Basic Set Theory

Paul L. Bailey

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

Contents

Preface v

Chapter I. Symbolic Logic 1
1. Propositions 1
2. Logical Operators 1
3. Tautologies and Contradictions 6
4. Generation of Operators 8
5. Exercises 11

Chapter II. Sets 13
1. Sets and Elements 13
2. Subsets and Quantifiers 14
3. Set Operations 15
4. Cartesian Product 17
5. Numbers 18
6. Exercises 20

Chapter III. Functions 21
1. Functions 21
2. Images and Preimages 23
3. Composition of Functions 25
4. Restrictions and Bijections 26
5. Exercises 27

Chapter IV. Collections 29
1. Collections of Sets 29
2. Collections of Functions 29
3. Power Sets 31
4. Partitions 32
5. Exercises 33

Chapter V. Relations 35
1. Relations 35
2. Partial Orders and Total Orders 36
3. Equivalence Relations 37
4. Equivalence Classes 38
5. Partitions induced by Equivalence Relations 39
6. Partitions induced by Functions 40
7. Functions defined on Partitions 41
8. Canonical Functions 42
9. Exercises 43

Chapter VI. Binary Operators 45
1. Binary Operators 45
2. Closure 46
3. Standard Notation 46
4. Properties of Binary Operators 47
5. Exercises 49

Chapter VII. Cardinality 51
1. Cardinality 51
2. Finite Sets 53
3. Levels of Infinity 53
4. Exercises 53

Chapter VIII. Natural Numbers 55
1. Natural Numbers 55
2. Induction 55
3. Recursion 57

Chapter IX. Integers 59
1. Motivation 59
2. Definition 60
3. Addition 61
4. Multiplication 62
5. Algebraic Properties 63
6. Embedding 65
7. Order 66
8. Exercises 67

Chapter X. Modular Integers 69
1. Well-Ordering Principle 69
2. Division Algorithm 70
3. Euclidean Algorithm 71
4. Prime Integers 72
5. Congruence Modulo n 73
6. Integers Modulo n 74
7. The Group of Integers Modulo n 75
8. Order of an Element in $\mathbb{Z}_n$ 76
9. The Ring of Integers Modulo n 77
10. Algebraic Equations in $\mathbb{Z}_n$ 78

Appendix A. Logic Notation Summary 79

Appendix B. Set Notation Summary 81

Appendix C. ZFC Axioms 83

Bibliography 85

Preface

This document is a introduction to the initial concepts of set, elements, functions, and relations. The ideas contained herein can be put on a solid foundation using an axiomatic approach to set theory. For the time being, we eschew this technical development in the interest of more rapidly attaining the important ideas behind functions and relations.

Our goal is to build enough tools to briefly define the set natural numbers, to thoroughly develop the integers from the natural numbers, to define modulo arithmetic, and to construct the rational numbers from the integers.

CHAPTER I

Symbolic Logic

1. Propositions

A *proposition* is a statement which is either true or false, although we may not know which. Propositions are denoted by lowercase letters such as p, q or r. The truth or falsity of the proposition is called its *truth value*, and the two possible truth values are labeled **T** for TRUE and **F** for FALSE. The truth value of the proposition p is denoted $\mathbf{V}(p)$.

For example, the statement "The sun rises in the east" is a proposition, and if we wish to label this statement p, we write

$$p = \text{“The sun rises in the east”}.$$

Similarly, we may write

$$q = \text{“The sun rises in the west”}.$$

In this case, $\mathbf{V}(p) = \mathbf{T}$ and $\mathbf{V}(q) = \mathbf{F}$.

2. Logical Operators

Propositions may be modified and combined by the use of *logical operators*, which take one or more propositions and create a new one which has its own truth value. The resultant truth value is uniquely determined by the proposition(s) operated upon and the operator(s) used. Operators which accept one input are called *unary* operators, and operators which accept two inputs are called *binary* operators.

The behavior of each logical operator is determined by a *truth table*. The truth table lists all possible combinations of the truth values of the inputs, and states the operator's output for each combination of inputs.

The simplest useful logical operator is the *negation* operator NOT ($\neg$), which operates on a single proposition and reverses its truth value. Thus

$$\neg(\text{“Pigs are mammals”}) = \text{“Pigs are not mammals”}.$$

The action that NOT has on the truth value of a proposition is defined by its truth table, which lists the possible truth values of a proposition p side by side with the truth value of $\neg p$:

p	$\neg p$
T	**F**
F	**T**

TABLE 1. NOT Truth Table

Assertion I.1. If p is any proposition, then

$$\mathbf{V}(\neg(\neg p)) = \mathbf{V}(p)$$

.

Proof. If p is TRUE, then $\neg p$ is FALSE, and so $\neg(\neg p)$ is TRUE. If p is FALSE, then $\neg p$ is TRUE, and so $\neg(\neg p))$ is FALSE. □

The next logical operator we consider is the *conjunction* operator AND ($\wedge$). The proposition $p \wedge q$ is true only when both p and q are true propositions. For example, if $p =$ "Pigs are mammals" and $q =$ "Pigs fly", then $p \wedge q$ may be interpreted as "Pigs are flying mammals". The AND operator is defined by a truth table which lists all possible combinations of the truth values of p and q:

p	q	$p \wedge q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**F**

TABLE 2. AND Truth Table

The *disjunction* operator OR ($\vee$) returns a value of TRUE whenever either proposition it operates upon is true, and therefore is defined by:

p	q	$p \vee q$
T	**T**	**T**
T	**F**	**T**
F	**T**	**T**
F	**F**	**F**

TABLE 3. OR Truth Table

Thus if let p and q be as above and we assume that pigs are mammals who cannot fly, we have $\mathbf{V}(p) = \mathbf{T}$, $\mathbf{V}(q) = \mathbf{F}$, $\mathbf{V}(p \wedge q) = \mathbf{F}$ and $\mathbf{V}(p \vee q) = \mathbf{T}$.

At this point we adopt the convention that the NOT operator takes "binds tighter" than any other operator, that is, it takes precedence in the order of operations and applies only to the object on its immediate right. Thus $\neg p \wedge q$ means $(\neg p) \wedge q$ as opposed to $\neg(p \wedge q)$. We are now ready for our first theorem.

Theorem I.2. *(DeMorgan's Laws) For any two propositions p and q we have*

(1) $\mathbf{V}(\neg(p \vee q)) = \mathbf{V}(\neg p \wedge \neg q)$;
(2) $\mathbf{V}(\neg(p \wedge q)) = \mathbf{V}(\neg p \vee \neg q)$.

Proof. The proofs of these assertions are truth tables in which each step is expanded, and the columns corresponding to either side of the equalities above are compared.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	**T**	**T**	**F**	**F**	**F**	**F**
T	**F**	**T**	**F**	**F**	**T**	**F**
F	**T**	**T**	**F**	**T**	**F**	**F**
F	**F**	**F**	**T**	**T**	**T**	**T**

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	**T**	**T**	**F**	**F**	**F**	**F**
T	**F**	**F**	**T**	**F**	**T**	**T**
F	**T**	**F**	**T**	**T**	**F**	**T**
F	**F**	**F**	**T**	**T**	**T**	**T**

□

If propositions are linked together to form new propositions via logical operators, the result may be called a *composite* proposition. Propositions which are not presented as composites are known as *atomic* propositions, or *atoms.* It is critical to realize that the propositional calculus we are developing cannot tell us anything about the truth or falsity of atoms. However, if we know the truth value of atoms prior to applying the propositional calculus to some composite of them, it will tell us the truth value of that composite.

The proof of DeMorgan's Laws points out that even complicated composites have corresponding truth tables which relate the possible truth values of potentially unknown propositions to the truth value of the composite. In particular, suppose we do not know the truth values of p and q, and we let $r = \neg(p \wedge q)$ and $s = \neg p \vee \neg q$. Then $\mathbf{V}(r) = \mathbf{V}(s)$ regardless of the meaning of p and q.

Corollary I.3. *The disjunction operator OR may be defined in terms of the negation operator NOT and the conjunction operator AND as*

$$\mathbf{V}(a \vee b) = \mathbf{V}(\neg(\neg a \wedge \neg b)).$$

Proof. Apply Assertion I.1 to DeMorgan's First Law (take the NOT of both sides). □

We may think of the NOT operator as distributing into the AND operator, but when it does so it changes AND to OR. An analogous statement applies to the OR operator. However, we do have a actual distributivity of AND over OR and of OR over AND.

Theorem I.4. *(Distributive Laws) For any two propositions p and q we have*

(1) $\mathbf{V}((p \vee q) \wedge r) = \mathbf{V}((p \wedge r) \vee (q \wedge r))$;
(2) $\mathbf{V}((p \wedge q) \vee r) = \mathbf{V}((p \vee r) \wedge (q \vee r))$.

Proof. The tables tell the story.

p	q	r	$p \vee q$	$(p \vee q) \wedge r$	$p \wedge r$	$q \wedge r$	$(p \wedge r) \vee (q \wedge r)$
T	**T**	**T**	**T**	**T**	**T**	**T**	**T**
T	**T**	**F**	**T**	**F**	**F**	**F**	**F**
T	**F**	**T**	**T**	**T**	**T**	**F**	**T**
T	**F**	**F**	**T**	**F**	**F**	**F**	**F**
F	**T**	**T**	**T**	**T**	**F**	**T**	**T**
F	**T**	**F**	**T**	**F**	**F**	**F**	**F**
F	**F**	**T**	**F**	**F**	**F**	**F**	**F**
F	**F**	**F**	**F**	**F**	**F**	**F**	**F**

p	q	r	$p \wedge q$	$(p \wedge q) \vee r$	$p \vee r$	$q \vee r$	$(p \vee r) \wedge (q \vee r)$
T	**T**	**T**	**T**	**T**	**T**	**T**	**T**
T	**T**	**F**	**T**	**T**	**T**	**T**	**T**
T	**F**	**T**	**F**	**T**	**T**	**T**	**T**
T	**F**	**F**	**F**	**F**	**T**	**F**	**F**
F	**T**	**T**	**F**	**T**	**T**	**T**	**T**
F	**T**	**F**	**F**	**F**	**F**	**T**	**F**
F	**F**	**T**	**F**	**T**	**T**	**T**	**T**
F	**F**	**F**	**F**	**F**	**F**	**F**	**F**

□

Intuitively we realize that AND and OR are *commutative* operators, which is to say that $p \wedge q$ means the same thing as $q \wedge p$ and $p \vee q$ is just another way of saying $q \vee p$. Thus we are content when we notice that our truth tables agree. It is also easily verified that AND and OR are *associative* operators, and we leave it to the reader to verify this.

Assertion I.5. (Commutativity Laws) For any two propositions p and q we have

(1) $\mathbf{V}(p \wedge q) = \mathbf{V}(q \wedge p)$;
(2) $\mathbf{V}(p \vee q) = \mathbf{V}(q \vee p)$.

Assertion I.6. (Associativity Laws) For any propositions p, q, and r we have

(1) $\mathbf{V}((p \wedge q) \wedge r) = \mathbf{V}(p \wedge (q \wedge r))$;
(2) $\mathbf{V}((p \vee q) \vee r) = \mathbf{V}(p \vee (q \vee r))$.

Commutativity and associativity do not hold for all of the commonly used logical operators. This brings us to the *implication* operator IMP ($\Rightarrow$), where we read $p \Rightarrow q$ as "p implies q" or as "if p, then q". We have a name for the components of an implication: p is called the *hypothesis* and q is called the *conclusion*. One may be surprised by the truth table of this logical operator the first time it is encountered:

p	q	$p \Rightarrow q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**T**
F	**F**	**T**

Table 4. IMP Truth Table

A false proposition implies anything one wishes it to imply. Thus the proposition "If pigs fly, then the earth if flat" is true whether or not the earth is indeed flat. Just to get our feet wet with the implication operator, we assert the following, which may be verified directly from the truth tables.

Assertion I.7. If p and q are propositions, then

(1) $p \Rightarrow (p \vee q)$;
(2) $(p \wedge q) \Rightarrow p$.

Theorem I.8. *The implication operator IMP may be built from the negation operator NOT and the conjunction operator AND operators since*

$$\mathbf{V}(p \Rightarrow q) = \mathbf{V}(\neg(p \wedge \neg q)).$$

At this point you may be asking why we chose for $p \Rightarrow q$ to be true even when p and q are both false. The others choices in the truth table for implication are easily justified by common sense, but why this one? The answer lies in the truth table for the equivalence operator and the theorem which follows it, a theorem which we very much want to be true and which depends on this choice.

The *equivalence* operator IFF ($\Leftrightarrow$) signifies logical equivalence, so that $p \Leftrightarrow q$ is read "p is logically equivalent to q" or "p if and only if q". This is the operator that answers the question "do p and q have the same truth value?"

p	q	$p \Leftrightarrow q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**T**

Table 5. IFF Truth Table

The following theorem justifies our double sided arrow notation.

Theorem I.9. *If p and q are propositions, then*

$$\mathbf{V}((p \Rightarrow q) \wedge (p \Rightarrow q)) = \mathbf{V}(p \Leftrightarrow q).$$

Proof. We have a proof by truth table.

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$	$p \Leftrightarrow q$
T	**T**	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**F**	**F**
F	**T**	**T**	**F**	**F**	**F**
F	**F**	**T**	**T**	**T**	**T**

□

Theorem I.10. *The equivalence operator IFF may be constructed from the negation operator NOT and the conjunction operator AND because*

$$\mathbf{V}(\neg(p \wedge \neg q) \wedge \neg(\neg p \wedge q)) = \mathbf{V}(p \Leftrightarrow q).$$

At this point we may abandon our $\mathbf{V}(p)$ notation in preference to usage of the IFF operator, for it is clear that for any two propositions p and q, then $\mathbf{V}(p) = \mathbf{V}(q)$ is the logical equivalent of $p \Leftrightarrow q$. For example, the above claim could be written

$$\mathbf{V}((\neg(p \wedge \neg q) \wedge \neg(\neg p \wedge q)) \Leftrightarrow (p \Leftrightarrow q)) = \mathbf{T},$$

or simply

$$(\neg(p \wedge \neg q) \wedge \neg(\neg p \wedge q)) \Leftrightarrow (p \Leftrightarrow q),$$

since asserting the above is taken to mean asserting that it is true.

3. Tautologies and Contradictions

In general, we need to know the truth value of the atomic components of a composite proposition in order to determine the truth value of the composite. However, this is not always the case. If a given proposition is always true regardless of the truth values of its atomic components, it is called a *tautology*. On the other hand, if a proposition is always false it is called a *contradiction*. Tautologies and contradictions are called *independent* of the truth values of the component atoms. A proposition which is neither a tautology nor a contradiction is called a *dependent*, or *indeterminate* proposition.

Examples of tautologies:

(1) $p \vee \neg p$
(2) $\neg(p \wedge \neg p)$
(3) $p \Leftrightarrow \neg(\neg p)$
(4) $\neg(p \vee q) \Rightarrow (p \Rightarrow q)$
(5) Demorgan's Laws
(6) Distributive Laws

Any two tautologies may be combined via the AND operator to form another tautology. Indeed, the tautology

$$(p \vee \neg p) \wedge \neg(p \wedge \neg p),$$

which states that either p is true or $\neg p$ is true, but not both, is often considered the basis of Western logic. Notice that the "but not both" part may be derived from the $p \vee \neg p$ part by an application of DeMorgan's Law.

Examples of contradictions:

(1) $p \wedge \neg p$
(2) $p \Rightarrow \neg p$
(3) $(p \Leftrightarrow (p \wedge q)) \wedge (p \Rightarrow q)$

Similarly, any two contradictions may be combined via the OR operator to form another contradiction (they may also be combined via the AND operator to form another contradiction, but this is a weaker statement).

Examples of indeterminate propositions:

(1) $(p \Rightarrow q) \Leftrightarrow (p \wedge q)$
(2) $(p \vee \neg q) \Rightarrow (p \vee \neg p)$
(3) $p \Rightarrow q$

In a certain sense, mathematics is the process of discovering tautologies. However, the superstructure of most theorems is of the indeterminate form $p \Rightarrow q$. Why, then, is it difficult to prove theorems? It may seem that one simply needs to determine the truth values of p and q and verify the truth or falsity of the theorem with a glance at the truth table for implication. This is far from the case; an implication is a description of the relationship between p and q, and not of their individual truth values. In fact, proving an implication involves verifying that all four rows of the truth table for implication are satisfied (although such proofs rarely take this explicit form).

Now we turn to a pair of constructions which are critically important for aspiring mathematicians to grasp. Suppose that p and q are propositions, and consider the implication $p \Rightarrow q$. The *converse* of this implication is the proposition $q \Rightarrow p$, whereas its *contrapositive* is the proposition $\neg q \Rightarrow \neg p$.

Assertion I.11. The contrapositive of an implication is logically equivalent to it. The converse of an implication is logically independent of it.

Proof. To explore the logical relations between any two propositions a and b, we construct the truth table of $a \Leftrightarrow b$. If this truth table contains nothing but **T**'s in the last column, then a and b are logically equivalent. If this truth table contains nothing but **F**'s in the last column, then a and b are logically incompatible. If this truth table contains some **T**'s and some **F**'s in its last column, then a and b are logically independent. We leave it as an exercise to determine what a and b should be in these cases and to complete the proof. □

An example is in order. Let p be the proposition “The egg falls fifty feet onto cement” and q be the proposition “The egg breaks”. Additionally, we assume that when an egg falls fifty feet onto cement, then it breaks, so that we are assuming that $p \Rightarrow q$ is true. Now it is clear that if the egg is not broken, it could not have fallen fifty feet onto cement. This is nothing more than the claim $\neg q \Rightarrow \neg p$. On the other hand, it is possible to break an egg without dropping it fifty feet onto cement; just because it is broken, we may not accurately conclude that it did drop fifty feet onto cement. So the converse $q \Rightarrow p$ is not necessarily true.

It is intuitively clear that the converse of an implication is not logically equivalent to the implication, and yet when immersed in the abstract world of mathematics, surrounded by definitions and related ideas which have not previously been contemplated, the distinction between an implication and its converse may seem to blur. Thus it is a good idea to keep in mind “the converse is not necessarily true” (even when the implication is).

On the other hand, many proofs depend on the contrapositive. It is often easier to prove that $\neg q \Rightarrow \neg p$ than $p \Rightarrow q$; but if we can prove that $\neg q \Rightarrow \neg p$, we get $p \Rightarrow q$ for free.

A related idea is that of proof by contradiction. Here we wish to prove some proposition a, where a may or may not be in the form of an implication. The roundabout method of proof by contradiction assumes that $\neg a$ is true, and arrives at a conclusion which is a proposition known to always be false, in other words, a contradiction. Thus the assumption that led to the contradiction $(\neg a)$ must be false, proving that a is true. This technique is invaluable in group theory and topology.

Often one finds proofs that masquerade as proofs by contradiction but are actually proofs by contrapositive. That is, one wishes to prove that $p \Rightarrow q$, and so assumes that $p \wedge \neg q$ is true, and arrives at a contradiction, without ever using the assumption p. This is not the preferred method.

4. Generation of Operators

In this section we introduce primitive logical operators which do not arise in ordinary language but which, nonetheless, arise from definitional truth tables which differ from those we have already encountered. These are XOR, NOR, and NAND.

The *exclusion* operator XOR ($\between$) stands for exclusive OR and means a or b, but not both.

a	b	$a \between b$
T	**T**	**F**
T	**F**	**T**
F	**T**	**T**
F	**F**	**F**

Table 6. XOR Truth Table

Assertion I.12. The XOR operator is the negation of IFF, i.e.,

$$(a \between b) \Leftrightarrow \neg(a \Leftrightarrow b).$$

The *alternate denial* operator NOR ($\uparrow$) means “neither a nor b”.

a	b	$a \uparrow b$
T	**T**	**F**
T	**F**	**F**
F	**T**	**F**
F	**F**	**T**

Table 7. NOR Truth Table

Assertion I.13. The NOR operator is the negation of OR, i.e.,

$$(a \uparrow b) \Leftrightarrow \neg(a \vee b).$$

The *joint denial* operator NAND ($\downarrow$) means “possibly a and possibly b, but not both”.

a	b	$a \downarrow b$
T	**T**	**F**
T	**F**	**T**
F	**T**	**T**
F	**F**	**T**

Table 8. NAND Truth Table

Assertion I.14. The NAND operator is the negation of AND, i.e.,

$$(a \downarrow b) \Leftrightarrow \neg(a \wedge b).$$

A collection of operators *generates* another operator if the truth table of generated operator can be derived through a combination of the generators. For example, we have already seen that NOT and AND together generate OR, IMP, and IFF. Since XOR is NOT IFF, NOR is NOT OR, and NAND is NOT AND, we can see that NOT and AND generate XOR, NOR, and NAND.

Theorem I.15. *The operators NOT, AND, OR, IMP, IFF, XOR, and NAND may be derived from NOR.*

Proof. It suffices to show that NOT and AND may be written in terms of NOR. The definition of NOR and DeMorgan’s Law gives us that

(1) $\neg a \Leftrightarrow (a \uparrow a)$;
(2) $(a \wedge b) \Leftrightarrow (\neg a \uparrow \neg b)$.

$\square$

Theorem I.16. *The operators NOT, AND, OR, IMP, IFF, XOR, and NOR may be derived from NAND.*

Proof. It suffices to show that NOT and AND may be written in terms of NAND. The definition of NAND and a glance at the truth tables gives us that

(1) $\neg a \Leftrightarrow (a \downarrow a)$
(2) $(a \wedge b) \Leftrightarrow \neg(a \downarrow b)$

□

There are four possible logical operators of a single proposition, and we have only discussed the identity operator ($\mathbf{V}$) and NOT. There are also the constant operators whose value is always $\mathbf{T}$ or $\mathbf{F}$. Notice that a constant operator cannot be generated from NOT because NOT NOT is the identity, NOT NOT NOT is NOT, etc. We use this fact in our final theorem.

Theorem I.17. *The operators NOR and NAND are the only binary operators which are sufficient by themselves to generate NOT, AND, OR, IMP, IFF, XOR, NOR, and NAND.*

Proof. In order for a generic binary operator GEN ($\pitchfork$) to generate NOT, $a \pitchfork b$ must be false when both a and b are true, for otherwise we can never achieve anything but true in the first row of a truth table of a composite proposition whose only operator is GEN. Similarly, $a \pitchfork b$ must be true whenever both a and b are false. Thus we have a partial truth table for GEN.

p	q	$p \pitchfork q$
$\mathbf{T}$	$\mathbf{T}$	$\mathbf{F}$
$\mathbf{T}$	$\mathbf{F}$	$\mathbf{V}_1$
$\mathbf{F}$	$\mathbf{T}$	$\mathbf{V}_2$
$\mathbf{F}$	$\mathbf{F}$	$\mathbf{T}$

Now suppose that GEN is not a commutative operator. If $\mathbf{V}_1 = \mathbf{T}$ and $\mathbf{V}_2 = \mathbf{F}$, then $(p \pitchfork q) \Leftrightarrow \neg(q)$ is a tautology, and if $\mathbf{V}_1 = \mathbf{F}$ and $\mathbf{V}_2 = \mathbf{T}$, then $(p \pitchfork q) \Leftrightarrow \neg(p)$ is a tautology. In either case, GEN may be constructed from NOT. However, NOT cannot generate a constant operator of a single atom such as $p \wedge \neg p$, which is always false, and thus NOT cannot generate AND.

Thus for GEN to generate the other logical operators, it must be commutative so that $\mathbf{V}_1 = \mathbf{V}_2 = \mathbf{V}$. If $\mathbf{V} = \mathbf{T}$, then GEN is NAND, and if $\mathbf{V} = \mathbf{F}$, then GEN is NOR. □

There are sixteen possible truth tables resulting from combinations of two propositions, and we have only mentioned seven of them. The reader is welcomed to explore the possibilities inherent in the others.

5. Exercises

Exercise I.1. Determine the truth table of the following composite propositions and state whether they are tautologies, contradictions, or indeterminate.

(a) $(p \vee q) \Rightarrow (p \wedge q)$
(b) $(p \wedge q) \vee (p \Rightarrow q)$
(c) $(p \Rightarrow q) \Rightarrow p$
(d) $p \Rightarrow (q \Rightarrow p)$
(e) $(p \Rightarrow q) \Rightarrow q$
(f) $p \Rightarrow (q \Rightarrow p)$
(g) $(p \Rightarrow q) \Rightarrow r$
(h) $p \Rightarrow (q \Rightarrow r)$
(i) $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
(j) $(p \wedge q) \Leftrightarrow (p \between q)$
(k) $(p \downarrow q) \Rightarrow (p \vee q)$

Exercise I.2. Complete the proof of Assertion I.11.

Exercise I.3. Write a logically equivalent statement using NOT, AND, and OR.

(a) $\neg(p \Rightarrow q)$
(b) $(p \Rightarrow q) \Rightarrow r$

Exercise I.4. Use truth tables to prove the following assertions.

(a) $(a \between b) \Leftrightarrow \neg(a \Leftrightarrow b)$
(b) $(a \uparrow b) \Leftrightarrow \neg(a \vee b)$
(c) $(a \downarrow b) \Leftrightarrow \neg(a \wedge b)$

Exercise I.5. Show that the logical operators NOT and OR are sufficient to generate AND, IMP, IFF, XOR, NOR, and NAND.

Exercise I.6. Develop the truth tables for logical operators of one proposition other than NOT. You should get three of these, and you will see that they may reasonably be called identity, constant truth, and constant falsehood.

Exercise I.7. Develop the truth tables for logical operators of two propositions other than AND, OR, IMP, IFF, XOR, NOR, and NAND. You should get nine of these. Give these new operators names. Relate them to the operators of one proposition identity, constant truth, constant falsehood, and negation. Relate them to the operators of two propositions AND, OR, IMP, IFF, XOR, NOR, and NAND.

CHAPTER II

Sets

1. Sets and Elements

Intuitively, a *set* is a collection of *elements*. We should not think of a set as a "container", but rather as the elements themselves. We assume that we can distinguish between different elements, and that we can determine whether or not a given element is in a given set.

The relationship of two elements a and b being the same is *equality* and is denoted $a = b$. The negation of this relation is denoted $a \neq b$, that is, $a \neq b \Leftrightarrow \neg(a = b)$.

The relationship of an element a being a member of a set A *containment* and is denoted $a \in A$. The negation of this relation is denoted $b \notin A$, that is, $b \notin A \Leftrightarrow \neg(b \in A)$.

A set is determined by the elements it contains. That is, two sets are considered equal if and only if they contain the same elements:

$$A = B \Leftrightarrow (a \in A \Leftrightarrow a \in B).$$

One way of describing a set is by explicitly listing its members. Such lists are surrounded by braces, e.g., the set of the first five prime integers is $\{2, 3, 5, 7, 11\}$. If the pattern is clear, we may use dots; for example, to label the set of all prime numbers as P, we may write $P = \{2, 3, 5, 7, 11, 13, \dots\}$. Thus $2 \in P$ and $23 \in P$, but $1 \notin P$ and $21 \notin P$. As another example, if we denote the set of all integers by $\mathbb{Z}$, we may write $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. Note that the order of elements in a list is irrelevant in determining a set, for example, $\{5, 3, 7, 11, 2\} = \{2, 3, 5, 7, 11\}$. Also, there is no such thing as the "multiplicity" of an element in a set, for example $\{1, 3, 2, 2, 1\} = \{1, 2, 3\}$.

2. Subsets and Quantifiers

If A and B are sets and all of the elements in A are also contained in B, we say that A is a *subset* of B or that A is *included* in B and write $A \subset B$:

$$A \subset B \Leftrightarrow (a \in A \Rightarrow a \in B).$$

For example, $\{1, 3, 5\} \subset \{1, 2, 3, 4, 5\}$. Note that any set is a subset of itself. We say that A is a *proper subset* of B is $A \subset B$ but $A \neq B$.

It follows immediately from the definition of subset that

$$A = B \Leftrightarrow (A \subset B \wedge B \subset A).$$

Thus to show that two sets are equal, it suffices to show that each is contained in the other.

A set containing no elements is called the *empty set* and is denoted $\varnothing$. Since a set is determined by its elements, there is only one empty set. Note that the empty set is a subset of any set.

We may construct new sets as subsets of existing sets by specifying properties. Specifically, we may have a proposition $p(x)$ which is true for some elements x in a set X and not true for others. Then we may construct the set

$$\{x \in X \mid p(x) \text{ is true}\};$$

this is read "the set of x in X such that $p(x)$". The construction of this set is called *specification.* For example, if we let $\mathbb{Z}$ be the set of integers, the set P of all prime numbers could be specified as $P = \{n \in \mathbb{Z} \mid n \text{ is prime}\}$.

Quantifiers help determine the domain of a proposition which varies upon input. For our purposes, we may think of quantifiers as abbreviations for phrases. Thus we use the following notation.

$\forall$	for every
$\exists$	there exists
$\exists!$	there exists uniquely
$\vdash$	such that

For example, let $p(x)$ be the proposition "x is prime". Then

$$\forall x \in \mathbb{Z}, p(x),$$

read "for all $x \in \mathbb{Z}$, x is prime" is false, but

$$\exists x \in \mathbb{Z} \vdash p(x),$$

read "there exists $x \in \mathbb{Z}$ such that x is prime" is true. The symbol $\forall$ is called the *universal quantifier*, and the symbol $\exists$ is called the *existential quantifier.*

3. Set Operations

Let A and B be subsets of some "universal set" U and define the following set operations:

$$\begin{aligned} \text{Intersection:} \quad & A \cap B = \{x \in U \mid x \in A \wedge x \in B\} \\ \text{Union:} \quad & A \cup B = \{x \in U \mid x \in A \vee x \in B\} \\ \text{Complement:} \quad & A \smallsetminus B = \{x \in U \mid x \in A \wedge x \notin B\} \end{aligned}$$

The pictures which correspond to these operations are called *Venn diagrams.*

Example II.1. Let $A = \{1, 3, 5, 7, 9\}$, $B = \{1, 2, 3, 4, 5\}$. Then $A \cap B = \{1, 3, 5\}$, $A \cup B = \{1, 2, 3, 4, 5, 7, 9\}$, $A \smallsetminus B = \{7, 9\}$, and $B \smallsetminus A = \{2, 4\}$. □

Example II.2. 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. □

If $A \cap B = \varnothing$, we say that A and B are *disjoint.*

Example II.3. 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. □

The following properties are sometimes useful in proofs:

- $A = A \cup A = A \cap A$
- $\varnothing \cap A = \varnothing$
- $\varnothing \cup A = A$
- $A \subset B \Leftrightarrow A \cap B = A$
- $A \subset B \Leftrightarrow A \cup B = B$

As an example, we prove one of these properties.

Proposition II.4. *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, $a \in B$. □

Now let us prove the analogous statement in compressed form.

Proposition II.5. *Let A and B be a sets. Then $A \subset B \Leftrightarrow A \cup B = B$.*

Proof.

($\Rightarrow$) 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 $a \in A \cup B$, so $a \in B$. Thus $A \subset B$. □

The following properties state that union and intersection are commutative and associative operations, and that they distribute over each other. These properties are intuitively clear via Venn diagrams, and can be proved rigorously from the definitions of intersection and union with the help of truth tables.

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

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.

The following properties of complement are known as *DeMorgan's Laws*. You should draw Venn diagrams of these situations to convince yourself that these properties are true (however, these diagrams should not be considered as proofs).

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

Here are a few more properties of complement:

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

4. Cartesian Product

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

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

This is the technical definition; think about how it relates to the intuitive approach below.

Intuitively, if a and b are elements, the *ordered pair* with first coordinate a and second coordinate b is something like a set containing a and b, but in such a way that the order matters. We denote this ordered pair by (a, b) and declare that it has the following "defining property":

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

The *cartesian product* of the sets A and B is denoted $A \times B$ and is defined to be the set of all ordered pairs whose first coordinate is in A and whose second coordinate is in B:

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

Example II.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. □

In general, if A contains m elements and B contains n elements, where m and n are natural numbers, then $A \times B$ contains mn elements.

Similarly, we have *ordered triples* (a, b, c), with a "defining property"

$$(a, b, c) = (d, e, f) \Leftrightarrow (a = d) \wedge (b = e) \wedge (c = f).$$

The we declare the cartesian product of three sets to be

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

By slight of hand which we will not discuss at this point, one may show that it is possible to "identify" the order pair $((a, b), c)$ with the ordered pair $(a, (b, c))$, so that $(A \times B) \times C$ is identified with $A \times (B \times C)$, and that both of these are "identified" with $A \times B \times C$. This forces a kind of associativity on the operation of cartesian product.

We continue with *ordered n-tuples* and the cartesian product of n sets, for any natural number n. If A is a set, the cartesian product of A with itself n times is denoted A^n. For example, $A^2 = A \times A$ and $A^3 = A \times A \times A$. The entries of an ordered n-tuple in such a cartesian product are called *coordinates.*

We have the following properties:

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

As an example, we prove one of these properties.

Proposition II.7. *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 $(x, y) \in (A \times B) \cap (C \times D)$. □

5. Numbers

Later, we will formally develop some of the standard number systems. For the time being, we use these familiar sets only in examples. Since they are useful for intuition into general set constructions, at this time we specify the standard names for the common sets of numbers.

The following sets of numbers are standard:

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

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

The following standard notation gives subsets of the real numbers, called *intervals*:

- $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ (closed)
- $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$ (open)
- $[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$
- $(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$
- $(-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$ (closed)
- $(-\infty, b) = \{x \in \mathbb{R} \mid x < b\}$ (open)
- $[a, \infty) = \{x \in \mathbb{R} \mid a \leq x\}$ (closed)
- $(a, \infty) = \{x \in \mathbb{R} \mid a < x\}$ (open)

Example II.8. 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. □

The first three of our standard sets of numbers, $\mathbb{N}$, $\mathbb{Z}$, 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 are the *geometric completion* of the rational numbers, constructed from the rational numbers by filling in the gaps. For example, the sequence

$$\{1, 1.4, 1.41, 1.414, 1.4142, 1.41421, 1414213, \dots\}$$

consists of rational numbers but converges to $\sqrt{2}$, which is not a rational number. The rational number line has "holes" where the irrational numbers belong, and for this reason it does not model the synthetic notion of a line as well as the real numbers.

We think of a point as zero-dimensional space. A set which represents zero-dimensional space is $\{0\}$. A line is one-dimensional space, and is represented by $\mathbb{R}$. A plane is two-dimensional space, and is represented by $\mathbb{R}^2$, the set of all ordered pairs of real numbers. Three-dimensional space is represented by $\mathbb{R}^3$, the set of all ordered triples of real numbers.

The complex numbers are the *algebraic closure* of the real numbers, and were developed from the real numbers so that all polynomials may be factored.

Example II.9. 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. □

Warning II.1. 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.

6. Exercises

Exercise II.1. 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 II.2. In each case, draw a Venn diagram representing the situation:
(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 II.3. Let A and B be subsets of a set U. The *symmetric difference* of A and B, denoted $A \triangle B$, is the set of points in U which are in either A or B but not in both.
(a) Draw a Venn diagram describing $A \triangle B$.
(b) Find two set expressions which could be used to define $A \triangle B$, and justify your answer.
(c) Choose one of your expressions above as a formal definition, and use it to prove that symmetric difference is commutative and associative. Your proof here may use the fact that intersection and union are commutative and associative without proving these facts.

In the next two exercises, you should read "show that" to mean "give a formal proof that".

Exercise II.4. Let A, B, and C sets. Show that

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

Exercise II.5. Let A, B, and C be sets. Show that

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

CHAPTER III

Functions

1. Functions

Let A and B be sets. A *function* from A to B is a subset $f \subset A \times B$ of the cartesian product of A with B such that for every $a \in A$ there exists a unique $b \in B$ such $(a, b) \in f$. This is the technical definition; think about how it relates to the intuitive approach below.

Intuitively, a *function* from a set A to a set B is an assignment of every element in A to some element in B. Another way of describing this is that we think of a function as a kind of vehicle, something which sends each element of A to an element of B. If we think of elements are the nouns of set theory and sets as the adjectives (an element has a property if it is in the set of things with that property), then we may think of functions as the verbs.

There are many familiar examples of functions from the set of real numbers into itself, for example, sin, cos, log, and so forth. It is essential in mathematics, and extremely useful as a way of thinking in general, to expand our view of functions so that they can send elements from any set to any other set.

Let f be a function from A to B. If $a \in A$, the element of B to which a is assigned by f is denoted $f(a)$; in other words, the place in B to which a is sent by f is denoted $f(a)$. We declare that a function must satisfy the following "defining property":

$$\forall a \in A \exists! b \in B \vdash f(a) = b.$$

In words, for every element a in A there exists a *unique* element b in B such that a is sent to b by f.

If f is a function from A to B, this fact is denoted

$$f : A \to B.$$

We say that f *maps* A *into* B, and that f is a function *on* A. For this reason, functions are sometimes called *maps* or *mappings*. If $f(a) = b$, we say that a is *mapped to* b by f. We may indicate this by writing $a \mapsto b$.

Two functions $f : A \to B$ and $g : A \to B$ are considered *equal* if they act the same way on every element of A:

$$f = g \Leftrightarrow (a \in A \Rightarrow f(a) = g(a)).$$

Thus to show that two functions f and g are equal, select an arbitrary element $a \in A$ and show that $f(a) = g(a)$.

If A is sufficiently small, we may explicitly describe the function by listing the elements of A and where they go; for example, if $A = \{1, 2, 3\}$ and $B = \mathbb{R}$, a perfectly good function is described by $\{1 \mapsto 23.432, 2 \mapsto \pi, 3 \mapsto \sqrt{593}\}$.

However, if A is large, the functions 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.

Example III.1. Let $\mathbb{R}$ be the set of real numbers. The following are all functions from $\mathbb{R}$ into $\mathbb{R}$:

- $f(x) = 0$;
- $f(x) = x$;
- $f(x) = x^3 + 3x + 17$;
- $f(x) = \sin(x)$;
- $f(x) = \exp(x)$.

The following are functions from the set of positive real numbers into $\mathbb{R}$:

- $f(x) = \sqrt{x}$;
- $f(x) = \log(x)$.

Note that $\tan(x)$ is not a function from $\mathbb{R}$ into $\mathbb{R}$, because it is not defined at (for example) the point $\frac{\pi}{2} \in \mathbb{R}$. $\square$

Some functions are constructed from existing functions by specifying cases.

Example III.2. Let $\mathbb{R}$ be the set of real numbers. Define $f : \mathbb{R} \to \mathbb{R}$ by

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

The reader familiar with calculus may ask himself whether or not the first, second, and third derivatives exist and are continuous for this function. $\square$

Example III.3. Let X be a set and let $A \subset X$. The *characteristic function* of A in X is a function $\chi_A : X \to \{0, 1\}$ defined by

$$\chi_A(x) = \begin{cases} 0 \text{ if } x \notin A; \\ 1 \text{ if } x \in A. \end{cases}$$

In particular, let $X = [0, 1] \subset \mathbb{R}$ be the closed unit interval and let $A = \mathbb{Q} \cap X$ be the set of rational numbers in this interval. Think about the graph of the function χ_A. $\square$

Example III.4. Suppose we designed a computer system that records information on patients in a hospital. Each patient is assigned a number upon admission, which is just the next available number, starting with zero. We create a program which allows the user to type a working diagnosis of 60 characters or less for this patient, and file this information under the patient number. We only allow the user to type capital letters, spaces, commas, and periods in this diagnosis. The file may be viewed as a function

$$\text{DIAG(patient number)} = \text{“patient diagnosis”};$$

here, $\text{DIAG} : \mathbb{N} \to B$, where B is the set of all possible strings of allowed characters with length less than or equal to 60 which can be typed on a computer keyboard. The size of B is 29^{60} (why?). $\square$

2. Images and Preimages

If $f : A \to B$, the set A is called the *domain* of the function and the set B is called the *codomain.* We often think of a function as taking the domain A and placing it in the codomain B. However, when it does so, we must realize that more than one element of A can be sent to a given element in B, and that there may be some elements in B to which no elements of A are sent.

If $C \subset A$, we define the *image* of C under f to be the set

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

The image of the domain is called the *range* of the function.

A function $f : A \to B$ is called *surjective* (or *onto*) if

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

Equivalently, f is surjective if $f[A] = B$.

If $D \subset B$, we define the *preimage* of D under f to be the set

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

If D is a singleton set, that is if $D = \{b\}$ for some $b \in B$, we may write $f^{-1}[b]$ instead of $f^{-1}[\{b\}]$.

A function $f : A \to B$ is called *injective* (or *one-to-one*) if

$$\forall a, b \in A, f(a) = f(b) \Rightarrow a = b.$$

Equivalently, f is injective if for all $b \in B$, $f^{-1}[b]$ contains at most one element in A.

A function $f : A \to B$ is called *bijective* if it is both injective and surjective. Such a function sets up a *correspondence* between the elements of A and the elements of B.

Example III.5. First we consider "real-valued functions of a real variable". This simply means that the domain and the codomain of the function is $\mathbb{R}$.

- $f(x) = x^3$ 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:

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

Example III.6. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = \sin x$. The set $A = \{\frac{k\pi}{3} \mid k \in \mathbb{Z}\}$ is the set of multiples of $\frac{\pi}{3}$. The image of this set under f is

$$f[A] = \{0, \frac{\sqrt{3}}{2}, -\frac{\sqrt{3}}{2}\}.$$

Let $B = \{0, \frac{1}{2}\}$. The preimage of this set under f is

$$f^{-1}[B] = \{k\pi \pm \frac{\pi}{6} \mid k \in \mathbb{Z}\}.$$

This function is not surjective, because there are points in $\mathbb{R}$ which are not the sine of any angle, and it is not injective, since more than one point is mapped to a given point in the range. □

Example III.7. Let $\mathbb{N}$ be the set of natural numbers and let $\mathbb{Z}$ be the set of integers. The function $f : \mathbb{Z} \to \mathbb{Z}$ given by $n \mapsto 2n$ is injective but not surjective.

The function $g : \mathbb{Z} \to \mathbb{N}$ given by $n \mapsto \sqrt{n^2}$ is surjective but not injective. The preimage of $5 \in \mathbb{N}$ under g is $\{-5, 5\}$.

The function $h : \mathbb{Z} \to \mathbb{Z}$ given by $n \mapsto -n$ is bijective. □

Example III.8. Let A be the set of all animals in a zoo and let B be the set of all species of animals on earth. Then we obtain a function $f : A \to B$ by defining $f(a) = b$, where the species of animal a is b. This function is surjective only if this is an unbelievably excellent (and large) zoo, for this would mean it has at least one animal of every species on earth. It is injective only if every animal is very lonely, for this would mean that the zoo contains at most one animal of a given species.

However, a function which assigns to every animal on Noah's Ark its species would be surjective but not injective, since he had two of every kind. Such a function is sometimes called "two-to-one". □

Example III.9. If DIAG is a function which assigns to a patient his diagnosis, then DIAG is injective unless two patients have the same diagnosis. It is not surjective unless we have admitted at least 29^{60} patients. □

The *graph* of a function $f : A \to B$ is defined to be

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

Example III.10. Let $\mathbb{R}$ denote the set of real numbers. Recall that $\mathbb{R}^n$ is the set of ordered n-tuples of real numbers. This set may be called *n-dimensional space.* Thus $\mathbb{R}^2$ is a plane and $\mathbb{R}^3$ is three-dimensional space. We consider functions defined on multidimensional space. Note that we identify $\mathbb{R}^m \times \mathbb{R}^n$ with $\mathbb{R}^{m+n}$. Thus the graph of a function $f : \mathbb{R}^m \to \mathbb{R}^n$ is

$$\{(x_1, \ldots, x_m, y_1, \ldots, y_n) \mid f(x_1, \ldots, x_m) = (y_1, \ldots, y_n)\}.$$

For example, the graph of a differentiable function $f : \mathbb{R} \to \mathbb{R}$ is a curve in $\mathbb{R}^2$ and the graph of a differentiable function $f : \mathbb{R}^2 \to \mathbb{R}$ is a surface in $\mathbb{R}^3$. □

3. Composition of Functions

Let A, B, and C be sets and let $f : A \to B$ and $g : B \to C$. The *composition* of f and g is the function

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

given by

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

The domain of $g \circ f$ is A and the codomain is C. The range of $g \circ f$ is the image under g of the image under f of the domain of f.

Example III.11. Let A be the set of living things on earth, B the set of species, and C be the set of positive real numbers. Let $f : A \to B$ assign each living thing to its species, and let $g : B \to C$ assign each species to its average mass. Then $g \circ f$ guesses the mass of a living thing. □

If f and g are injective, then $g \circ f$ is injective. If f and g are surjective, then $g \circ f$ is surjective. For example, we prove the first of these statements.

Proposition III.12. *Let A, B and C be sets and let $f : A \to B$ and $g : B \to C$ be injective functions. Then $g \circ f$ 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. □

Example III.13. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^2$ and let $g : \mathbb{R} \to \mathbb{R}$ be given by $g(x) = \sin x$. Then $g \circ f : \mathbb{R} \to \mathbb{R}$ is given by $g \circ f(x) = \sin x^2$ and $f \circ g : \mathbb{R} \to \mathbb{R}$ is given by $f \circ g(x) = \sin^2 x$. □

This example demonstrates that composition of functions is not a commutative operation. However, the next proposition tells us that composition of functions is associative.

Proposition III.14. *Let A, B, C, and D be sets and let $f : A \to B$, $g : B \to C$, and $h : C \to D$ be functions. Then $h \circ (g \circ f) = (h \circ g) \circ f$.*

Proof. To show that two functions are equal, it suffices to show that they act the same way on an arbitrary element of the domain.

Let $a \in A$. Then

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

□

4. Restrictions and Bijections

Let $f : X \to Y$ be a function and let $Z = f(X)$ be the range of f. The same function f can be viewed as a function $f : X \to Z$. It is standard in this case to call the function, viewed in this way, by the same name. Note that the function $f : X \to Z$ is surjective. Thus any function is a surjective function onto its range.

Let $f : X \to Y$ be a function and let $A \subset X$ be a subset of the domain of f. The *restriction* of f to A is a function

$$f \restriction_A : A \to Y \text{ given by } f \restriction_A (a) = f(a).$$

Thus given any function and any subset of the domain, there is a function which coincides with the original one, but whose domain is the subset. For example, the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ can certainly be viewed as a function on the integers, sending each integer to its square.

Notice that restriction of a function to a subset of the domain does not necessarily effect the range. For example, if $f : \mathbb{R} \to \mathbb{R}$ is the sine function $f(x) = \sin x$, then the range of $f \restriction_{[0,2\pi]}$ is the same as the range of f on the entire real line.

However, if the original function is injective, then so is any restriction of it.

Let A be any set. The *identity function* on A if the function $\mathrm{id}_A : A \to A$ given by $\mathrm{id}_A(a) = a$ for every $a \in A$. Thus the identity function on A is that function which does nothing to A.

Let $f : A \to B$ be a function. 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 III.15. *Let $f : A \to B$ be a function. Then f is invertible if and only if f is bijective.*

Proof.

($\Rightarrow$) 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 to 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 $\mathrm{id}_A(a_1) = \mathrm{id}_A(a_2)$. But this implies that $a_1 = a_2$, so that f is injective.

($\Leftarrow$) Suppose that f is bijective. We wish to show that f is invertible. Let $b \in B$. Since f is surjective, there exists $a \in A$ such that $f(a) = b$. Since f is injective, a is unique with this property. Define $g(b) = a$. Since b was arbitrary, this defines a function $g : B \to A$.

Now $f(g(b)) = f(a) = b$, so $f \circ g = \mathrm{id}_B$. Also $g(f(a)) = g(b) = a$, so $g \circ f = \mathrm{id}_A$. This completes the proof. □

Let X be a set. A *permutation* of X is a bijective function $\phi : X \to X$. The set of permutations of X is called the *symmetric group* on X and is denoted $\mathrm{Sym}(X)$:

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

5. Exercises

Exercise III.1. Let P be the set of people who ever lived. Which of the following are functions 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 III.2. 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 III.3. Let $\mathbb{N}$ be the set of natural numbers. Let A be a subset of $\mathbb{N}$ given by $[50, 70] \cap \mathbb{N}$, where $[50, 70]$ is the closed unit interval of real numbers between 50 and 70.

Define a function $f : \mathbb{N} \to \mathbb{N}$ by $f(n) = 3n$. Note that A is in both the domain and the codomain 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 III.4. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^3 - 6x^2 + 11x - 3$. Find $f^{-1}[\{3\}]$.

Exercise III.5. 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 III.6. 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?

Exercise III.7. Let $f : X \to Y$ be a function and let $A, B \subset X$.
(a) Show that $f[A \cup B] = f[A] \cup f[B]$.
(b) Show that $f[A \cap B] \subset f[A] \cap f[B]$.
(c) Give an example where $f[A \cap B] \neq f[A] \cap f[B]$.

Exercise III.8. Let $f : X \to Y$ be a function and let $C, D \subset Y$.
(a) Show that $f^{-1}[C \cup D] = f^{-1}[C] \cup f[D]$.
(b) Show that $f^{-1}[C \cap D] = f^{-1}[C] \cap f[D]$.

Exercise III.9. Let $f : X \to Y$ and $g : Y \to Z$ be surjective functions. Show that $g \circ f$ is surjective.

Exercise III.10. 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) Give an example where $g \circ f$ is injective but g is not.

(c) Show that if g is injective and $g \circ f$ is surjective, the f is surjective.
(d) Give an example where $g \circ f$ is surjective, but f is not.

Exercise III.11. Let $f : X \to Y$ be a function.
(a) Show that f is surjective if and only if there exists $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$.
(b) Show that f is injective if and only if there exists $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$.

Exercise III.12. Let X be a set and let $\phi, \psi \in \mathrm{Sym}(X)$. Show that $\phi \circ \psi \in \mathrm{Sym}(X)$.

Exercise III.13. Let X be a set containing n elements. Try to count the number of functions in $\mathrm{Sym}(X)$.

CHAPTER IV

Collections

1. Collections of Sets

We do not disallow the possibility that a set may be an element of another set. In fact, this idea is very useful. For example, we may talk about the set of lines in a plane, even though each line is a set of points in the plane. The set of lines is a set of subsets of the points in the plane. It is common to call sets whose elements are subsets of a given set a *collection* of subsets.

Let X be a set and let $\mathcal{C}$ be a collection of subsets of X. Then the *intersection* and *union* of the sets in the collection are defined by

- $\cap\mathcal{C} = \{x \in X \mid x \in C \text{ for all } C \in \mathcal{C}\}$;
- $\cup\mathcal{C} = \{x \in X \mid x \in C \text{ for some } C \in \mathcal{C}\}$.

Thus $\cap\mathcal{C}$ is the intersection of all the sets in $\mathcal{C}$ and $\cup\mathcal{C}$ is their union.

Example IV.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;
- $\cup\mathcal{C} = \{2, 3, 4, 5, 7, 9, 11, 13, 15, 16, 17, 19, 21, 23\}$.

□

Example IV.2. Let $A = \{n \in \mathbb{N} \mid n < 1000\}$. For each $d \leq \mathbb{N}$, define

$$D_d = \{n \in A \mid n = dm \text{ for some } m \in \mathbb{N}\}.$$

Let $\mathcal{D} = \{D_p \mid p \text{ is prime and } p \leq 7\}$. Find $\cap\mathcal{D}$.

Solution. The set D_d is the set of positive multiples of d which are less then 1000. The set $\mathcal{D}$ is the collection of all D_p such that p is a prime which is less than 7. Thus $\mathcal{D} = \{D_2, D_3, D_5, D_7\}$. Then $\cap\mathcal{D}$, being the intersection of these sets, is the set of natural numbers less than 1000 which are multiples of 2, 3, 5, and 7. Such a number must be a multiple of 210. Also, any multiple of 210 which is less than 1000 is in all four sets. Thus $\cap\mathcal{D} = \{210, 420, 630, 840\}$. □

2. Collections of Functions

We may also consider sets whose members are functions.

Example IV.3. Let X be a set and let $\mathrm{Sym}(X)$ be the set of all bijective functions on X. Then $\mathrm{Sym}(X)$ is a collection of functions. □

If A and B are sets, we may speak of the set of all functions from A to B. We shall denote this set by $\mathcal{F}(A, B)$:

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

Example IV.4. 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:

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

□

Example IV.5. Let $\mathcal{F} = \mathcal{F}(\mathbb{R}, \mathbb{R})$ denote the set of all real valued functions of a real variable:

$$\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}\}.$$

Let $\mathcal{D}$ denote the set of all differentiable functions in $\mathcal{F}$:

$$\mathcal{D} = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is differentiable}\}.$$

Note that $\mathcal{D} \subset \mathcal{F}$.

The differentiation operator is a function

$$\frac{d}{dx} : \mathcal{D} \to \mathcal{F}.$$

Not every function is the derivative of a function, so $\frac{d}{dx}$ is not surjective. Since two functions which differ by a constant have the same derivative, $\frac{d}{dx}$ is not injective. □

3. Power Sets

Let X be a set. The *power set* of X is denoted $\mathcal{P}(X)$ and is defined to be the set of all subsets of X:

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

Here are a few examples:

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

and so forth. Here are some properties:

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

Let X be any set and let $T = \{0, 1\}$. 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 1 is thought of as "ON" or "TRUE" and the element 0 is thought of as "OFF" or "FALSE". Specifically, given $f : X \to T$, define A to the preimage of 1:

$$A = \{a \in A \mid f(a) = 1\};$$

that is, $A = f^{-1}[\{1\}]$.

On the other hand, given a subset of X, we can construct a function

$$\chi_A : X \to T$$

by defining

$$\chi_A(x) = \begin{cases} 0 & \text{if } x \notin A; \\ 1 & \text{if } x \in a. \end{cases}$$

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 $\mathcal{F}(X, T)$.

4. Partitions

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 the sets in $\mathcal{C}$ are *mutually disjoint* if $\cap\mathcal{C} = \varnothing$. If for every two distinct sets $C, D \in \mathcal{C}$, we have $C \cap D = \varnothing$, we say that the members of $\mathcal{C}$ are *pairwise disjoint*. If the sets of a collection are pairwise disjoint, then they are mutually disjoint, but the converse of this is not necessarily true.

Example IV.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. □

A *partition* of X is a collection of pairwise disjoint nonempty subsets of X which covers X. The members of a partition are called *blocks*.

Suppose that $\mathcal{C}$ is a partition of X. If $x \in X$, then there is a unique $A \in \mathcal{C}$ such that $x \in A$; x is certainly in one of them, because X is covered by the members of $\mathcal{C}$; x is in no more than one, for otherwise the ones containing x would overlap and not be disjoint. Put another way, every $x \in X$ is in exactly one of the members of $\mathcal{C}$.

Example IV.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 IV.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:

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

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. □

5. Exercises

Exercise IV.1. Design a collection $\mathcal{C}$ of subsets of $\mathbb{N}$ which has all of the following properties:

(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 that we have given the name "partition" to collections of sets satisfying the first two properties.

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

Exercise IV.4. 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 $\mathcal{P}(A) \cup \mathcal{P}(B) \subset \mathcal{P}(A \cup B)$.
(c) Find an example such that $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$.

Exercise IV.5. Let X be a set. Find an injective function $\phi : X \to \mathcal{P}(X)$.

Exercise IV.6. Let X be as set. Show that there does not exist a surjective function $\phi : X \to \mathcal{P}(X)$.
(Hint: select an arbitrary function $\phi : X \to \mathcal{P}(X)$, and construct a set in $\mathcal{P}(X)$ which is not in the image of ϕ.)

Exercise IV.7. Let X be a set. Define a function $\phi : \mathcal{P}(X) \to \mathcal{P}(X)$ by $A \mapsto X \smallsetminus A$. Show that ϕ is bijective.

Exercise IV.8. Let X be a set and let $T = \{0, 1\}$. Show that there is a correspondence between the sets $\mathcal{P}(X)$ and $\mathcal{F}(X, T)$.

Exercise IV.9. Let X be a set containing n elements. Try to count the size of the set $\mathcal{P}(X)$.

Exercise IV.10. 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 IV.11. 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 $\mathfrak{P}$.

CHAPTER V

Relations

1. Relations

Let A be a set. A *relation* R on A is a subset of the cartesian product of A with itself: $R \subset A \times A$. If $(a, b) \in R$, we say that a is related to b, and may write aRb.

For example, suppose that A is the set of all inhabitants of some island. Let U be the subset of $A \times A$ given by

$$(a, b) \in U \Leftrightarrow a \text{ is the uncle of } b.$$

Let N be the subset of $A \times A$ given by

$$(a, b) \in N \Leftrightarrow a \text{ is the niece of } b.$$

Note that aNb does not imply bUa, nor does aUb imply aNb. However, if we had $S \subset A \times A$ given by

$$(a, b) \in T \Leftrightarrow a \text{ is the sibling of } b,$$

then $aSb \Leftrightarrow bSa$.

Let $R \subset A \times A$ be a relation. We say that R is:

- *reflexive* if aRa for all $a \in A$;
- *symmetric* if $aRb \Leftrightarrow bRa$;
- *antisymmetric* if $aRb \wedge bRa \Rightarrow a = b$;
- *transitive* if $aRb \wedge bRc \Rightarrow aRc$;
- *definite* if $aRb \vee bRa$ for all $a, b \in A$.

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.

2. Partial Orders and Total Orders

A *partial order* on a set A is a relation, usually denoted by $\leq$ instead of by a letter like R, which is reflexive, antisymmetric, and transitive. That is:

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

A partial order relation is called a *total order* relation if it is definite:

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

Example V.1. Let X be a set and let $A = \mathcal{P}(X)$ be the set of all subsets of X. Then inclusion ($\subset$) is a partial order relation on $\mathcal{P}(X)$. However, this is not a total order relation. For example, if $X = \{1, 2, 3, 4, 5\}$, then the sets $\{1, 3, 5\}$ and $\{1, 2, 3\}$ are not related by inclusion. □

Example V.2. 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 V.3. Let $X = \mathbb{Z} \times \mathbb{Z}$, and let $\leq$ be the standard total order on $\mathbb{Z}$. Define a relation R on X by

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

Show that R is a partial order.

Solution. We wish to show that R 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 $(a, b)R(a, b)$, and R is reflexive.

(Antisymmetry) Let $(a, b), (c, d) \in X$ such that $(a, b)R(c, d)$ and $(c, d)R(a, b)$. 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 $(a, b)R(c, d)$ and $(c, d)R(e, f)$. 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). □

3. Equivalence Relations

Let A be a set and consider the relation

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

Then E is simply the relation of equality. The set E is sometimes called the *diagonal* of $A \times A$. This is because if we graph E (say that $A = \mathbb{R}$), we obtain the diagonal line which is the graph of the equation $y = x$. Notice that the relation of equality is reflexive, symmetric, and transitive.

Let A be a set and let $\equiv$ be a relation on A. We say that $\equiv$ is an *equivalence relation* if it is reflexive, symmetric, and transitive:

- $a \equiv a$ (reflexivity);
- $a \equiv b$ if and only if $b \equiv a$ (symmetry);
- if $a \equiv b$ and $b \equiv c$, then $a \equiv c$ (transitivity).

Example V.4. Let A be the set of all animals in the world. Define a relation R by

$$R = \{(a, b) \in A \times A \mid a \text{ and } b \text{ are of the same species } \}.$$

Note that we could have written this

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

Then R 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). □

Example V.5. Let $X = \mathbb{N} \times \mathbb{N}$. Define a relation on X by

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

This is an equivalence relation. □

Example V.6. Let $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ be the set of nonzero integers. Let $X = \mathbb{Z} \times \mathbb{Z}^*$. Define a relation on X by

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

Show that this is an equivalence relation.

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

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

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

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

so $\equiv$ is symmetric.

(Transitivity) Let $(a, b), (c, d), (e, f) \in X$. Suppose that $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$. 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 cancelation, we have $ae = bf$. Thus $(a, b) \equiv (e, f)$, and $\equiv$ is transitive. □

4. Equivalence Classes

Relations of this type are particularly important, 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.

Let $\equiv$ be an equivalence relation on a set A. We say that two element $a, b \in A$ are *equivalent* if $a \equiv b$. Since $\equiv$ is symmetric, this is the case if and only if $b \equiv a$. The *equivalence class* of a, denoted $[a]$, is the set of all elements of A which are equivalent to a:

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

Example V.7. Suppose A is the set of all animals in the world, and $\equiv$ is the relation of being in the same species. Let p be a pig. Then $[p]$ is the set of all pigs in the world. One can see that if q is also a pig, then $[p] = [q]$. Also it is clear that if a is an anteater, then $[p] \cap [a] = \varnothing$. Note there is exactly one equivalence class $[x]$ for each species of animal on earth such that x is an animal of that species. We now proceed to formalize these assertions. □

Proposition V.8. *Let A be a set and let $\equiv$ be an equivalence relation on A. Then the following conditions are equivalent:*

(1) $a \equiv b$*;*
(2) $[a] = [b]$*;*
(3) $b \in [a]$.

Proof. To prove a statement of this kind, we need to show that (1) is logically equivalent to (2), that (2) is logically equivalent to (3), and that (3) is logically equivalent to (1). It suffices to show that (1) implies (2), that (2) implies (3), and that (3) implies (1).

(1) ⇒ (2) Suppose that $a \equiv b$. By symmetry of $\equiv$, we know that $b \equiv a$. We wish to show that $[a] = [b]$. We show containment both ways.

Let $c \in [a]$. Then $a \equiv c$ by definition of $[a]$. Thus $b \equiv c$ by transitivity of $\equiv$, because $b \equiv a$ and $a \equiv c$. Thus $c \in [b]$ by definition of $[b]$. This shows that $[a] \subset [b]$.

Simply by reversing the roles of a and b is the above argument, we see that $[b] \subset [a]$. Therefore $[a] = [b]$.

(2) ⇒ (3) Suppose that $[a] = [b]$. We wish to show that $b \in [a]$. Now by reflexivity, $b \equiv b$. Thus $b \in [b]$. Since $[a]$ is the same set as $[b]$, we must have $b \in [a]$.

(3) ⇒ (1) Suppose that $b \in [a]$. We wish to show that $a \equiv b$. But this follows by the definition of $[a]$. □

5. Partitions induced by Equivalence Relations

Proposition V.9. *Let A be a set and let $\equiv$ be an equivalence relation on A. Then the collection of equivalence classes*

$$\mathcal{C} = \{[a] \in \mathcal{P}(A) \mid a \in A\}$$

forms a partition of A.

Proof. We wish to show that the equivalence classes are pairwise disjoint and cover A. It is clear that they cover, since for any $a \in A$, we have $a \in [a]$.

Let $a, b \in A$ so that $[a], [b] \in \mathcal{C}$ are arbitrary equivalence classes. Suppose that their intersection is nonempty, say $c \in [a] \cap [b]$. Then $[c] = [a]$ and $[c] = [b]$; thus $[a] = [b]$. This tells us that the only way two equivalence classes can have a nonempty intersection is if they are the same class. Thus distinct equivalence classes are disjoint. This was our condition to call the sets in a collection of subsets pairwise disjoint. □

The collection of equivalence classes referred to above is called the *partition induced by the equivalence relation.*

Proposition V.10. *Let A be a set and let $\mathcal{C}$ be a partition of A. Define a relation R on A by*

$$R = \{(a, b) \in A \times A \mid a \in [b]\}.$$

Then R is an equivalence relation.

Proof. We wish to show that R is reflexive, symmetric, and transitive.

Since $\mathcal{C}$ is a partition, every element of $a \in A$ is in exactly one member of $\mathcal{C}$. Let us denote this member by $[a]$. We first note that for $a, b \in A$, $a \in [b]$ if and only if $[a] = [b]$. To see this, suppose that $a \in [b]$. Then $[b]$ is the unique member of the partition $\mathcal{C}$ which contains a. Since we are calling this member $[a]$, we have $[a] = [b]$. On the other hand, if $[a] = [b]$, we know that $a \in [a]$, so $a \in [b]$.

We have $a \in [a]$, so $(a, a) \in R$. Thus R is reflexive.

Suppose aRb. We wish to show that bRa. Now aRb means that $a \in [b]$, so $[a] = [b]$. Thus $a \in [b]$; therefore bRa. Reversing the roles of a and b shows that $bRa \Rightarrow aRb$. Thus $aRb \Leftrightarrow bRa$, and R is symmetric.

Suppose that aRb and bRc. We wish to show that aRc. Rephrased, we wish to show if $a \in [b]$ and $b \in [c]$, then $a \in [c]$. But $a \in [b]$ implies that $[a] = [b]$, and $b \in [c]$ implies that $[b] = [c]$; thus $[a] = [c]$, so $a \in [c]$, and aRc. Thus R is transitive. □

The relation defined above is called the *equivalence relation induced by the partition.* The above two propositions say that the concepts of partition and equivalence relation correspond to each other in a natural way. A partition is an equivalence relation by considering its blocks as equivalence classes, and an equivalence relation partitions the set into blocks which are equivalence classes.

6. Partitions induced by Functions

We now show that if $f : A \to B$ is a function, then f induces an equivalence relation on the domain A.

Proposition V.11. *Let $f : A \to B$ be a function. Define a relation $\equiv$ on A by*

$$a \equiv b \Leftrightarrow f(a) = f(b).$$

Then $\equiv$ is an equivalence relation.

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

It is reflexive because $f(a) = f(a)$. It is symmetric because $f(a) = f(b) \Leftrightarrow f(b) = f(a)$. It is transitive because $f(a) = f(b)$ and $f(b) = f(c)$ implies that $f(a) = f(c)$. □

The relation defined above is called the *equivalence relation induced by the function*, and the associated partition, naturally enough, is called the *partition induced by the function.* The blocks of this partition are nothing but the preimages of points in B under the map A. The equivalence relation induced by a function is sometimes called a *kernel equivalence.* The equivalence class of a under such an equivalence is sometimes denoted $\overline{a}$ instead of $[a]$. The set of equivalence classes may be denoted $\overline{A}$.

Example V.12. 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

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

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 V.13. 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. □

7. Functions defined on Partitions

Let A be a set and let $\mathcal{A}$ be a partition of A. For a given $a \in A$, let $[a]$ denote the block in $\mathcal{A}$ which contains a. We say that *a represents* the block $[a]$, or that a is a *choice of representative*. Suppose B is another set and we wish to define a function $\alpha : \mathcal{A} \to B$, and we do so by saying where each block $[a] \in \mathcal{A}$ should be sent in B. Perhaps we use some formula or algorithm which depends on the choice of representative $a_1 \in [a]$. Then we better be certain that, if a_2 is another element representing $[a]$, then the algorithm gives the same value for a_2 as it did for a_1.

Example V.14. Let $X = \mathbb{R} \smallsetminus \{0\}$ be the set of nonzero real numbers. Let $Y = \{x \in X \mid x > 0\}$ be the set of positive real numbers and let $Z = X \smallsetminus Y$ 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 $[1] = [2]$, but $f([1]) = 1$ and $f([2]) = 4$.

However, if we attempt to define a function $g : \mathcal{X} \to \mathbb{Z}$ by $[x] \mapsto \frac{x}{|x|}$, 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. □

Let A be a set and let $\mathcal{A}$ be a partition of A. Let $g : A \to B$ be a function. Suppose we define a function $f : \mathcal{A} \to B$ by specifying $f([a]) = g(a) \in B$. If $g(a_1) = g(a_2)$ whenever $[a_1] = [a_2]$, we say the function is *well-defined.*

Example V.15. Let V be the set of vertebrate animals in the world and let $\mathcal{V}$ 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 $f : \mathcal{A} \to B$ by

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

Then f is well-defined, since all the vertebrates of the same species are of the same type.

However, if we attempt to define $g : \mathcal{A} \to \mathbb{R}$ by

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

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

8. Canonical Functions

Let $\overline{A}$ be a partition of a set A, and for $a \in A$ let $\overline{a}$ denote the block containing a. Then there is a *canonical function*

$$\beta : A \to \overline{A}$$

given by $f(a) = \overline{a}$. Each element simply is sent to the block containing it. That is, each element is sent to its equivalence class in the equivalence relation corresponding to the partition. The function β is surjective, since every block contains an element (we made it part of our definition of partition that its members are nonempty).

Theorem V.16. *Let $\phi : A \to B$ be a function. Let $\overline{A}$ be the set of equivalence classes of A induced by f. Let $\beta : A \to \overline{A}$ be the canonical function given by $a \mapsto \overline{a}$. Then there exists a unique injective function*

$$\overline{\phi} : \overline{A} \to B$$

such that $\phi = \overline{\phi} \circ \beta$. If ϕ is surjective, then $\overline{\phi}$ is bijective.

Proof. Define $\overline{\phi}$ by $\overline{\phi}(\overline{a}) = \phi(a)$. We must show that this is well defined and injective, that $\phi = \overline{\phi} \circ \beta$, and that any other function $\psi : \overline{A} \to B$ such that $\phi = \psi \circ \beta$ is equal to $\overline{\phi}$.

Note that $\overline{\phi}$ is defined via a choice of representative for a given block in $\overline{A}$. To show that $\overline{\phi}$ is well-defined, we must show that the definition of $\overline{\phi}$ is independent of the choice of representative. Thus let $a_1, a_2 \in A$ such that $\overline{a_1} = \overline{a_2}$. Thus a_1 and a_2 are inverse images of the same point in B under the map ϕ. That is, $\phi(a_1) = \phi(a_2)$. Therefore $\overline{\phi}(\overline{a_1}) = \phi(a_1) = \phi(a_2) = \overline{\phi}(\overline{a_2})$, and $\overline{\phi}$ is well-defined.

To see that $\overline{\phi}$ is injective, let $\overline{a_1}, \overline{a_2} \in \overline{A}$ such that $\overline{\phi}(\overline{a_1}) = \overline{\phi}(\overline{a_2})$. Then $\phi(a_1) = \phi(a_2)$. By definition of kernel equivalence, $\overline{a_1} = \overline{a_2}$, so $\overline{\phi}$ is injective.

To see that $\phi = \overline{\phi} \circ \beta$, note that for $a \in A$, $\phi(a) = \overline{\phi}(\overline{a}) = \overline{\phi}(\beta(a))$. Thus this holds essentially by definition of $\overline{\phi}$ and of β.

Suppose that $\psi : \overline{A} \to B$ is another function such that $\phi = \psi \circ \beta$. Then $\psi(\overline{a}) = \phi(a) = \overline{\phi}(\overline{a})$, so $\overline{\phi} = \psi$ since it acts the same way on every element of its domain. Thus $\overline{a}$ is the unique function with this property. □

Example V.17. Let A be the set of animals on earth and let S be the set of species. Let $\phi : A \to S$ 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 ϕ. Let $\beta : A \to \overline{A}$ 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 $\overline{\phi}$, whose existence is guaranteed by the above theorem, sends each block to the species to which the animals in the block belong. □

9. Exercises

Exercise V.1. Let A and B be sets and let $\leq$ be a total order on B. Let $f : A \to B$ be a function and define a relation $\preccurlyeq$ on A by

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

(a) Show that if f is injective, $\preccurlyeq$ is a total order on A.
(b) Give an example where f is not injective and $\preccurlyeq$ is not a partial order on A.

Exercise V.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 V.3. Let X be a set and let $\mathcal{C} \subset \mathcal{P}(X)$. Define a relation $\equiv$ on $\mathcal{C}$ by

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

Show that $\equiv$ is an equivalence relation.

Definition V.18. 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.

Exercise V.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 V.5. 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 V.6. Let $\mathcal{C} \subset \mathcal{P}(\mathbb{R}^2)$ be the collection of all circles in the cartesian plane. Define a relation $\equiv$ on $\mathcal{C}$ by

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

Is $\equiv$ an equivalence relation?

Exercise V.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 V.8. Let $X = \{1, 2, 3\}$. Define a function $f : \mathcal{P}(X) \smallsetminus \{\varnothing\} \to X$ by

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

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

Exercise V.9. Let $X = \mathbb{N} \times \mathbb{N}$. Define a relation on X by

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

(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 V.10. Define a relation $\equiv$ on $\mathbb{Z}$ by

$$a \equiv b \Leftrightarrow 6 \mid (a - b).$$

(a) Show that $\equiv$ 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 V.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 V.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 $\equiv$ 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 VI

Binary Operators

1. Binary Operators

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

$$* : A \times A \to A.$$

A binary operator is simply something that takes two elements of a set and gives back a third element of the same set.

Example VI.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.

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

Example VI.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 $A, B \subset X$. $\square$

Example VI.3. 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 $\circ(\phi, \psi) = \phi \circ \psi$. $\square$

Let A be a set and let $* : A \times A \to A$ be a binary operator. As in the above examples, it is customary to write $a * b$ instead of $*(a, b)$, where $a, b \in A$. However, we keep in mind that $*$ is a function and that $a * b \in A$.

2. Closure

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

Example VI.4. 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 VI.5. 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 VI.6. 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. Standard Notation

It is very common that binary operations be named addition or multiplication, even if the elements of the set are not numbers in the common sense.

If the operation on A is named addition and denoted $+$, then it is standard that the identity element be named zero and denoted 0 and that the inverse of a is denoted $-a$. By convention, one may assume that an operation denoted by $+$ is commutative and associative. If n is a natural number and $a \in A$, then na means a added to itself n times.

If the operation on A is denoted $\cdot$, it is usually but not always called multiplication and the $\cdot$ is dropped, so that ab means $a \cdot b$. The identity element in this notation is usually called one and written 1. The inverse of a, if it exists, is denoted a^{-1}. If n is a natural number and $a \in A$, the a^n means a multiplied by itself n times.

When people refer to general binary operations, usually multiplicative notation is used, since it is the simplest. We also use $*$ to mean a “generic” binary operation.

4. Properties of Binary Operators

Let A be a set and let $* : A \times A \to A$ be a binary operator on A.

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

$$a * b = b * a.$$

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

$$(a * b) * c = a * (b * c).$$

We say that $e \in A$ is an *identity element* for $*$ if for every $a \in A$ we have

$$e * a = a * e = a.$$

We note that if $*$ has an identity element, then it is necessarily unique. For suppose that e and f are both identity elements for the operation $*$. Then $e * f = f$ since e is an identity, but also $e * f = e$ since f is an identity. Thus $e = f$.

Suppose that e is an identity for $*$. We say that $b \in A$ is an *inverse* for $a \in A$ if

$$a * b = b * a = e.$$

We note that when $*$ is associative, then inverses are unique. Indeed, if b and c are both inverses for a, then $a*b = e$, and applying c on the left gives $c*(a*b) = c*e = c$. But if $*$ is associative, $c * (a * b) = (c * a) * b = e * b = b$, so $c = b$. If $a \in A$ has an inverse, we say that a is *invertible*.

If $*$ has an identity and every element has an inverse, we say that $*$ is an *invertible* operation.

Example VI.7. 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 VI.8. 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

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

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

Example VI.9. 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 VI.10. 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 is a function

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

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

Example VI.11. 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,

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

Example VI.12. 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 labeled 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.

5. Exercises

Exercise VI.1. In each case, we define a binary operation $*$ on $\mathbb{R}$. Determine if $*$ is commutative and/or associative, find an identity if it exists, and find any invertible elements.
(a) $x * y = xy + 1$;
(b) $x * y = \frac{1}{2}xy$;
(c) $x * y = |x|^y$.

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

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

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

Exercise VI.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 VI.4. Let X and Y be sets and let $* : Y \times Y \to Y$ 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

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

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

Exercise VI.5. Let X and Y be sets and let $* : Y \times Y \to Y$ be a binary operation on Y. Let $\mathcal{F}(X, Y)$ be the set of all functions from X to Y. Show that $*$ induces a binary operation, which may also be called $*$, on $\mathcal{F}(X, Y)$.

Exercise VI.6. Let X be a set and let $* : X \times X \to X$ be a binary operation on X which is associative and invertible. Show that $*$ induces a binary operation, which may also be called $*$, on $\mathcal{P}(X)$. Is it associative? Does it have an identity? Is it invertible?

CHAPTER VII

Cardinality

1. Cardinality

Let U be a *universal set.* That is, U is an extremely large set containing all elements that we care about. In particular, let U contain $\mathbb{R}$ and as many power sets of power sets of $\mathbb{R}$ as you wish.

Let $A, B \subset U$. We say that A and B have the same *cardinality* if there exists a bijective function between them. If A and B have the same cardinality, we write $A \sim B$. Then $\sim$ is a relation on $\mathcal{P}(U)$.

Proposition VII.1. *The relation $\sim$ is an equivalence relation on $\mathcal{P}(U)$.*

Proof. Note that for $A \in \mathcal{P}(U)$, the identity function $\mathrm{id}_A : A \to A$ is bijective. Thus $\sim$ is reflexive.

If $\phi : A \to B$ is bijective, then $\phi^{-1} : B \to A$ is also bijective. Thus $\sim$ is symmetric.

Since the composition of bijective functions is bijective, $\sim$ is transitive. □

We shall call the equivalence classes of the relation the *cardinal numbers in U*. Let $\beth$ denote the set of cardinal number in U. If $A \subset U$, the equivalence class to which it belongs is denoted $|A|$, and is called the *cardinality* of A.

Define a relation $\leq$ on $\beth$ by

$$|A| \leq |B| \Leftrightarrow \exists \text{ injective } \phi : A \to B;$$

where $A, B \subset U$ are representatives of the cardinal numbers $|A|$ and $|B|$ respectively.

Proposition VII.2. *The relation $\leq$ on $\beth$ is well defined.*

Proof. Let $A_1, A_2, B_1, B_2 \subset U$ such that $A_1 \sim A_2$ and $B_1 \sim B_2$, and such that $|A_1| \leq |B_1|$. We wish to show that $|A_2| \leq |B_2|$.

Since $A_1 \sim A_2$, there exists a bijective function $\alpha : A_1 \to A_2$. Since $B_1 \sim B_2$, there exists a bijective function $\beta : B_1 \to B_2$. Since $|A_1| \leq |B_1|$, there exists an injective function $\phi : A_1 \to B_1$.

Since α is bijective, the inverse function α^{-1} exists and is bijective. Then the function

$$\beta \circ \phi \circ \alpha^{-1} : A_2 \to B_2$$

is injective, because the composition of injective functions is injective. Thus $|A_2| \leq |B_2|$. □

Proposition VII.3. *The relation $\leq$ on $\beth$ is a total order.*

Proof. Exercise. □

To prove the above proposition, you will need the following theorem.

Theorem VII.4. Schroder-Bernstein Theorem
Let X and Y be sets and let $f : X \to Y$ and $g : Y \to X$ be injective functions. Then there exists a bijective function $q : X \to Y$.

Proof. Project. □

2. Finite Sets

We say that $A \subset U$ is *finite* if there is not a surjective function $A \to \mathbb{N}$.

For $n \in \mathbb{N}$, let us denote the set $\{0, 1, \ldots, n-1\} \subset \mathbb{N}$ by $\mathbb{N}_n$.

Proposition VII.5. *A set $A \subset U$ is finite if and only if it has the same cardinality as $\mathbb{N}_n$ for some $n \in \mathbb{N}$.*

3. Levels of Infinity

If $|A| \leq |B|$ but $|A| \neq |B|$, we write $|A| < |B|$. We now consider an amazing fact.

Proposition VII.6. *Let $A \subset U$. Then $|A| < \mathcal{P}(A)$.*

4. Exercises

Problem VII.1. Let X and Y be sets and let $f : X \to Y$ and $g : Y \to X$ be functions. Show that there exist subsets $A \subset X$ and $B \subset Y$ such that $f[A] = B$ and $g[Y \smallsetminus B] = X \smallsetminus A$.

Problem VII.2. Schroder-Bernstein Theorem Let X and Y be sets and let $f : X \to Y$ and $g : Y \to X$ be injective functions. Show that there exists a bijective function $h : X \to Y$.

Problem VII.3. Show that $\leq$ is a total order on $\beth$.

CHAPTER VIII

Natural Numbers

1. Natural Numbers

We wish to create a set which is allows us to count in a more or less formal way. The numbers we use to count are be labeled 0, 1, 2, et cetera, defined in a manner which reflects what we memorized as infants.

Having built the language of sets, we start with the simplest set, which is the empty set, and call it 0. Now 1 is naturally thought of as a set containing one element, and the most obvious choice for an this element is 0. Proceeding in this way, we would obtain

- $0 = \varnothing$;
- $1 = \{\varnothing\}$;
- $2 = \{\varnothing, \{\varnothing\}\}$;
- $3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$;

and so forth. We could have written this as

- $0 = \varnothing$;
- $1 = \{0\}$;
- $2 = \{0, 1\}$;
- $3 = \{0, 1, 2\}$;

and so forth. Under this interpretation, a given natural number should be the set containing all of the previous natural numbers. Having made a plan for defining natural numbers, we proceed to attempt to formalize it.

We define 0 to be the empty set. If x is a set, the *successor* of x is denoted x^+ and is defined as

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

The *natural numbers* are the set $\mathbb{N}$ defined by following properties:

(1) $0 \in \mathbb{N}$;
(2) if $n \in \mathbb{N}$, then $n^+ \in \mathbb{N}$;
(3) if $S \subset \mathbb{N}$, $0 \in S$, and $n \in S \Rightarrow n^+ \in S$, then $S = \mathbb{N}$.

2. Induction

Note that the third property of natural numbers asserts that only eventual successors of 0 are in $\mathbb{N}$; that is, this property asserts that $\mathbb{N}$ is a minimal set containing eventual successors of 0, and that $\mathbb{N}$ is the unique set satisfying (1) through (3). This property is known as the *Principal of Mathematical Induction.*

Suppose that for every natural number n, we have a proposition $p(n)$ which is either true or false. Let

$$S = \{n \in \mathbb{N} \mid p(n) \text{ is true}\}.$$

Now if $p(0)$ is true, and if the truth of $p(n)$ implies the truth of $p(n^+)$, then the set S contains 0 and it contains the successor of every element in it. Thus, in this case, $S = \mathbb{N}$, which means that $p(n)$ is true for all $n \in \mathbb{N}$. We state this as

Theorem VIII.1. Induction Theorem
Let $p(n)$ be a proposition for each $n \in \mathbb{N}$. If

(1) *$p(0)$ is true;*
(2) *If $p(n)$ is true, then $p(n^+)$ is true;*

then $p(n)$ is true for all $n \in \mathbb{N}$.

For $m, n \in \mathbb{N}$, we say the m is less than or equal to n if $m \subset n$:

$$m \leq n \Leftrightarrow m \subset n.$$

Now 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 VIII.2. Strong Induction Theorem
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 $p(n+1)$ 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 $n \in \mathbb{N}$. □

3. Recursion

We now state the Recursion Theorem, which will allows us to define addition and multiplication of natural numbers. It is possible to prove this theorem using strong induction.

Theorem VIII.3. 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 $n \in \mathbb{N}$.

Let $f : \mathbb{N} \to \mathbb{N}$ be given by $f(n) = n^+$. Let $\sigma_m : \mathbb{N} \to \mathbb{N}$ be the unique function, whose existence is guaranteed by the Recursion Theorem, defined by $\sigma_m(0) = m$ and $\sigma_m(n^+) = f(\sigma_m(n)) = (\sigma_m(n))^+$. Then $\sigma_m(n)$ is defined to be the *sum* of m and n:

$$m + n = \sigma_m(n).$$

Let $f : \mathbb{N} \to \mathbb{N}$ be given by $f = \sigma_m$. Let $\mu_m : \mathbb{N} \to \mathbb{N}$ be the unique function, whose existence is guaranteed by the Recursion Theorem, defined by $\mu_m(0) = 0$ and $\mu_m(n^+) = f(\mu_m(n)) = \sigma_m(\mu_m(n)) = m + \mu_m(n)$. Then $\mu_m(n)$ is defined to be the *product* of m and n:

$$mn = \mu_m(n).$$

The following properties of natural numbers can be proved using the above definitions:

- $m + n = n + m$ (commutativity of addition);
- $(m + n) + o = m + (n + o)$ (associativity of addition);
- $mn = nm$ (commutativity of multiplication);
- $(mn)o = m(no)$ (associativity of multiplication);
- $m(n + o) = mn + mo$ (distributivity of multiplication over addition);
- $m + 0 = m$ (0 is an additive identity);
- $1m = m$ (1 is a multiplicative identity);
- $0m = 0$.

We state two additional properties, which we will use to show that multiplication of integers is well-defined.

Proposition VIII.4. Cancelation Law of Addition
Let $a, b, c \in \mathbb{N}$ and suppose that $a + c = b + c$. Then $a = b$.

Proposition VIII.5. Cancelation Law of Multiplication
Let $a, b, c \in \mathbb{N}$ and suppose that $ac = bc$. Then $a = b$.

CHAPTER IX

Integers

1. Motivation

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.

2. Definition

Proposition IX.1. *Let $X = \mathbb{N} \times \mathbb{N}$. Define a relation on X by*

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

Then $\equiv$ is an equivalence relation.

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

(Reflexivity) Let $(a, b) \in X$. Then $a + b = b + a$ because addition of natural numbers is commutative. Thus $(a, b) \equiv (a, b)$, and $\equiv$ is reflexive.

(Symmetry) Let $(a, b), (c, d) \in X$. Then by symmetry of equality and commutativity of addition of natural numbers,

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

Thus $\equiv$ is symmetric.

(Transitivity) Let $(a, b), (c, d), (e, f) \in X$. Suppose that $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$. 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 cancelation, we obtain $a + f = b + e$. Thus $(a, b) \equiv (e, f)$, and $\equiv$ is transitive. □

The set of equivalence classes in this equivalence relation is called the set of *integers*, and is denoted $\mathbb{Z}$. The equivalence class of (a, b) is denoted $[a, b]$.

3. Addition

We define addition in $\mathbb{Z}$ by

$$[a, b] + [c, d] = [a + c, b + d].$$

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 IX.2. *Addition in $\mathbb{Z}$ 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 $(a_1, b_1) \equiv (a_2, b_2)$ and $(c_1, d_1) \equiv (c_2, d_2)$, 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 $[a_2 + c_1, b_1 + d_1] = [a_2 + c_2, b_2 + d_2]$.

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 $(a_1+c_1, b_1+d_1) \equiv (a_2+c_2, b_2+d_2)$. Therefore $[a_1+c_1, b_1+d_1] = [a_2+c_2, b_2+d_2]$, and addition is well-defined. □

4. Multiplication

We define multiplication in $\mathbb{Z}$ by

$$[a, b] \cdot [c, d] = [ac + bd, ad + bc].$$

Proposition IX.3. *Multiplication in $\mathbb{Z}$ is well defined.*

Proof. 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 $(a_1, b_1) \equiv (a_2, b_2)$ and $(c_1, d_1) \equiv (c_2, d_2)$, 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

$$z = a_1d_2 + b_2d_1 + b_1c_2 + a_2c_1.$$

By the cancelation law of addition of natural numbers, it suffices to show that $x + z = y + z$. This is accomplished by showing that each side is equal to $2(a_1b_2)(c_1d_2)$.

First add z to both sides of the definition of x, expand z on the right side, and use commutativity of addition to insert shuffle the terms of z 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 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

$$(a_1 + b_2 + b_1 + a_2)(c_1 + d_2) = x + z.$$

Since $a_1 + b_2 = a_2 + b_1$, we have

$$2(a_1 + b_2)(c_1 + d_2) = x + z.$$

Perform the same manner of computation on the equation defining y, and you will find that

$$2(a_1 + b_2)(c_1 + d_2) = y + z.$$

□

5. Algebraic Properties

Theorem IX.4. *Let $a, b, c \in \mathbb{Z}$. Then*

1. $a + b = b + a$ (commutativity of addition)*;*
2. $a + (b + c) = (a + b) + c$ (associativity of addition)*;*
3. $\exists! z \in \mathbb{Z}$ *such that* $a + z = a$ (additive identity)*;*
4. $\exists! - a \in \mathbb{Z}$ *such that* $a + (-a) = z$ (additive inverses)*;*
5. $ab = ba$ (commutativity of multiplication)*;*
6. $a(bc) = (ab)c$ (associativity of multiplication)*;*
7. $\exists! e \in \mathbb{Z}$ *such that* $ae = a$ (multiplicative identity)*;*
8. $a(b + c) = ab + ac$ (distributivity of multiplication over addition).

These eight properties state that $\mathbb{Z}$ is a *commutative ring.* We prove or comment on each.

Proposition IX.5. *Let $a, b \in \mathbb{Z}$. Then $a + b = b + a$.*

Proof. Since a and b are integers, they are represented by pairs of natural numbers, say $a = [m, n]$ and $b = [u, v]$. Then

$$a + b = [m, n] + [u, v] = [m + u, n + v] = [u + m, v + n] = [u, v] + [m, n] = b + a.$$

□

Proposition IX.6. *Let $a, b, c \in \mathbb{Z}$. Then $(a + b) + c = a + (b + c)$.*

Proof. This follows easily from the definitions and the fact that addition is associative in the natural numbers in a manner entirely analogous to the proof above. □

Proposition IX.7. *There exists a unique element $z \in \mathbb{Z}$ such that for every $a \in \mathbb{Z}$ we have $a + z = a$.*

Proof. Let $z = [0, 0]$. The fact that $a + z = a$ is immediate from the definition and the analogous fact in $\mathbb{N}$. Later, we will justify calling this element z by the name zero.

For uniqueness, suppose that y also satisfies $a + y = a$ for all $a \in \mathbb{Z}$. Then $z = z + y = y + z = y$. □

Proposition IX.8. *For every $a \in \mathbb{Z}$ there exists a unique element $-a \in \mathbb{Z}$ such that $a + (-a) = z$.*

Proof. Let $a = [m, n]$, where $m, n \in \mathbb{N}$. Define $-a = [n, m]$. Then $a + (-a) = [m + n, m + n] = [0, 0]$. Call this element *negative* a.

For uniqueness, suppose $a + b = z$. Then $a + b = a + (-a)$. By commutativity, $b + a = (-a) + a$. Adding $(-a)$ to both sides gives $b = b + z = b + a + (-a) = (-a) + a + (-a) = (-a) + z = (-a)$. □

Now we may define *subtraction* on $\mathbb{Z}$ by

$$a - b = a + (-b).$$

Clearly subtraction in not commutative or associative.

Proposition IX.9. *Let $a, b \in \mathbb{Z}$. Then $ab = ba$.*

Proof. Let $a = [m, n]$ and $b = [u, v]$. Then $ab = [mu + nv, mv + nu] = [um + vn, vm + un] = ba$. □

Proposition IX.10. *Let $a, b, c \in \mathbb{Z}$. Then $a(bc) = (ab)c$.*

Proof. Same idea as the proof of commutativity. □

Proposition IX.11. *There exists a unique element $e \in \mathbb{Z}$ such that for every $a \in \mathbb{Z}$ we have $ae = a$.*

Proof. Let $e = [1, 0]$ and let $a = [m, n]$. Then $ae = [1m+0n, 1n+0m] = [m, n] = a$.

For uniqueness, suppose that $y \in \mathbb{Z}$ also satisfies $ay = a$ for all $a \in \mathbb{Z}$. Then $y = ye = ey = e$. □

Proposition IX.12. *Let $a, b, c \in \mathbb{Z}$. Then $a(b + c) = ab + ac$.*

Proof. Let $a = [m, n]$, $b = [u, v]$, and $c = [x, y]$. Then

$$\begin{aligned} a(b + c) &= [m, n][u + x, v + y] \\ &= [m(u + x) + n(v + y), m(v + y) + n(u + x] \\ &= [mu + mx + nv + ny, mv + my + nu + nx] \\ &= [mu + nv + mx + ny, mv + nu + my + nx] \\ &= [mu + nv, mv + nu] + [mx + my, my + nx] \\ &= [m, n][u, v] + [m, n][x, y] \\ &= ab + ac. \end{aligned}$$

□

To define exponentiation in $\mathbb{Z}$, one may use the Recursion Theorem.

Let $b \in \mathbb{Z}$ and let $f : \mathbb{Z} \to \mathbb{Z}$ be given by $f(a) = ba$. Let $\epsilon_b : \mathbb{N} \to \mathbb{Z}$ be the unique function, whose existence is guaranteed by the Recursion Theorem, defined by $\epsilon_b(0) = 1$ and $\epsilon_b(n^+) = f(\epsilon_b(n)) = b\epsilon_b(n)$. Then $\epsilon_b(n)$ is defined to be b raised to the n^{th} power, and is denoted by b^n:

$$b^n = \epsilon_b(n).$$

Note that if $a \in \mathbb{Z}$, then b^a is undefined.

6. 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. Thus we want our injective function to preserve these properties.

Let $\phi : \mathbb{N} \to \mathbb{Z}$. We say that ϕ is an *embedding* if

- $\phi(1) = e$, where e is the multiplicative identity of $\mathbb{Z}$;
- $\phi(m + n) = \phi(m) + \phi(n)$;
- $\phi(mn) = \phi(m)\phi(n)$.

There is a unique function $\phi : \mathbb{N} \to \mathbb{Z}$ which satisfies all of these properties, and it is given by $\phi(n) = [n, 0]$.

This also gives us additional properties which motivated us in the first place:

- $\forall n \in \mathbb{N} \exists b \in \mathbb{Z}$ such that $\phi(n) + b = \phi(0)$;
- $\forall a \in \mathbb{Z} \exists n \in \mathbb{N}$ such that either $a = \phi(n)$ or $a = -\phi(n)$.

The first of these says that $\mathbb{Z}$ contains the additive inverses of the natural numbers, and the second 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 $a \in \phi(\mathbb{N}) \subset \mathbb{Z}$. The meaning should be clear from the context.

In particular, $\phi(1) = e$ by definition and $\phi(0) = z$ because the additive identity of $\mathbb{Z}$ is unique. Thus we identity 1 with e and 0 with z, and may drop these temporary names.

7. Order

Let $\phi : \mathbb{N} \hookrightarrow \mathbb{Z}$ be the embedding given by $n \mapsto [n, 0]$.

We define a relation $\leq$ on $\mathbb{Z}$ by

$$a \leq b \Leftrightarrow b - a \in \phi(\mathbb{N}).$$

This leads to other relations:

- $a < b \Leftrightarrow (a \leq b) \wedge (a \neq b)$;
- $a > b \Leftrightarrow \neg(a \leq b)$;
- $a \geq b \Leftrightarrow \neg(a < b)$.

Proposition IX.13. *The relation $\leq$ on $\mathbb{Z}$ is a total order.*

Proposition IX.14. *Let $m, n \in \mathbb{N}$. Then $m \leq n$ if and only if $\phi(m) \leq \phi(n)$.*

Proposition IX.15. *The relation $\leq$ on $\mathbb{Z}$ has the following properties:*

(1) $a \leq b \Rightarrow a + c \leq b + c$;
(2) $(c \geq 0) \wedge (a \leq b) \Rightarrow ac \leq bc$;
(3) $(c \leq 0) \wedge (a \leq b) \Rightarrow ac \geq bc$.

We define a function $|\cdot| : \mathbb{Z} \to \mathbb{N}$ by

$$|a| = \begin{cases} a \text{ if } a \geq 0; \\ -a \text{ otherwise} . \end{cases}$$

We call $|a|$ the *absolute value* of a.

8. Exercises

Construct the rational numbers as follows.

Exercise IX.1. Find an appropriate set on which to work. Define an relation on this set, and show that it is an equivalence relation. Define the set $\mathbb{Q}$ of rational numbers to be the equivalence classes of this equivalence relation.

Exercise IX.2. Define addition and multiplication on $\mathbb{Q}$ and show that it is well defined.

Exercise IX.3. Let $a, b, c \in \mathbb{Q}$. Show that

(1) $a + b = b + a$;
(2) $a + (b + c) = (a + b) + c$;
(3) $\exists ! 0 \in \mathbb{Q}$ such that $a + 0 = a$;
(4) $\exists ! - a \in \mathbb{Q}$ such that $a + (-a) = 0$;
(5) $ab = ba$;
(6) $a(bc) = (ab)c$;
(7) $\exists ! 1 \in \mathbb{Q}$ such that $a1 = a$;
(8) $a \neq 0 \Rightarrow \exists a^{-1} \in \mathbb{Q}$ such that $aa^{-1} = 1$;
(9) $a(b + c) = ab + ac$.

The nine properties above assert that $\mathbb{Q}$ is a *field*.

Exercise IX.4. Define a relation on $\mathbb{Q}$ which coincides with the common notion of their ordering, and show that this is a total order relation.

CHAPTER X

Modular Integers

1. Well-Ordering Principle

First we establish a few properties of the integers which we need in order to understand the ring of integers modulo n. One tool which can be used to establish these properties is the Well-Ordering Principle.

Proposition X.1. Well-Ordering Principle
Let $X \subset \mathbb{N}$ be a nonempty set of natural numbers. Then X contains a smallest, element; that is, there exists $x_0 \in X$ such that for every $x \in X$, $x \leq x_0$.

Proof. Since X is nonempty, it contains an element, say x_1. If x_1 is the smallest member of X, we are done, so assume that the set

$$Y = \{x \in X \mid y < x_1\}$$

is nonempty. Since there are only finitely many natural numbers less than a given natural number, Y is finite.

Proceed by induction on $\pmod{Y}$. If $\pmod{Y} = 1$, then Y contains exactly one element, which is vacuously the smallest member of Y.

Now assume that $\pmod{Y} = n$. By induction, we assume that any nonempty set with less than n elements contains a smallest member. Since Y is nonempty, let $x_2 \in Y$. If x_2 is the smallest member of Y, we are done, so assume that the set

$$Z = \{x \in Y \mid x < x_2\}$$

is nonempty. Since $x_2 \notin Z$, $\pmod{Z} < n$, so Z contains a smallest member (by our inductive hypothesis), say x_0. Then x_0 is also smaller than any element in Y. This completes the proof by induction.

Thus every finite set of natural numbers has a smallest element, and since Y is finite, is has a smallest element. This element is the smallest member of X. □

2. Division Algorithm

Definition X.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 $n = km$.

Exercise X.1. Show that the relation $\mid$ is a partial order on the set of positive integers.

Proposition X.3. Division Algorithm for Integers
Let $m, n \in \mathbb{Z}$. There exist unique integers $q, r \in \mathbb{Z}$ such that

$$n = qm + r \qquad \textit{and} \qquad 0 \le r < \ (\mathrm{mod}\ m).$$

Proof. 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 $0 \le r$. Also, $r < \ (\mathrm{mod}\ m)$, for otherwise, $r - \ (\mathrm{mod}\ m)$ is positive, less than r, and in X.

For uniqueness, assume $n = q_1 m + r_1$ and $n = q_2 m + r_2$, where $q_1, r_1, q_2, r_2 \in \mathbb{Z}$, $0 \le r_1 < m$, and $0 \le r_2 < m$. 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 $q_1 = q_2$. □

Definition X.4. 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

(1) $d \mid m$ and $d \mid n$;
(2) If $e \mid m$ and $e \mid n$, then $e \mid d$.

Proposition X.5. *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 $0 \le r < d$. 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 $d = e$. □

Exercise X.2. 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 X.3. Let $m, n \in \mathbb{N}$ and suppose that $m \mid n$. Show that $\gcd(m, n) = m$.

3. Euclidean Algorithm

There is an effective procedure for finding the greatest common divisor of two integers. It is based on the following proposition.

Proposition X.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 $m = r q_2 + r_3$, 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, $15 = 210 \cdot 4 + 165 \cdot (-5)$.

4. Prime Integers

Definition X.7. An integer $p \in \mathbb{Z}$ is called *prime* if

(1) $p \geq 2$;
(2) $p \mid ab \Rightarrow p \mid a$ or $p \mid b$, where $a, b \in \mathbb{N}$.

Definition X.8. An integer $p \in \mathbb{Z}$ is called *irreducible* if

(1) $p \geq 2$;
(2) $p = ab \Rightarrow a = 1$ or $b = 1$, where $a, b \in \mathbb{N}$.

Exercise X.4. Let $p \in \mathbb{Z}$. Show that p is prime if and only if p is irreducible.

Exercise X.5. Let $a, p \in \mathbb{Z}$ such that p is prime.
Show that $\gcd(a, p) = 1$ or $\gcd(a, p) = p$.

Here is an interesting exercise. The standard proof is by contradiction.

Exercise X.6. Show that there are infinitely many prime integers.
(Hint: assume there are only finitely many, multiply them, and add 1.)

The following series of exercises constitutes a proof that every integer greater than one has a unique factorization into prime integers.

Exercise X.7. Let $p \in \mathbb{Z}$ be prime and let $m, n \in \mathbb{Z}$.
Show that if $p \mid mn$, then $p \mid m$ or $p \mid n$.

Exercise X.8. Let $p \in \mathbb{Z}$ be prime and let $n_1, \dots, n_r \in \mathbb{Z}$.
Show that if $p \mid n_1 \dots n_r$, then $p \mid n_i$ for some $i = 1, \dots, r$.
(Hint: proceed by induction on r.)

Exercise X.9. Let $a \in \mathbb{Z}$ such that $a \geq 2$.
Show that $a = p_1 \dots p_2$, where p_i is prime for $i = 1, \dots, r$.
(Hint: proceed by strong induction on n.)

Exercise X.10. Let $p_1, \dots, p_r, q_1, \dots, q_s$ be prime integers.
Show that if $p_1 \dots p_r = q_1 \dots q_s$, then $r = s$ and that the q_j's can be relabeled so that $p_i = q_i$ for $i = 1, \dots, r$.
(Hint: assume not, and let m be the smallest integer that has two different prime factorizations.)

5. Congruence Modulo n

Definition X.9. Let $n \in \mathbb{N}$, and define a relation $\equiv_n$ on $\mathbb{Z}$ by

$$a \equiv_n b \Leftrightarrow n \mid (a-b).$$

This relation is called *congruence modulo n*; that is, if $a \equiv_n b$, we say that a is *congruent* to b modulo n. Sometimes this is written $a \equiv b \pmod{n}$. If the n is understood, we may drop the " (mod n)" from the notation.

Proposition X.10. *Let $n \in \mathbb{N}$. Then $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.*

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

(*Reflexivity*) Let $a \in \mathbb{Z}$. Now $0 \cdot n = 0 = a - a$; thus $n \mid (a-a)$, so $a \equiv a$. Therefore $\equiv$ is reflexive.

(*Symmetry*) Let $a, b \in \mathbb{Z}$. Suppose that $a \equiv b$; then $n \mid (a-b)$. Then there exists $k \in \mathbb{Z}$ such that $nk = a - b$. Then $n(-k) = b - a$, so $n \mid (b-a)$. Thus $b \equiv a$. Similarly, $b \equiv a \Rightarrow a \equiv b$. Therefore $\equiv$ is symmetric.

(*Transitivity*) Let $a, b, c \in \mathbb{Z}$, and suppose that $a \equiv b$ and $b \equiv c$. Then $nk = a-b$ and $nl = b - c$ for some $k, l \in \mathbb{Z}$. Then $a - c = nk - nl = n(k-l)$, so $n \mid (a-c)$. Thus $a \equiv c$. Therefore $\equiv$ is transitive. □

Proposition X.11. *Let $n \in \mathbb{N}$ and let $a_1, a_2 \in \mathbb{Z}$. By the Division Algorithm, there exist unique integers $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ such that*

- *$a_1 = nq_1 + r_1$, where $0 \le r_1 < n$;*
- *$a_2 = nq_2 + r_2$, where $0 \le r_2 < n$.*

Then $a_1 \equiv a_2 \pmod{n}$ if and only if $r_1 = r_2$.

Proof.

($\Rightarrow$) Suppose that $a_1 \equiv a_2$. Then $n \mid (a_1 - a_2)$. This means that $nk = a_1 - a_2$ for some $k \in \mathbb{Z}$. But $a_1 - a_2 = n(q_1 - q_2) + (r_1 - r_2)$. Then $n(k + q_1 - q_2) = r_1 - r_2$, so $n \mid r_1 - r_2$.

Multiplying the inequality $0 \le r_2 < n$ by -1 gives $-n < -r_2 \le 0$. Adding this inequality to the inequality $0 \le r_1 < n$ gives $-n < r_1 - r_2 < n$. But $r_1 - r_2$ is an integer multiple of n; the only possibility, then, is that $r_1 - r_2 = 0$. Thus $r_1 = r_2$.

($\Leftarrow$) Suppose that $r_1 = r_2$. Then $a_1 - a_2 = nq_1 - nq_2 = n(q_1 - q_2)$. Thus $n \mid (a_1 - a_2)$, so $a_1 \equiv a_2$. □

6. Integers Modulo n

Definition X.12. The partition of $\mathbb{Z}$ induced by the equivalence relation $\equiv_n$ is called the set of *integers modulo* n, and is denoted $\mathbb{Z}_n$. For an integer $a \in \mathbb{Z}$, denote its equivalence class under the equivalence relation by $[a]_n$. If the n is understood, we may write this equivalence class as $[a]$ or $\overline{a}$.

An element $r \in \mathbb{Z}$ is called a *preferred representative* for $[a]_n$ if $r \in [a]_n$ and $0 \leq r < n$.

The division algorithm for the integers assures us that there is a unique preferred representative for each equivalence class. Also, as r ranges over the integers from 0 to $n-1$, the equivalence classes $[r]_n$ are distinct. Thus there are exactly n equivalence classes in the set of integers modulo n; that is, $(\bmod \mathbb{Z}_n) = n$. For example,

$$\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}.$$

Proposition X.13. *Let $n \in \mathbb{Z}$. Define the binary operations of addition and multiplication in $\mathbb{Z}_n$ by*

$$\overline{a} + \overline{b} = \overline{a+b} \text{ and } \overline{a} \cdot \overline{b} = \overline{ab}.$$

These operations are well-defined.

Proof. Select $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ such that $a_1 \equiv a_2$ and $b_1 \equiv b_2$; say $a_1 - a_2 = kn$ and $b_1 - b_2 = ln$ for some $k, l \in \mathbb{Z}$.

(*Addition*) We wish to show that $\overline{a_1 + b_1} = \overline{a_2 + b_2}$, i.e., that $a_1 + b_1 \equiv a_2 + b_2$. We simply add the equations above to obtain

$$a_1 - a_2 + b_1 - b_2 = kn + ln;$$

thus

$$(a_1 + b_1) - (a_2 + b_2) = (k + l)n;$$

from this, $n \mid ((a_1 + b_1) - (a_2 + b_2))$, so $a_1 + b_1 \equiv a_2 + b_2$.

(*Multiplication*) We wish to show that $\overline{a_1} \cdot \overline{b_1} = \overline{a_2} \cdot \overline{b_2}$, i.e., that $a_1 b_1 \equiv a_2 b_2$. To do this, adjust the original equations to obtain

$$a_1 = a_2 + kn \qquad \text{and} \qquad b_1 = b_2 + ln$$

and multiply them to obtain

$$a_1 b_1 = a_2 b_2 + a_2 ln + b_2 kn + kln^2,$$

whence

$$a_1 b_1 - a_2 b_2 = (a_2 l + b_2 k + kln)n;$$

thus $n \mid (a_1 b_1 - a_2 b_2)$, so $a_1 b_1 \equiv a_2 b_2$. □

7. The Group of Integers Modulo n

Proposition X.14. *Addition on $\mathbb{Z}_n$ is commutative, associative, and invertible, with identity element $\overline{0}$.*

Proof. Now select $a, b \in \mathbb{Z}$ so that $\overline{a}$, $\overline{b}$, and $\overline{c}$ are arbitrary members of $\mathbb{Z}_n$.

To see that $+$ is commutative, note that

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \text{ by definition of } + \\ &= \overline{b+a} \text{ by commutativity in } \mathbb{Z} \\ &= \overline{b} + \overline{a} \end{aligned}$$

To see that $+$ is associative, note that

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

To see that $\overline{0}$ is an additive identity, note that $\overline{0} + \overline{a} = \overline{0+a} = \overline{a}$.

The additive inverse of $\overline{a}$ is $\overline{-a}$, since $\overline{a} + \overline{-a} = \overline{a-a} = \overline{0}$. □

Remark X.1. A *group* $(G, \cdot, e)$ is a set G together with a binary operation

$$\cdot : G \times G \to G$$

which is associative and invertible with identity element e. If the operation is also commutative, the group is called an *abelian group.*

The above proposition tells us that $(\mathbb{Z}_n, +, \overline{0})$ is an abelian group.

8. Order of an Element in $\mathbb{Z}_n$

For any $k \in \mathbb{N}$ and any $\overline{a} \in \mathbb{Z}_n$, define $k\overline{a}$ to be $\overline{a}$ added to itself k times:

$$k\overline{a} = \sum_{i=1}^{k} \overline{a}.$$

Proposition X.15. *Let $k \in \mathbb{N}$ and $\overline{a} \in \mathbb{Z}_n$. Then $k\overline{a} = \overline{ka}$.*

Proof. Since addition is associative, we can ignore parentheses. Then

$$k\overline{a} = \sum_{i=1}^{k} \overline{a} = \overline{\sum_{i=1}^{k} a} = \overline{ka}.$$

□

Definition X.16. Let $\overline{a} \in \mathbb{Z}_n$. Define the *order* of $\overline{a}$ to be smallest positive integer k such that $k\overline{a} = \overline{0}$. The order of $\overline{a}$ is denoted $\operatorname{ord}(\overline{a})$.

Proposition X.17. *Let $\overline{a} \in \mathbb{Z}_n$ and let $\operatorname{ord}(\overline{a}) = k$. Then*
(a) $j\overline{a} = \overline{0} \Leftrightarrow k \mid j$;
(b) $n\overline{a} = \overline{0}$;
(c) $k \mid n$.

Proof.

(a) If $k \mid j$, then $j = lk$ for some $l \in \mathbb{Z}$. In this case, $j\overline{a} = l\overline{0} = \overline{0}$.

Conversely, suppose that $j\overline{a} = \overline{0}$. Write $j = qk + r$, where $0 \leq r < k$. Then $j\overline{a} = qk\overline{a} + r\overline{a} = r\overline{a}$ since $k\overline{a} = 0$. But k is the smallest positive integer such that $k\overline{a} = \overline{0}$. Thus $r = 0$, and $j = qk$. Thus $k \mid j$.

(b) Note that $n\overline{a} = \overline{na} = \overline{0}$. Thus $n\overline{a} = \overline{0}$.

(c) By (b), $n\overline{a} = \overline{0}$. Thus $k \mid n$ by part (a). □

Exercise X.11. Let $\overline{a} \in \mathbb{Z}_n$ and let $d = \gcd(a, n)$.
Then $\operatorname{ord}(\overline{a}) = \frac{n}{d}$.
(Hint: let $k = \operatorname{ord}(\overline{a})$, and show that $k \mid \frac{n}{d}$ and that $\frac{n}{d} \mid k$.)

Exercise X.12. Find the order of $\overline{6}$, $\overline{11}$, $\overline{18}$, and $\overline{28}$ in $\mathbb{Z}_{36}$.

9. The Ring of Integers Modulo n

Proposition X.18. *Multiplication on $\mathbb{Z}_n$ is commutative and associative, with identity element $\overline{1}$. Furthermore, multiplication distributes over addition:*

$$\overline{a} \cdot (\overline{b} + \overline{c}) = (\overline{a} \cdot \overline{b}) + (\overline{a} \cdot \overline{c})$$

for all $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}$.

Proof. Select $a, b, c \in \mathbb{Z}$ so that $\overline{a}$, $\overline{b}$, and $\overline{c}$ are arbitrary members of $\mathbb{Z}_n$.

(*Commutativity*) $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$.

(*Associativity*) $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{abc} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$.

(*Identity*) $\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a} = \overline{1 \cdot a} = \overline{1} \cdot \overline{a}$.

(*Distributivity*)

$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b + c} = \overline{a(b + c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = (\overline{a} \cdot \overline{b}) + (\overline{a} \cdot \overline{c})$. □

Remark X.2. A *ring* $(R, +, 0, \cdot, 1)$ is a set R together with a pair of binary operations $+$ and $\cdot$ such that $+$ is commutative, associative, and invertible with identity element 0, and $\cdot$ is associative with identity element 1, such that $\cdot$ distributes over $+$. If additionally $\cdot$ is commutative, the ring is called a *commutative ring*.

The above proposition, together with the fact that addition is commutative, associative, and invertible, say that $(\mathbb{Z}_n, +, \overline{0}, \cdot, \overline{1})$ is a *commutative ring*.

Proposition X.19. *Let $\overline{a} \in \mathbb{Z}_n$. Then $\overline{a} \cdot \overline{0} = \overline{0} \cdot \overline{a} = \overline{0}$.*

Proof. By definition of multiplication in $\mathbb{Z}_n$, $\overline{a} \cdot \overline{0} = \overline{a \cdot 0} = \overline{0} = \overline{0 \cdot a} = \overline{0} \cdot \overline{a}$. □

An element $\overline{a} \in \mathbb{Z}_n$ is called *invertible* if there exists an element $\overline{b} \in \mathbb{Z}_n$ such that $\overline{a} \cdot \overline{b} = \overline{1}$.

Proposition X.20. *Let $n \in \mathbb{N}$ and let $\overline{a} \in \mathbb{Z}_n$.*
Then $\overline{a}$ is invertible if and only if $\gcd(a, n) = 1$.

Proof.

($\Rightarrow$) Suppose that $\overline{a}$ is invertible, and let $\overline{b}$ be its inverse. Then $\overline{ab} = \overline{1}$, so $ab \equiv 1 \pmod{n}$. That is, $kn = ab - 1$ for some $k \in \mathbb{Z}$. Thus $ab + (-k)n = 1$. Therefore $\gcd(a, n) = 1$.

($\Leftarrow$) Suppose that $\gcd(a, n) = 1$. Then there exist $x, y \in \mathbb{Z}$ such that $xa + yn = 1$. Then $\overline{x} \cdot \overline{a} + \overline{y} \cdot \overline{n} = \overline{1}$. But $\overline{n} = \overline{0}$, so $\overline{y} \cdot \overline{n} = \overline{0}$. Thus $\overline{x} \cdot \overline{a} = \overline{1}$, and $\overline{x}$ is the inverse of $\overline{a}$, so $\overline{a}$ is invertible. □

Exercise X.13. Let $p \in \mathbb{N}$ be a prime number.
Show that every nonzero element of $\mathbb{Z}_p$ is invertible.

An element $\overline{a} \in \mathbb{Z}_n$ is called a *zero divisor* if it is not zero and if there exists a nonzero element $\overline{b} \in \mathbb{Z}_n$ such that $\overline{a} \cdot \overline{b} = \overline{0}$.

For example, in $\mathbb{Z}_6$, the invertible elements are 1 and 5. The zero divisors are $\overline{2}$, $\overline{3}$, and $\overline{4}$. For example, $\overline{3} \cdot \overline{4} = \overline{12} = \overline{0}$.

Exercise X.14. Let $n \in \mathbb{N}$ and let $\overline{a} \in \mathbb{Z}_n$ be a nonzero element.
Show that $\overline{a}$ is invertible if and only if $\overline{a}$ is not a zero divisor.

Exercise X.15. Show that if $n \in \mathbb{N}$ is not a prime number, then $\mathbb{Z}_n$ contains zero divisors.

10. Algebraic Equations in $\mathbb{Z}_n$

It is convenient to drop the BAR notation. That is, all numbers are to be interpreted as members of $\mathbb{Z}_n$ for some fixed n, and if we say 0, 1, or a, we mean $\overline{0}$, $\overline{1}$, or $\overline{a}$.

Having dropped the BAR notation, we use the preferred representatives for equivalence classes. Note that $-\overline{a} = \overline{-a} = \overline{n-a}$. For example, in $\mathbb{Z}_8$, we have $-2 = 6$ and $-4 = 4$ (modulo 8).

We now turn our attention to the question of when an equation, such as $14x = 1$ or $x^2 + 1 = 0$, has a solution in $\mathbb{Z}_n$, and how many solutions it has. For example, $14x = 1$ has a solution if and only if 14 is invertible in $\mathbb{Z}_n$, and this is the case if and only if n and 14 are relatively prime. In fact, we have an explicit technique for finding the inverse 14. This technique makes repeated use of the division algorithm.

Suppose $n = 33$. Then 14 and 33 are relatively prime, so there exist integers x and y such that $14x + 33y = 1$. To find them, we divide:

- $33 = 14 \cdot 2 + 5$;
- $14 = 5 \cdot 2 + 4$
- $5 = 4 \cdot 1 + 1$;
- $2 = 1 \cdot 2 + 0$.

The second to last remainder is 1, so $\gcd(14, 33) = 1$. Now work backwards to find x and y:

- $1 = 5 - 4$;
- $1 = 5 - (14 - 5 \cdot 2) = 5 \cdot 3 - 14 \cdot 1$;
- $1 = (33 - 14 \cdot 2) \cdot 3 - 14 \cdot 1 = 33 \cdot 3 - 14 \cdot 7$.

Thus the inverse of 14 in $\mathbb{Z}_{33}$ is $-7 = 26$.

Exercise X.16. Find the inverse of 15 in $\mathbb{Z}_{49}$.

The equation $x^2 + 1 = 0$ is more interesting. To understand it, note that -1 exists in $\mathbb{Z}_n$ as $\overline{n-1}$. So a solution to the equation $x^2 + 1 = 0$ would be a square root of negative 1 in $\mathbb{Z}_n$. For example, in $\mathbb{Z}_5$, we have $2^2 = 4 = -1 \pmod 5$.

It is also possible that a quadratic equation, such as $x^2 - 1 = 0$, can have more than two solutions in $\mathbb{Z}_n$. Note that $x^2 - 1 = (x+1)(x-1)$, even in $\mathbb{Z}_n$. Suppose that $n = 15$. Then $x = 1$ and $x = -1 = 14$ are solutions, but so is 4, since $(4+1)(4-1) = 5 \cdot 3 = 0$ (modulo 15).

However, suppose that $n = p$ is a prime number. Then in $\mathbb{Z}_p$, a quadratic equation can have at most 2 roots. This is because $\mathbb{Z}_p$ has no zero divisors. If the quadratic has a root, it factors; then if the product of the factors is zero, one of them must be zero.

For example, let us find the roots of $x^2 + 8x + 1 = 0$ in $\mathbb{Z}_{11}$. Now $8 \equiv -3 \pmod{11}$ and $1 \equiv -10 \pmod{11}$, so our equation becomes $x^2 - 3x - 10 = 0$. This factors as $(x-5)(x+2) = 0$. Since 11 is prime, the only roots are 5 and $-2 = 8$.

Exercise X.17. Find all square roots of -1 in $\mathbb{Z}_{101}$.

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	$p \Leftrightarrow q$
$\between$	XOR	Exclusion	$p \between q$
$\uparrow$	NOR	Alternate Denial	$p \uparrow q$
$\downarrow$	NAND	Joint Denial	$p \downarrow q$

TABLE 1. Logical Operators

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$	$p \between q$	$p \uparrow q$	$p \downarrow q$
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
$\vdash$	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	$A \subset B \Leftrightarrow (a \in A \Rightarrow a \in B)$
$\cap$	intersection	$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
$\cup$	union	$A \cup B = \{x \mid x \in A \text{ or } x \in B$
$\smallsetminus$	complement	$A \smallsetminus B = \{x \mid x \in A \text{ and } x \notin B\}$
$\times$	cartesian product	$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$

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	$\{a + ib \mid a, b \in \mathbb{R} \text{ and } i^2 = -1\}$
$\mathbb{R}^2$	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

ZFC Axioms

The *Zermelo-Fraenkel* axioms are intended to place set theory on a solid logical foundation. Together with the Axiom of Choice, these form the **ZFC** axioms of set theory, upon which the bulk of modern mathematics is based.

Axiom C.1 (Axiom of Extension)**.** *Two sets are equal if and only if they have the same elements.*

$$\forall A, \forall B \; : \; A = B \iff (\forall C \; : \; C \in A \Leftrightarrow C \in B)$$

Axiom C.2 (Axiom of the Empty Set)**.** *There is a set with no elements.*

$$\exists \varnothing, \forall x \; : \; \neg(x \in \varnothing)$$

Axiom C.3 (Axiom of Pairing)**.** *If A and B are sets, then there is a set containing A and B as its only elements.*

$$\forall A, \forall B, \exists C, \forall D \; : \; D \in C \iff (D = A \vee D = B)$$

Axiom C.4 (Axiom of Union)**.** *If A is a set, there is a set whose elements are precisely the elements of the elements of A.*

$$\forall A, \exists B, \forall C \; : \; C \in B \iff (\exists D \; : \; C \in D \wedge D \in A)$$

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

$$\exists N \; : \; \varnothing \in N \wedge (\forall A \; : \; A \in N \Rightarrow A \cup \{A\} \in N)$$

Axiom C.6 (Axiom of Powers)**.** *If A is a set, there is a set whose elements are precisely the subsets of A.*

$$\forall A, \exists \mathcal{P}(A), \forall B \; : \; B \in \mathcal{P}(A) \iff (\forall C \; : \; C \in B \Rightarrow C \in A)$$

Axiom C.7 (Axiom of Regularity)**.** *If A is a set, there is an element of A which is disjoint from A.*

$$\forall A \; : \; \neg(A = \varnothing) \Rightarrow (\exists B \; : \; B \in A \wedge \neg(\exists C \; : \; C \in A \wedge C \in B))$$

Axiom C.8 (Axiom of Separation)**.** *Given any set A and any proposition $p(x)$, there is a subset of A containing precisely those x for which $p(x)$ is true.*

$$\forall A, \exists B, \forall C \; : \; C \in B \iff C \in A \wedge p(C).$$

Axiom C.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 C.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.*

NOTES May 20, 2006

Classes extending Sets: Derived from Morse-Kelly Set Theory

See web page http://en.wikipedia.org/wiki/Morse-Kelley_set_theory.

A convenient set of axioms for this theory (which entails choice in an amusing way, following von Neumann) is the following:

axiom of extensionality: classes with the same elements are the same.

axiom of class comprehension: for any formula f, there is a class whose elements are exactly those sets x such that f.

axiom of pairs: for any sets x and y, there is a set {x,y} whose elements are exactly x and y. In terms of these unordered pairs, we can define the usual Kuratowski ordered pair and use class comprehension to show that relations and functions on sets can be defined as usual, thus providing support for the following axiom.

axiom of limitation of size: a class C is a proper class iff there is a bijection between C and the class V of all sets.

axiom of power set: the class P(A) of all subsets of a set A is a set.

axiom of union: the class of all elements of elements of a set A is a set.

axiom of infinity: there is a set I which contains the empty set as an element and contains as an element for each element y of I.

axiom of foundation: Each nonempty class is disjoint from at least one of its elements.

Class is a primitive term; being an *element* of a class is a primitive relation. A *set* is a class which is an element of a class.

Axiom C.11. (Axiom of Class Extensionality)
Two classes are equal if and only if they have the same elements.

Axiom C.12. (Axiom of Class Comprehension)
Given any proposition $p(x)$, there is a class whose elements are precisely those sets x for which $p(x)$ is true.

Axiom C.13. (Axiom of Class Foundation)
Each nonempty class is disjoint from at least one of its elements.

Bibliography

[Ha60] Halmos, Paul R., *Naive Set Theory*, Undergraduate Texts in Mathematics, Springer-Verlag (1960,1974)

[St87] Stewart,James *Calculus*, 2$^{\text{nd}}$ edition, Brooks/Cole Publishing Company (1987,1991)