \mathbb{N}$. Then $p \mid ab$, so $p \mid a$ or $p \mid b$. Without loss of generality, suppose that $p \mid a$. Then $a = kp$ for some $k \in \mathbb{Z}$. Since a and p are positive, so is k (see Problem 7.2), and k is a natural number. Moreover, $p = ab = kpb = kbp$, so by the cancellation law of multiplication, $kb = 1$. Since k and b are natural numbers, $k = b = 1$ by Proposition 6.48. [RETURN - want PropNaturalUnits as a separate Prop? it seems silly]

($\Leftarrow$) Suppose that p is irreducible, and that $p \mid ab$ for some $a, b \in \mathbb{N}$. Then $ab = kp$ for some $k \in \mathbb{Z}$. Since p is irreducible, either $\gcd(a, p) = 1$ or $\gcd(a, p) = p$. If $\gcd(a, p) = p$, then p divides a, and we are done, so assume that $\gcd(a, p) = 1$. Then there exist $x, y \in \mathbb{Z}$ such that $xa + yp = 1$. Multiply both sides by b to obtain $xab + ypb = b$. Now $b = xkp + ypb = (xk + yb)p$, so p divides b. □

Proof. Suppose n is not prime. Then $n = ab$ for some $a, b \in \mathbb{N}$ with a and b not equal to one. Now a and b cannot be zero since $n \geq 2$; thus $a \geq 2$ and $b \geq 2$. Since $1 < b$, then $a < ab = n$; thus $2 \leq a < n$. □

Problem 12.1. Let $a, p \in \mathbb{Z}$ such that p is prime.
Show that $\gcd(a, p) = 1$ or $\gcd(a, p) = p$.

Lemma 12.10. *Let $p \in \mathbb{Z}$ be prime and let $n_1, \ldots, n_r \in \mathbb{Z}$.*
If p divides $\prod_{i=1}^{r} n_i$, then p divides n_k for some $k \in \mathbb{N}_r^+$. [RETURN - family of elements, indexed by $\mathbb{N}_r^+$?]

Proof. Proceed by induction on r.

For $r = 1$, we are given $p \mid n_1$, so $p \mid n_k$ for some $k \in \{1\}$.

Set $a = \prod_{i=1}^{r-1} n_i$ and $b = n_r$, so that $ab = \prod_{i=1}^{r} n_k$. Assume that if $p \mid a$, then $p \mid n_k$ for some $k \in \mathbb{N}_{r-1}^+$. Suppose $p \mid ab$. Then, by Definition 12.7, either $p \mid a$ or $p \mid b$. If $p \mid b$, then $p \mid n_r$; otherwise, $p \mid a$, so $p \mid n_k$ for some $k \in \mathbb{N}_{r-1}^+$. In either case, $p \mid n_k$ for some $k \in \mathbb{N}_r^+$. □

Lemma 12.11. *Let $n \in \mathbb{Z}$ with $n \geq 2$. Then there exist prime numbers $p_1, \ldots, p_r$ such that $n = \prod_{i=1}^{r} p_i$.*

Proof. Proceed by strong induction on n.

If n is prime, set $r = 1$ and $p_1 = n$ to obtain the conclusion.

The base case is $n = 2$, and since 2 is prime, the base case is satisfied.

Suppose $n > 2$; if n is prime, the conclusion is true, so assume n is not prime. Then there exist $a, b \in \mathbb{Z}$ with $1 < a < n$ and $1 < b < n$ such that $n = ab$. Since a and b are less than n, there exist prime numbers $x_1, \ldots, x_s$ and $y_1, \ldots, y_t$ such that $a = \prod_{j=1}^{s} x_j$ and $b = \prod_{k=1}^{t} y_k$. Let $r = s + t$ and

$$p_i = \begin{cases} x_i & \text{if } 1 \leq i \leq s; \\ y_{(i-s+1)} & \text{if } s+1 \leq i \leq s+t. \end{cases}$$

By associativity of multiplication, the conclusion follows. □

Lemma 12.12. *Let $p_1, \ldots, p_r, q_1, \ldots, q_s$ be prime numbers such that*

$$\prod_{i=1}^{r} p_i = \prod_{i=1}^{s} q_i.$$

Then $r = s$ and there exists a permutation $\sigma \in \mathrm{Sym}(\mathbb{N}_r^+)$ such that $p_i = q_{\sigma(i)}$.

Proof. Let $n = \prod_{i=1}^{r} p_i$, and proceed by induction on r.

If $r = 1$, we have $n = p_1$, which is prime; then it is clear from Proposition 12.9 that $s = 1$ and $p_1 = q_1$.

Assume $r > 1$. Now p_r divides $n = \prod_{i=1}^{s} q_i$, so p_r divides q_k for some k, and since q_k is prime, this implies that $p_r = q_k$. Let α be the permutation of $\mathbb{N}_s^+$ defined by

$$\alpha(i) = \begin{cases} i & \text{if } 1 \leq i \leq k-1; \\ s & \text{if } i = k; \\ i-1 & \text{if } k \leq i \leq s. \end{cases}$$

Now by commutativity of multiplication, [RETURN - generalized assoc after definition of recursive binaries; generalized comm/assoc stated using permutations?]

$$\left(\prod_{i=1}^{r-1} p_i\right) p_r = \prod_{i=1}^{s} q_i = \left(\prod_{i=1}^{s-1} q_{\alpha(i)}\right) q_k,$$

and by the cancellation law of multiplication,

$$\prod_{i=1}^{r-1} p_i = \prod_{i=1}^{s-1} q_{\alpha(i)}.$$

By induction, $r-1 = s-1$, which implies that $r = s$; moreover, there exists a permutation $\gamma \in \mathrm{Sym}(\mathbb{N}^+_{r-1})$ such that $p_i = q_{\gamma(i)}$ for $i \in \mathbb{N}^+_{r-1}$. Define a permutation $\beta \in \mathrm{Sym}(\mathbb{N}^+_r)$ by

$$\beta(i) = \begin{cases} \gamma(i) & \text{if } 1 \le i \le r-1; \\ r & \text{if } i = r. \end{cases}$$

Set $\sigma = \beta \circ \alpha$. Now σ has the desired property. □

Lemma 12.13. *Let $\le$ be a total order on a set A. Let $n \in \mathbb{N}^+$ and let $f : \mathbb{N}^+_n \to A$ be a function. Then there exists a bijective function $g : \mathbb{N}^+_n \to \mathbb{N}^+_n$ such that if $h = f \circ g$, then $i \le j$ implies $h(i) \le h(j)$. [RETURN - relabel, or put into previous chapter; state fund thm using ordered primes to nail down uniqueness]*

Proof. Proceed by induction on n.

If $n = 1$, the conclusion is satisfied by letting $g = \mathrm{id}_{\mathbb{N}^+_1}$.

Assume $n > 1$. Now $\mathbb{N}^+_{n-1} \subset \mathbb{N}^+_n$; let $f' = f \restriction_{\mathbb{N}^+_{n-1}}$. By induction, there exists a bijective function $g' : \mathbb{N}^+_{n-1} \to \mathbb{N}^+_{n-1}$ such that if $h' = f' \circ g'$, then $i \le j$ implies $h'(i) \le h'(j)$. Let $B = \{k \in \mathbb{N}^+_{n-1} \mid f(n) \le h'(k)\}$. If B is empty, let $m = n$; otherwise, let $m = \min B$. Define a function $g : \mathbb{N}^+_n \to \mathbb{N}^+_n$ by

$$g(k) = \begin{cases} g'(k) & \text{if } k < m; \\ n & \text{if } k = m; \\ g'(k-1) & \text{if } k > m. \end{cases}$$

Define $h : \mathbb{N}^+_n \to A$ by $h = f \circ g$; then h is given by

$$h(k) = \begin{cases} h'(k) & \text{if } k < m; \\ f(n) & \text{if } k = m; \\ h'(k-1) & \text{if } k > m. \end{cases}$$

Now g and h have the desired properties. □

Theorem 12.14. (Fundamental Theorem of Arithmetic)
Let $n \in \mathbb{Z}$ with $n \ge 2$. Then there exist prime number $p_1, \ldots, p_r$, unique up to order, such that $n = \prod_{i=1}^r p_i$.

4. From Rationals

Proposition 12.15. *Let $x \in \mathbb{Q}$. Then there exist unique $a, b \in \mathbb{Q}$ with $\gcd(a,b) = 1$ and $b > 0$ such that $x = \frac{a}{b}$.*

Proof. Let $A = \{b \in \mathbb{Z} \mid b > 0 \text{ and } x = [a,b]\}$. Then A has a minimum element, which we call b, and there exists $a \in \mathbb{Z}$ such that $x = \frac{a}{b}$. We have $b > 0$; let $d = \gcd a, b$. There exist integers u, v such that $a = ud$ and $b = vd$, and we see that $[a,b] = [u,v]$. If $d > 1$, then $vd > d$, which contradicts that b is the minimum element of A. Thus $d = 1$.

To see that a and b are unique, suppose that $[a,b] = [u,v]$ for some $u, v \in \mathbb{Z}$ with $\gcd(u,v) = 1$ and $v > 0$. Then $av = bu$, and since $\gcd(a,b) = 1$, we must have

$a \mid u$ and $b \mid v$ [RETURN]. Thus $u = ca$ and $v = db$ for some $c, d \in \mathbb{Z}$. Substituting this into $av = bu$, we see that $abd = abc$, so by cancellation, $c = d$. Then d divides both u and v, so $c = d = 1$. Thus $a = u$ and $b = v$. □

5. Denouement

The rational numbers appear to be the culmination of our attempt to find an adequate system of numbers in which to do arithmetic; we can add them, subtract them, multiply them, and almost always divide them. Solving equations like $x^2 - 2 = 0$ in the rationals, however, is a different story.

Proposition 12.16. *Let $p \in \mathbb{Z}$ be prime. There does not exist a rational number $x \in \mathbb{Q}$ such that $xx = 2$.*

Proof. For $x \in \mathbb{Q}$, let $x^2 = xx$. Suppose, by way of contradiction, that there exists a rational number $x \in \mathbb{Q}$ such that $x^2 = 2$. By Proposition 12.15, there exist unique $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and $b > 0$ such that $x = \frac{a}{b}$. Now

$$\begin{aligned}
\left(\frac{a}{b}\right)^2 = 2 &\Rightarrow \frac{a^2}{b^2} = 2 \\
&\Rightarrow a^2 = 2b^2 \\
&\Rightarrow 2 \mid a^2 \\
&\Rightarrow 2 \mid a && \text{because 2 is prime} \\
&\Rightarrow 4 \mid a^2 \\
&\Rightarrow a^2 = 4k && \text{for some } k \in \mathbb{Z} \\
&\Rightarrow 4k = 2b^2 \\
&\Rightarrow 2k = b^2 \\
&\Rightarrow 2 \mid b^2 \\
&\Rightarrow 2 \mid b && \text{because 2 is prime.}
\end{aligned}$$

Thus $2 \mid a$ and $2 \mid b$, which contradicts that $\gcd(a, b) = 1$. □

The Pythagorean Theorem [RETURN] provides *geometric* motivation for solving the equation $x^2 - 2 = 0$. For suppose that we walk one mile north, then one mile west. How far do we need to walk in a straight line to return to our place of origin? That would be $\sqrt{2}$, if such a number existed. This number is a legitimate *distance*; so to geometrically model a line, we need to include it in the model.

We can arrange the rational numbers on a line, but the line apparently has holes in it where no rational number exists. The motivation for our construction of the reals is to locate these holes by cutting the rational number line into two pieces; when we cut, we will either cut at a rational number, or we will find a hole.

6. Positive Rational Subsets

Definition 12.17. Let $X \subset \mathbb{Q}$. Then *positive part* of A is

$$X^+ = \{x \in X \mid x > 0\}.$$

Definition 12.18. Let $X, Y \subset \mathbb{Q}^+$.

The *sum* of A and B is

$$X + Y = \{z \in \mathbb{Q}^+ \mid z = x + y \text{ for some } x \in X, y \in Y\}.$$

The *product* of A and B is

$$XY = \{z \in \mathbb{Q}^+ \mid x = xy \text{ for some } x \in X, y \in Y\}.$$

Proposition 12.19. *Let $X, Y, Z \subset \mathbb{Q}^+$. Then*

(a) $X + Y = Y + X$;
(b) $(X + Y) + Z = X + (Y + Z)$;
(c) $XY = YX$;
(d) $(XY)Z = X(YZ)$;
(e) $(X + Y)Z \subset XZ + YZ$.

Definition 12.20. Let $X \subset \mathbb{Q}^+$. We say that X is a *Dedekind precut* if

(a) $X \neq \mathbb{Q}^+$;
(b) $x \in X$ and $u \in \mathbb{Q}^+ \setminus X$ implies $x < u$;
(c) X does not contain a maximum element.

****

APPENDIX A

Logic Notation Summary

Symbol	Abbrev	Name	Format
$\neg$	NOT	Negation	$\neg p$
$\wedge$	AND	Conjunction	$p \wedge q$
$\vee$	OR	Disjunction	$p \vee q$
$\Rightarrow$	IMP	Implication	$p \Rightarrow q$
$\Leftrightarrow$	IFF	Equivalence	$p \Leftrightarrow q$
$\updownarrow$	XOR	Exclusion	$p \updownarrow q$
$\uparrow$	NOR	Alternate Denial	$p \uparrow q$
$\downarrow$	NAND	Joint Denial	$p \downarrow q$

TABLE 1. Logical Operators

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$	$p \updownarrow q$	$p \uparrow q$	$p \downarrow q$
T	**T**	**F**	**T**	**T**	**T**	**T**	**F**	**F**	**F**
T	**F**	**F**	**F**	**T**	**F**	**F**	**T**	**F**	**T**
F	**T**	**T**	**F**	**T**	**T**	**F**	**T**	**F**	**T**
F	**F**	**T**	**F**	**F**	**T**	**T**	**F**	**T**	**T**

TABLE 2. Truth Tables

Precedence of Operators

(1) NOT
(2) AND, OR
(3) XOR, NOR, NAND
(4) IMP
(5) IFF

Symbol	Abbrev	Meaning
$\forall$	FORALL	for every (for all)
$\exists$	EXISTS	there exists (for some)
$\exists!$	UNIQUE	there exists uniquely
$\ni$	ST	such that

TABLE 3. Quantifiers

APPENDIX B

Set Notation Summary

Symbol	Meaning	Definition
$\in$	is an element of	Example: $\pi \in \mathbb{R}$
$\notin$	is not an element of	Example: $\pi \notin \mathbb{Q}$
$\subset$	is a subset of	$A \subset B \Leftrightarrow (a \in A \Rightarrow a \in B)$
$\subsetneq$	is a proper subset of	$A \subsetneq B \Leftrightarrow (A \subset B$ and $A \neq B)$
$\cup$	union	$A \cup B = \{x \mid x \in A$ or $x \in B$
$\cap$	intersection	$A \cap B = \{x \mid x \in A$ and $x \in B\}$
$\setminus$	complement	$A \setminus B = \{x \mid x \in A$ and $x \notin B\}$
$\triangle$	symmetric difference	$A \triangle B = (A \cup B) \setminus (A \cap B)$
$\times$	cartesian product	$A \times B = \{(a, b) \mid a \in A$ and $b \in B\}$

TABLE 1. Set Operations

Set	Name	Definition
$\mathbb{N}$	Natural Numbers	$\{1, 2, 3, \dots\}$
$\mathbb{Z}$	Integers	$\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Q}$	Rational Numbers	$\{p/q \mid p, q \in \mathbb{Z}\}$
$\mathbb{R}$	Real Numbers	{"Dedekind Cuts"}
$\mathbb{C}$	Complex Numbers	$\{a + ib \mid a, b \in \mathbb{R}$ and $i^2 = -1\}$
$\mathbb{R}^2$	Euclidean Plane	$\{(a, b) \mid a, b \in \mathbb{R}\}$
$\mathbb{R}^3$	Euclidean Space	$\{(a, b, c) \mid a, b, c \in \mathbb{R}\}$

TABLE 2. Standard Sets

APPENDIX C

Greek Letters

Name	Uppercase	Lowercase	Uppervar	Lowervar
alpha		α		
beta		β		
gamma	Γ	γ	$\varGamma$	
delta	Δ	δ	$\varDelta$	
epsilon		ϵ		ε
zeta		ζ		
eta		η		
theta	Θ	θ	$\varTheta$	ϑ
iota		ι		
kappa		κ		$\varkappa$
lambda	Λ	λ	$\varLambda$	
mu		μ		
nu		ν		
xi	Ξ	ξ	$\varXi$	
pi	Π	π	$\varPi$	ϖ
rho		ρ		ϱ
sigma	Σ	σ	$\varSigma$	ς
tau		τ		
upsilon	Υ	υ	$\varUpsilon$	
phi	Φ	ϕ	$\varPhi$	φ
chi		χ		
psi	Ψ	ψ	$\varPsi$	
omega	Ω	ω	$\varOmega$	

Bibliography

[De69] Dedekind, Richard, *Essays on the Theory of Numbers*, Dover (1969)

[Ga98] Gaughan, Edward D., *Introduction to Analysis*,Brooks/Cole Publishing (1998)

[Ha60] Halmos, Paul R., *Naive Set Theory*, Undergraduate Texts in Mathematics, Springer-Verlag (1960,1974)

[KF70] Kolmogorev and Fomin, *Introductory Real Analysis*, Dover (1975)

[La66] Landau, Edmund, *Foundations of Analysis*, Chelsea Publishing Company (1966)

[Me87] Mendelson, Elliott, *Introduction to Mathematical Logic*, 3^{rd} edition, Wadsworth Inc. (1987)

[Mu75] Munkres, James R., *Topology: A First Course*, Prentice-Hall Inc. (1975)

[Ro80] Ross, Kenneth A., *Elementary Analysis: The Theory of Calculus*, Undergraduate Texts in Mathematics, Springer Verlag (1980)

[SS72] Saxena and Shah, *Introduction to Real Variable Theory*, International Textbook Company (1972)

[St87] Stewart,James, *Calculus*, 2^{nd} edition, Brooks/Cole Publishing Company (1987,1991)