Basic Set Theory

To my wife, Sally, and our children,

Courtney, Rebecca, and Benjamin,

whose support made this book possible

David A. Smith

Basic Set Theory

That Anyone Can Understand

First Edition

Direct Knowledge

Cover photo attribution: *Southern Ring Nebula (NIRCam and MIRI Images Side by Side)* courtesy of NASA, ESA, CSA, STScI. Published on July 12, 2022. For more information visit: https://webbtelescope.org

ISBN: 978-1-951290-27-6

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Neither the Authors, nor the Publishers, nor the Editors give any warranty, express or implied, with respect to the material contained herein or for any any errors or omissions that may have been made.

Typeset with LaTeX and written in the United States of America.

David A. Smith
B.S. Mathematics, M.S. Mathematics
https://directknowledge.com

Direct Knowledge

Preface

Writing Philosophy

To be a successful writer, you must possess an inherent confidence and have something to say. You also need the capacity to think critically (and creatively) in order to create powerful arguments when conveying ideas; these are key elements necessary for writing mathematics clearly and effectively. Additionally, there are technical standards that I practice to ensure quality. I've specified my writing practices in detail; and you can find them online at https://directknowledge.com/writing

Acknowledgements

It is impossible to overstate the importance of those who helped bring this book into its completed form. I am deeply grateful for their generous contributions and would like to express my sincere appreciation.

David A. Smith \ Fort Worth, Texas

Table of contents

Chapter 1

Propositional Logic

Logic is the study of correct reasoning. It can be used to figure out whether an argument is valid, to find flaws in arguments, and to construct new arguments. In mathematics, logic is used to develop proofs – short, convincing arguments that something is true. A proof is like a puzzle: each piece (or step) fits together until the whole picture is complete.

By a **mathematical statement** (or **statement**, or **proposition**) we mean a declarative sentence that can be classified as either true or false, but not both. For example, the sentences

- $1 + 3 = 4$,
- $1 + 3 = 5$, and
- July is not a month

can be accepted as statements. The first one is true, and the second two are false. It is currently unknown whether or not the following statement (known as Goldbach's Conjecture) is true or false:

> Every even integer greater than 2 is the sum of two primes.

In either case, Goldbach's Conjecture is a mathematical statement.

Propositional logic is a system of reasoning that uses simple statements, called "propositions," to draw conclusions. For example, consider the following argument:

> All dogs are animals. Rover is a dog. Therefore, Rover is an animal.

This argument is valid because it follows the rules of propositional logic. The first two statements are called "premises," and the last statement is called the "conclusion."

We will define the following seven **logical connectives**:

$$\neg \quad \vee \quad \wedge \quad \rightarrow \quad \leftrightarrow \quad \downarrow \quad \uparrow$$

and in doing so, we will use these symbols to represent the follows words:

- $\neg$ for **not** or **negation**,
- $\vee$ for **and/or** or **disjunction**,
- $\wedge$ for **and** or **conjunction**,
- $\rightarrow$ for **implies** or **if ... then ...** ,
- $\leftrightarrow$ for **if and only if** or **equivalent**,
- $\downarrow$ for **joint negation** or **not both**, and
- $\uparrow$ for **alternative negation** or **neither nor**.

Informally, we say a statement is **simple** whenever it does not use one of the seven connectives. Examples of simple statements are:

- $3 + 4 = 7$
- Samuel is 46 years old.
- $3 + 4 = 8$
- The current month is December.
- It is raining.
- Right now it is 3 o'clock.

Statements that are made up of one or more simple statements using logical connectives are called **compound** statements.

The convention used here is that p or P may denote a statement. We use P sometimes to emphasis that P may be a compound statement.

Formally, compound statements are defined as follows.

1. All simple statements are compound statements.
2. If p and q are compound statements, then so are

$$\neg p \quad p \wedge q \quad p \vee q \quad p \rightarrow q \quad p \leftrightarrow q$$

3. Nothing else is a compound statement unless it can be obtained by a finite number of applications of statement (1) and (2) above.

For instance, the propositional variables for the statement $p \wedge (q \vee r)$ are p, q, and r. Using this definition one can prove that every statement can be decomposed into a finite number of simple statements in a unique way. For a given statement P, it's corresponding simple statements are called the **statement variables** (or **propositional variables**) of P.

We now consider each one of these connectives in turn, starting with the simplest first. As we do so, we illustrate truth values of statements, using **T** for true and **F** for false.

Table 1.1: The logical connective **Negation**

p	$\neg p$
T	F
F	T

Definition 1.1. The statement $\neg p$, read **not** p and called the **negation** of statement p, is defined to be the denial of statement p. That is, $\neg p$ is false if p is true, and $\neg p$ is true if p is false.

Basically, the **not** connective converts true to false and false to true.

Definition 1.2. The statement $p \wedge q$, read p **and** q and called the **conjunction** of p and q, is true when both p and q are true and is false otherwise.

Table 1.2: The logical connective **And**

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

Conjunction has the usually meaning of **and**, except that the two statements need not be related. Thus we state

$$1 + 4 = 5 \quad \text{and} \quad \text{July is a month}$$

as being a true conjunction. If we associate $1 + 4 = 5$ with the propositional variable p and **July is a month** with q, then we have the conjunction $p \wedge q$ which is easily seen to be true.

Definition 1.3. The statement $p \vee q$, read p **or** q and called the **disjunction** of p and q, is false when both p and q are false and is true otherwise.

Table 1.3: The logical connective **Or**

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

Disjunction is used logically in the inclusive **and/or** sense. The word disjunction, as written in Latin, is *vel.* and so we see that the symbol for disjunction, namely $\vee$, looks like its first letter in its Latin form. Now we see that

$$1 + 4 = 5 \quad \text{or} \quad \text{July is a month}$$

is a true disjunction; and that

$$0 + 4 = 5 \quad \text{or} \quad \text{July is a month}$$

is also a true disjunction.

Definition 1.4. The statement $p \to q$, read p **implies** q and called the **implication** (or **conditional** of p and q, is false when p is true and q is false, and is true otherwise.

Table 1.4: The logical connective **Implication**

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

In any implication $p \to q$, p is called the **hypothesis** (or **antecedent** or **premise**) and q is called the **consequence** (or **conclusion**.

Notice that an implication $p \to q$ is true when both p and q are true, and is false only in the case that p is true and q is false, and when p is false (no matter what truth value q has) the implication is true. This way of defining implication is more general than the meaning used in everyday English.

For example, the implication

If it is cloudy today, then we will not go back to the beach.

is an implication used in normal language, since there is a relationship between the hypotheses and the conclusion. On the other hand, the implication

$$\text{If today is Monday, then } 1+4=6.$$

is true every day except Monday, from the definition of implication.

Using words and symbols is the usual approach the everyday mathematics. Here are some common ways to express the conditional $p \to q$.

- p implies q
- if p then q
- if p, q
- q, if p
- p only if q
- p is sufficient for q
- q is necessary for p
- whenever p, q
- q whenever p

Definition 1.5. The statement $p \leftrightarrow q$, read p **if and only if** q and called the **equivalence** (or **biconditional**) of p and q, is true if and only if p and q are true or both are false.

Table 1.5: The logical connective **Biconditional**

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Note that the biconditional $p \leftrightarrow q$ is true precisely when both implications $q \to p$ and $p \to q$ are true. Here are some common ways to express the biconditional $p \leftrightarrow q$.

- p if and only if q,
- p is necessary and sufficient for q,
- p is equivalent to q, and
- p and q are equivalent.

As a summary of the truth tables for the logical connectives see Table 1.6.

The connectives $\downarrow$ and $\uparrow$ will be explored in the exercises.

Table 1.6: Summary of logical connectives

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$	$p \uparrow q$	$p \downarrow q$
T	T	T	T	T	T	F	F
T	F	F	T	F	F	T	F
F	T	F	T	T	F	T	F
F	F	F	F	T	T	T	T

1.1 Constructing Truth Tables

From the point of view of logic, it is the structure of a compound statement that makes it important. When constructing the truth table of a statement we will take into account this structure by parsing a statement into simpler statements.

Table 1.7: Truth table conventions

p	q	r
T	T	T
T	T	F
T	F	T
T	F	F
F	T	T
F	T	F
F	F	T
F	F	F

When constructing compound statements, parentheses are used to specify the order in which the various logical connectives in a compound statement are applied. In particular, the logical connectives in the innermost parentheses are applied first. For example, $(p \wedge q) \vee (\neg r)$ is the disjunction of $(p \wedge q)$ and $\neg r$. To cut down on the number of parentheses used, we specify that the negation connective is applied before all other connectives. For instance, $\neg p \vee q$ is the disjunction of $\neg p$ and q, namely $(\neg p) \vee q$, not the negation of the conjunction of p and q. Further, when working with compound propositions the order from highest priority to lowest is $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.

We agree that, in any truth table, the symbols for the propositional variables $p, q, r, ...$ are in alphabetical order, and to make the rightmost column $T, F, T, F, ...$ the next column leftward $T, T, F, F, ...$, and so forth. As examples of this convention see Table 1.6 and Table 1.7.

1.2 Tautologies, Contradictions, and Contingencies

We sometimes classify statements according to whether or not they are always true, always false, or otherwise.

Definition 1.6. A proposition that is always true, regardless of what truth values are assigned to its statement variables, is called a **tautology**; a proposition that is always false, regardless of what truth values are assigned to its statement variables, is called a **contradiction**; and otherwise a proposition is called a **contingency**.

Example 1.1. Determine whether or not the statement

$$(p \to (q \wedge p)) \vee (q \to (p \wedge q))$$

is a tautology.

Solution. We begin by parsing the statement $(p \to (q \wedge p)) \vee (q \to (p \wedge q))$ into simpler forms, namely, $q \wedge p$, $p \to (q \wedge p)$, and $q \to (p \wedge q)$. We place these simpler forms into three columns in the table to aid in the computation of the values in the final column. The following truth table Table 1.8 shows that the statement $(p \to (q \wedge p)) \vee (q \to (p \wedge q))$ is a tautology because every entry in the last column is true. More precisely, regardless of what truth values are assigned to its statement variables, $(p \to (q \wedge p)) \vee (q \to (p \wedge q))$ has a true truth value.

Table 1.8: Example of a **tautology**

p	q	$q \wedge p$	$p \to (q \wedge p)$	$q \to (p \wedge q)$	$(p \to (q \wedge p)) \vee (q \to (p \wedge q))$
T	T	T	T	T	T
T	F	F	F	T	T
F	T	F	T	F	T
F	F	F	T	T	T

In general if a proposition contains n variables then it takes 2^n rows to determine whether a proposition is a tautology or not. The problem of determining whether any given proposition is a tautology is called the **tautology problem**.

> Is there a better way to solve the tautology problem than the brute force method of a truth table?

We now list several important tautologies, leaving their proofs for the reader as exercises. Each of the names of the tautologies are listed also. It is important to know their names as well, as tautologies are usually referred to by name.

Theorem 1.1 (Tautologies Used in Proofs)**.** *The following statements are tautologies.*

Statement	*Name*
$p \vee \neg p$	***excluded middle***
$(p \wedge q) \to p$	***simplification***
$p \to (p \vee q)$	***construction***
$((p \vee q) \wedge \neg p) \to q$	***syllogism***
$(p \wedge (p \to q)) \to q$	***modus ponens***
$(\neg q \wedge (p \to q)) \to \neg p$	***modus tollens***
$(p \to q) \leftrightarrow (\neg p \vee q)$	***conditional disjunction***
$(p \to q) \leftrightarrow (\neg q \to \neg p)$	***contrapositive***
$((p \to r) \wedge (q \to r)) \leftrightarrow ((p \vee q) \to r)$	***proof by cases***
$(p \to (q \wedge \neg q)) \leftrightarrow \neg p$	***indirect proof***

Proof. The proof is left for the reader as Exercise 1.7.

□

Theorem 1.2 (Order Related Tautologies)**.** *The following statements are tautologies.*

Statement	*Name*
$p \to p$	***reflexive***
$((p \to q) \wedge (q \to r)) \to (p \to r)$	***transitivity***
$((p \leftrightarrow q) \wedge (q \leftrightarrow r)) \to (p \leftrightarrow r)$	***transitivity***

Proof. The proof is left for the reader as Exercise 1.10.

□

1.3 Contrapositive, Converse, and Inverse

Three important statements are associated with any implication $p \to q$, namely

- the statement $\neg q \to \neg p$ is called the **contrapositive** of $p \to q$,

- the statement $q \to p$ is called the **converse** of $p \to q$, and
- the statement $\neg p \to \neg q$ is called the **inverse** of the implication $p \to q$.

It is easy to show that every implication is logically equivalent to its contrapositive. Try it. Notice that the inverse and converse of $p \to q$ are logically equivalent.

p	q	$\neg p$	$\neg q$	$\neg p \to \neg q$	$q \to p$
T	T	F	F	T	T
T	F	F	T	T	T
F	T	T	F	F	F
F	F	T	T	T	T

Further, an implication is not necessarily equivalent to its converse (inverse).

1.4 Modus Ponens and Substitution

In propositional logic, modus ponendo ponens (or *modus ponens*), which is Latin for **the way that affirms by affirming**, is a valid, simple argument form and rule of inference.

Theorem 1.3 (Modus Ponens)**.** *Let P and Q be statements. If the statements P and $P \to Q$ are tautologies, then so is the statement Q.*

Proof. Suppose the statements P and $P \to Q$ are tautologies. Assume for a contradiction that Q is not a tautology. Then it must be possible to have a truth assignment to the statement variables of Q which yields false.

However, since P is a tautology and $P \to Q$ is a tautology, we now have a truth assignment of $P \to Q$ which yields false. Yet all truth assignments for $P \to Q$ yield true. This contradiction shows that the hypothesis that Q is not a tautology can not hold. Therefore Q must be a tautology.

□

Theorem 1.4 (Substitution Rule)**.** *Let P be a tautology, and suppose that P contains the distinct statement variables $p_1, p_2, \ldots, p_n$ (and perhaps others as well). Suppose further that $Q_1, Q_2, \ldots, Q_n$ are statements. Then, if in the tautology P, we replace p_1 by Q_1, replace p_2 by Q_2, and so on, then the resulting statement is also a tautology.*

Proof. This proof is left as Exercise 1.22.

□

Example 1.2. Show that the statement

$$(p \wedge \neg q) \rightarrow [(\neg p \vee \neg q) \rightarrow (p \wedge \neg q)] \tag{1.1}$$

is a tautology.

Solution. Notice the compound statement in (1.1) has the form

$$P \rightarrow (Q \rightarrow P) \tag{1.2}$$

where $P := p \wedge \neg q$ and $Q := \neg p \vee \neg q$. Therefore, by Theorem 1.4, it suffices to verify that (1.2) is in fact a tautology. We leave this verification to the reader.

Example 1.3. Show that the statement

$$(p \rightarrow \neg q) \vee \neg(p \rightarrow \neg q) \tag{1.3}$$

is a tautology.

Solution. It is easy to see that the statement $P \vee \neg P$ is a tautology; and thus by Theorem 1.4, we see that (1.3) is also a tautology.

1.5 Inference Rules

By a **mathematical proof** (or **proof**) we shall mean the assertion that a certain statement (the **conclusion**) follows from other statements (the **premises**). A proof will be said to be (logically) **valid**, if and only if the conjunction of the premises implies the conclusion, that is, if the premises are all true, the conclusion **must** also be true. In order to determine whether a mathematical proof is valid we need to be able to accomplish two goals: a valid **logically argument** and **justifications** for each statement.

It's important to realize that a logically argument depends upon its form in that it does not matter what the components of the argument are. For example, is the following argument valid?

$$\text{If } p \rightarrow q \text{ and } q \rightarrow r, \text{ then } p \rightarrow r. \tag{1.4}$$

Since the implication $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ is a tautology, (1.4) is a valid argument, as can be proven by constructing a truth table. Indeed

(1.4) is valid as an argument regardless of the meaning of p, q and r. A proof demonstrates that the conclusion must happen and is a consequence of the premises.

Theorem 1.5. *Suppose the statement r is a consequence of the premises $p_1, p_2, ...p_k$ and also suppose another statement q is a consequence of the same premises $p_1, p_2, ..., p_k$ and r. Then q is a consequence of just $p_1, p_2, ..., p_k$.*

Proof. Let P_k denote $p_1 \wedge \cdots \wedge p_k$. For a rigorous proof we need to show that

$$((P_k \to r) \wedge (P_k \wedge r \to q)) \to (P_k \to q) \tag{1.5}$$

is a tautology. To understand why (1.5) is a tautology, let p be the variable for $p_1 \wedge p_2 \wedge \cdots \wedge p_k$ and consider the truth table for $p \to q$. In any row where p is false, $p \to q$ is true by definition of →. In any row where p is true, r must also be true, since $p \to r$ is a tautology. But since $(p \wedge r) \to q$ is always true, this guarantees that in every row where p is true, q must also be true. Therefore, $p \to q$ is a tautology, as desired.

□

Before we begin writing proofs, let's review the following tautologies.

Inference Rule	Tautology	Name
p $\therefore p \vee q$	$p \to (p \vee q)$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Simplification
p q $\therefore p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
p $p \to q$ $\therefore q$	$[p \wedge (p \to q)] \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$[\neg q \wedge (p \to q)] \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Hypothetical syllogism

Inference Rule	Tautology	Name
$p \vee q$ $\neg p$ $\therefore q$	$[(p \vee q) \wedge \neg p] \to q$	Disjunctive syllogism

1.6 Logical Equivalence

In propositional logic, statements p and q are logically equivalent if they have the same semantic meaning. In other words, two statements are equivalent if they have the same truth value for every possible assignment.

Another way to say this is the following: for each assignment of truth values to the simple statements which make up P and Q, the statements P and Q have identical truth values. We will see that, from a practical point of view, we can replace a variable in a tautology by any logically equivalent statement and still have a tautology.

Definition 1.7. Let P and Q be statements. We say that P is **logically equivalent** to Q, denoted by $P \equiv Q$, provided that P and Q have the same truth-value for every possible choice of truth values of the propositional variables involved in P and Q.

Example 1.4. Verify the following are logical equivalencies:

1. $p \to q \equiv \neg p \vee q$
2. $\neg(p \to q) \equiv p \wedge \neg q$

Solution. The following truth table clearly demonstrates that $p \to q$ and $\neg p \vee q$ are logically equivalent (columns 5 & 6).

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

It also shows that $\neg(p \to q)$ and $p \wedge \neg q$ are logically equivalent (columns 7 & 8).

There are, of course, an infinite number of tautologies and logical equivalences. However, as we have seen, the method of truth tables is exponential in the number of variables. Thus we need practical methods of determining whether a given statement is a tautology or whether two given statements are logical equivalent or not.

Theorem 1.6 (Logical Equivalence)**.** *Two compound statements P and Q are logically equivalent if and only if the compound statement $P \leftrightarrow Q$ is a tautology.*

Proof. If $P \leftrightarrow Q$ is a tautology, then any assignment of truth values to the statement variables makes the statement $P \leftrightarrow Q$ true, that is, it gives the same truth values to both P and Q. Therefore, P and Q are logically equivalent.

Conversely, if P and Q are logically equivalent, then any assignment of truth values to the statement variables of P and Q gives the same truth value to both P and Q. Whence $P \leftrightarrow Q$ is a tautology.

□

Theorem 1.7 (Properties of Logical Equivalence)**.** *Let p and q be statements.*

- *The* ***commutative*** *properties:*
  - $(p \wedge q) \equiv (q \wedge p)$
  - $(p \vee q) \equiv (q \vee p)$
- *The* ***associative*** *properties:*
  - $((p \wedge q) \wedge r) \equiv (p \wedge (q \wedge r))$
  - $((p \vee q) \vee r) \equiv (p \vee (q \vee r))$
- *The* ***distributive*** *properties:*
  - $(p \wedge (q \vee r)) \equiv ((p \wedge q) \vee (p \wedge r))$
  - $(p \vee (q \wedge r)) \equiv ((p \vee q) \wedge (p \vee r))$
- *The* ***idempotent*** *properties:*
  - $p \vee p \equiv p$
  - $p \wedge p \equiv p$
- ***De Morgan*** *laws:*
  - $\neg(p \wedge q) \equiv \neg p \vee \neg q$
  - $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- ***Law of excluded middle:***
  - $p \vee \neg p$ *is a tautology*
  - $p \wedge \neg p$ *is a contradiction*

Proof. The proof is left for the reader as Exercise 1.8.

□

Theorem 1.8 (Properties of Logical Equivalence II)**.** *Let p and q be statements.*

- *An implication and contrapositive are logically equivalent:*

$$p \to q \equiv \neg p \to \neg q.$$

- *The converse and inverse of the implication $p \to q$ are logically equivalent:*

$$q \to p \equiv \neg q \to \neg p.$$

- *Let T denote a tautology and F denote a contradiction. Then*
    - $p \vee T \equiv T$
    - $p \wedge T \equiv p$
    - $p \vee F \equiv p$
    - $p \wedge F \equiv F$

Proof. The proof is left for the reader as Exercise 1.9.

□

Theorem 1.9 (Logical Equivalence/Substituton)**.** *Let P and Q be logically equivalent statements, and suppose that P and Q contain the statement variables $p_1, p_2, \ldots, p_n$ (and possible others). Suppose further that $Q_1, Q_2, \ldots, Q_n$ are statements. Then, if we replace p_1 by Q_1, replace p_2 by Q_2, and so on, in both P and Q, then the resulting statements are still logically equivalent.*

Proof. Denote the statements obtained by replacing p_1 by Q_1, p_2 by Q_2, and so on, in P and Q by P' and Q', respectively. We will show that P' and Q' are logically equivalent. By Theorem 1.6, P' and Q' are logically equivalent if and only if the statement $P' \leftrightarrow Q'$ is a tautology. Now since our hypothesis is that P and Q are logically equivalent we know that $P \leftrightarrow Q$ is a tautology, also by Theorem 1.6. Therefore, by Theorem 1.4} we see that $P' \leftrightarrow Q'$ is a tautology as needed.

□

Example 1.5. Use properties of logical equivalence to show that

$$\neg(p \leftrightarrow q) \equiv \neg q \leftrightarrow p \tag{1.6}$$

is a tautology.

Solution. We apply the properties of logical equivalence as follows:

$$\begin{aligned}
\neg(p \leftrightarrow q) &\equiv \neg[(p \to q) \wedge (q \to p)] \\
&\equiv \neg(p \to q) \vee \neg(q \to p) \\
&\equiv (p \wedge \neg q) \vee (q \wedge \neg p) \\
&\equiv [(p \wedge \neg q) \vee q] \wedge [(p \wedge \neg q) \vee \neg p] \\
&\equiv [(p \vee q) \wedge (\neg q \vee q)] \wedge [(p \vee \neg p) \wedge (\neg q \vee \neg p)] \\
&\equiv [(p \vee q) \wedge T] \wedge [T \wedge (\neg q \vee \neg p)] \\
&\equiv (p \vee q) \wedge (\neg q \vee \neg p) \\
&\equiv (q \vee p) \wedge (\neg p \vee \neg q) \\
&\equiv (\neg q \to p) \wedge (p \to \neg q) \\
&\equiv \neg q \leftrightarrow p
\end{aligned}$$

1.7 Exercises

Exercise 1.1. Consider the following statement:

If $x = 0$, then $x^2 = 0$ and if $x^2 = 0$, then $x = 0$.

1. Express this statement in symbolic form using only conjunction and conditional.
2. Express this statement in symbolic form using only biconditional.

Exercise 1.2. Rewrite each statement in the form **If ..., then ...**.

1. A nessary condition for two triangles to be congruent is that three sides of one be equal respectively to the three sides of the other.
2. A sufficient condition for two triangles to be congruent is that the three sides of one be equal respectively to the three sides of the other.
3. The base angles of an isosceles triangle are equal.

Exercise 1.3. Construct a truth table and identify whether the proposition is either a tautology, contradiction, or a contingency.

1. $(p \wedge q) \rightarrow (p \vee q)$
2. $(p \vee q) \vee (p \rightarrow q)$
3. $(p \rightarrow q) \vee (p \wedge \neg q)$
4. $(\neg p \wedge q) \wedge \neg(p \rightarrow \neg q)$
5. $\neg(p \vee q) \wedge \neg(p \rightarrow q)$
6. $(p \wedge q) \wedge \neg(p \vee \neg q)$
7. $((p \wedge q) \vee r) \rightarrow \neg q$
8. $((r \wedge q) \vee p) \rightarrow \neg q$

Exercise 1.4. Show the following statements are contingencies.

1. $(p \wedge q) \wedge (p \rightarrow q)$
2. $((p \wedge q) \rightarrow (p \vee q)) \rightarrow p \wedge q$

Exercise 1.5. Find a tautology that contains the statement $p \wedge (q \rightarrow \neg p)$. Find a contingency that contains the statement $(p \wedge q) \wedge (p \vee \neg q)$. Find a contradiction that contains the statement $p \wedge (p \wedge \neg q)$.

Exercise 1.6. Construct truth tables for each of the following and arrange them so that each compound statement implies all the following ones.

1. $\neg p \leftrightarrow q$
2. $p \rightarrow (\neg p \rightarrow q)$
3. $\neg (p \rightarrow (q \rightarrow p))$
4. $p \vee q$
5. $\neg p \wedge q$

Exercise 1.7. Prove Theorem 1.1.

Exercise 1.8. Prove Theorem 1.7.

Exercise 1.9. Prove Theorem 1.8.

Exercise 1.10. Prove Theorem 1.2.

Exercise 1.11. First explain why all propositional forms with just one variable are logically equivalent with one of the following four: P or $\neg P$ or $P \vee \neg P$ or $P \wedge \neg P$. Now do the following:

1. Explain why all propositional forms with two variables are logically equivalent with 1 of 16 possibilities.
2. Using only $\vee$ and $\wedge$, together with the variables P and Q, give examples of all 16 possibilities in part (b), using the fewest number of symbols.
3. Find a formula for the number of logically nonequivalent types of propositional forms of three variables.
4. Repeat with n variables.
5. Explain why your formulas are correct.
6. Explain how to rewrite all of the possibilities in part (c), using only $\vee$ and $\neg$. Repeat using only $\wedge$ and $\neg$.

Exercise 1.12. Write the converse, contrapositive, and inverse of each statement. Further, determine whether the given statement and/or its converse is true.

1. If $x \neq 0$, then $x^2 \neq 0$.
2. If $xy = 0$, then $x = 0$
3. If x is a real number, then x is a rational number.
4. If x is positive and $x^2 = 4$, then $x = 2$.
5. If $x \neq 2$ and $x^2 + 3x + 1 = 0$, then $x = 1$.
6. If n is an even integer or a prime number, then n is not an even nonnegative integer.

A collection of logical connectives is called **functionally complete** if every compound statement is logically equivalent to a compound statement involving only these logical connectives.

Exercise 1.13. Show that $\neg$, $\vee$, and $\wedge$ form a functionally complete collection of logical connectives.

Exercise 1.14. Show that $\neg$ and $\vee$ form a functionally complete collection of logical connectives.

Exercise 1.15. Show that $\neg$ and $\wedge$ form a functionally complete collection of logical connectives.

Exercise 1.16. In this exercise we will show that $\uparrow$ forms a functionally complete collection of logical connectives.

1. Show that $p \downarrow p$ is logically equivalent to $\neg p$.
2. Show that $(p \downarrow q) \downarrow (p \downarrow q)$ is logically equivalent to $p \vee q$.
3. Explain how Exercise 1.14 applies.

Exercise 1.17. Show that $\neg$ and $\rightarrow$ form a functionally complete collection of logical connectives.

Exercise 1.18. Show that the five connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ can each be defined in terms of only $\uparrow$. Do the same as (a) with $\downarrow$.

Exercise 1.19. Prove that if P is logically equivalent to Q, and Q is logically equivalent to R, then P is logically equivalent to R.

Exercise 1.20. Use Exercise 1.19, to prove that any two of the following three statements are logically equivalent.

1. $p \rightarrow q$
2. $(p \wedge \neg q) \rightarrow \neg p$
3. $(p \wedge \neg q) \rightarrow q$

Exercise 1.21. Use Theorem 1.9 to prove the logical equivalences.

1. $\neg[(p \leftrightarrow q) \vee (p \wedge \neg q)] \equiv \neg(p \leftrightarrow q) \wedge \neg(p \wedge \neg q)$
2. $(p \vee q) \rightarrow (p \wedge q) \equiv [((p \vee q) \wedge \neg(p \wedge q)) \rightarrow \neg(p \vee q)]$
3. $(r \wedge \neg p) \wedge ((r \wedge \neg p) \vee (p \wedge \neg q)) \equiv r \wedge \neg p$
4. $(p \wedge r) \wedge ((p \rightarrow q) \vee r) \equiv [(p \wedge r) \wedge (p \rightarrow q)] \vee [(p \wedge r) \wedge r]$

Exercise 1.22. Prove Theorem 1.4.

Chapter 2

Predicate Logic

Predicate logic is a more powerful system of reasoning that can be used to express more complicated ideas. In predicate logic, we can make statements about things that have certain properties. For example, consider the following argument:

> Every animal that is a mammal has fur. Rover is a mammal. Therefore, Rover has fur.

This argument is also valid because it follows the rules of predicate logic. In this case, the first statement is called the "universal quantifier," the second statement is the "existential quantifier," and the last statement is the "conclusion."

Variables in mathematical statements can be quantified in different ways. First, the symbol $\forall$ is called a **universal quantifier** and is used to express that a variable may take on any value in a given collection. For example, $\forall x$ is a symbolic representation for any of the following

- For any x, ...
- For every x, ...
- For all x, ...
- Given any x, ...
- If x is any ...

Another quantifier $\exists$ is called an **existential quantifier** and is used to express that a variable can take on at least one value in a given collection. For example $\exists x$ is a symbolic representation for any of the following

- For some x, ...

- There exists an x, ...
- There is an x, ...
- There are x, ...

Mathematical statements are sometimes written with hidden quantifiers and so you may want to rephrase a given statement before writing it in symbolic form or before applying a logic rule. For example, what are the hidden quantifiers in the following statement?

> In 1941, Joe Dimaggio had a 56-game hitting streak.

Namely,

> In 1941, there existed a sequence of 56 consecutive games, such that for all games in this sequence, there was at least one at-bat in which Joe Dimaggio got a hit.

In this section, we discuss quantified statements and logic rules for working with them. Here are some examples of logic rules.

- **Logic Rule 1**: The negation of the statement:
$$\forall\, x, P(x)$$
is the statement
$$\exists\, x, \neg P(x)$$
- **Logic Rule 2**: The negation of the statement:
$$\exists\, x, P(x)$$
is the statement
$$\forall\, x, \neg P(x)$$

Before we discuss quantifiers in detail, let's first understand what $P(x)$ means.

Notice that the statement

> x is less than 5

has two parts. The first is the variable x which is the subject of the statement. The second part, **is less than 5** is called the **predicate** and refers to a property that the subject of the statement can have. We denote the statement "x is less than 5" by $P(x)$, where P denotes the predicate and x is the variable. Once a value as been assigned to the variable x, the sentence $P(x)$ becomes a proposition and has a truth value. For instance, what are the truth values of $P(1)$ and $P(2)$?

Definition 2.1. A **propositional function** in the variable x is a sentence $P(x)$ about x that becomes a statement when x is given a particular value.

In general, a sentence involving the n variables $x_1, x_2, \dots, x_n$ is denoted by

$$P(x_1, x_2, \dots, x_n).$$

A statement of the form $P(a_1, a_2, \dots, a_n)$ is the value of the **propositional function** P at the n-tuple $(a_1, a_2, \dots, a_n)$ and P is called the **predicate**.

Example 2.1. Let $P(x, y, z)$ denote the sentence "$x - y = z$". What are the truth values of the propositions $P(2, 3, -1)$ and $P(5, 0, 7)$?

Solution. The statement $P(2, 3, -1)$ corresponds to $2 - 3 = -1$ which is true; and the statement $P(5, 0, 7)$ corresponds to $5 - 0 = 7$ which is false.

2.1 Universal Quantifier

Definition 2.2. The statement

$$\text{For all } x,\ P(x).$$

is symbolized by the formula

$$\forall x, P(x).$$

The symbol $\forall$ is called an **universal quantifier** and translates as "for all".

Is this statement true or false?

Example 2.2. Express the statement

> Every student in this class has studied calculus. as a universal quantification.

Solution. Let $P(x)$ denote the statement: "x has studied calculus". Then the statement can be written $\forall\, x, P(x)$ where the universe of discourse is the set of students in this class.

Example 2.3. Let $P(x)$ be the statement "$x > 3$". What is the truth value of the quantification $\forall x, P(x)$, where the universe of discourse is the set of real numbers?

Solution. Notice that $P(x)$ is not true for all real numbers x, since we can find one value in the universe of discourse, say 2, and $P(2)$ is false. Consequently $\forall x, P(x)$ is false.

When the universe of discourse is finite, say $x_1, x_2, \dots, x_n$, then the universal quantification $\forall x, P(x)$ has the same truth value as the conjunction

$$P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n) \tag{2.1}$$

since $P(x_1)$, $P(x_2)$, ..., $P(x_n)$ are all true if and only if the conjunction is true.

Example 2.4. What is the truth value of the statement $\forall x, P(x)$ where $P(x)$ is the statement

$x^2 < 5$

and the universe of discourse is the set of the negative integers not less than -3?

Solution. The statement $\forall x, P(x)$ is the same as the conjunction

$$P(-3) \wedge P(-2) \wedge P(-1)$$

since the universe of discourse consists of the integers $-3, -2$, and -1. Since $P(-3)$ is false, it follows that the statement $\forall x, P(x)$ is false.

2.2 Existential Quantifier

Definition 2.3. The statement

There exists an x such that $P(x)$.

is symbolized by the formula

$$\exists x, P(x).$$

The symbol $\exists$ is called an **existential quantifier** and translates as “there exists”.

Notice that P(1) is also true and that 1 is a rational number.

Example 2.5. Let $P(x)$ denote the statement

$x < 5$

What is the truth value of the quantification $\exists x, P(x)$, where the universe of discourse is the set of rational numbers?

Solution. In order for the statement $\exists x, P(x)$ to be true, we need to demonstrate at least one value x in the universe of discourse where $P(x)$ is true. Since 2 is a rational number number and $P(2)$ is true, we see that $\exists x, P(x)$ is true.

What if we change the universe of discourse to the set of complex numbers?

Example 2.6. Let $P(x)$ be the statement

$$x^2 = -1$$

What is the truth value of the quantification $\exists x, P(x)$, where the universe of discourse is the set of rational numbers?

Solution. Since $x^2 = -1$ is false for every rational number x, the existential quantification of $P(x)$, namely $\exists x, P(x)$ is false.

When the universe of discourse is finite, say $x_1, x_2, \dots, x_n$, then the existential quantification $\exists x, P(x)$ has the same truth value as the disjunction

$$P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n) \tag{2.2}$$

since at least one of $P(x_1)$, $P(x_2)$, ..., $P(x_n)$ is true if and only if the disjunction is true.

Example 2.7. What is the truth value of $\exists x, P(x)$ where $P(x)$ is the statement

$$x^4 < 1$$

and the universe of discourse consists of the negative integers not less than -5?

Solution. Since the universe of discourse is $\{-5, -4, -3, -2, -1\}$, the proposition $\exists x, P(x)$ is the same as the disjunction

$$P(-5) \vee P(-4) \vee P(-3) \vee P(-2) \vee P(-1).$$

Since $P(-5), P(-4), P(-3), P(-2)$, and $P(-1)$ are all false, it follows that the statement $\exists x, P(x)$ is false.

2.3 Uniqueness Quantifier

What are other ways of expressing his quantifier in English?

Definition 2.4. The statement

There exists a unique x such that $P(x)$.

is symbolized by the formula

$$\exists!\, x, P(x).$$

The symbol $\exists!$ is called an **uniqueness quantifier** and translates as "there exists a unique".

Example 2.8. What is the truth value of $\exists!\, x, P(x)$ where $P(x)$ is the statement

$x^4 \leq 1$"

and the universe of discourse consists of the negative integers not less than -5?

Solution. The universe of discourse is the set $\{-5, -4, -3, -2, -1\}$ and since $P(-5), P(-4), P(-3), P(-2)$ are all false and $P(-1)$ is true, we see that exactly one, namely $P(-1)$ is true. Hence, it follows that the statement $\exists!\, x, P(x)$ is true.

2.4 Negating Quantifiers

Now we discuss the two logic rules mentioned above.

Theorem 2.1 (Negating Quantifiers). *Let $P(x)$ be a propositional function and let A be a set. Then,*

1. $\neg[\forall x \in A, P(x)]$ *is a true proposition if and only if* $\exists x \in A, \neg P(x)$ *is a true proposition.*
2. $\neg[\exists x \in A, P(x)]$ *is a true proposition if and only if* $\forall x \in A, \neg P(x)$ *is a true proposition.*

Proof. We prove (2) and leave the first part as Exercise 2.7. Suppose that

$$\neg[\exists x \in A, P(x)]$$

is a true proposition. Then there is no x in A such that $P(x)$ is true. Thus, for each $x \in A$, $P(x)$ is false. Therefore, $\neg P(x)$ is true for every x in the set A, and so $\forall x \in A, \neg P(x)$ is a true proposition.

Conversely, assume that $\forall x \in A, \neg P(x)$ is a true proposition. Then $\neg P(x)$ is a true statement for every x in the set A. So $P(x)$ is false for every

x in the set A; that is, there does not exist an element x of the set A such that $P(x)$ is true. Therefore, we see that $\neg[\exists x \in A, P(x)]$ is a true proposition.

□

Example 2.9. Write the negation of the statements

1. $\forall\, n \in \mathbb{N}, n^2 - n + 3 = 0$
2. $\exists\, n \in \mathbb{N}, n^2 - n + 3 = 0,$

and for each one, explain whether it or its negation is true.

Solution. By Theorem 2.1,

$$\forall\, n \in \mathbb{N}, n^2 - n + 3 = 0 \quad \text{has negation:} \quad \exists\, n \in \mathbb{N}, n^2 - n + 3 \neq 0$$

and

$$\exists\, n \in \mathbb{N}, n^2 - n + 3 = 0 \quad \text{has negation:} \quad \forall\, n \in \mathbb{N}, n^2 - n + 3 \neq 0 \quad (2.3)$$

The first statement $\forall\, n \in \mathbb{N}, n^2 - n + 3 = 0$ is not true simply note that when $n = 2$, then $(2)^2 - (2) + 3 = 5 \neq 0$. Therefore its negation must be true. The second statement $\exists\, n \in \mathbb{N}, n^2 - n + 3 = 0$ is false since there does not exist $n \in \mathbb{N}$ such that $n^2 - n + 3 = 0$.

Example 2.10. Write the negation of the statement

$$\exists!\, n \in \mathbb{N}, n^2 - n + 3 = 0.$$

Solution. We want to write negation of the statement

There is one and only one $n \in \mathbb{N}$ such that $n^2 - n + 3 = 0$.

The negation is "There is no $n \in \mathbb{N}$ such that $n^2 - n + 3 = 0$ or there is more than one $n \in \mathbb{N}$ such that $n^2 - n + 3 = 0$". Another way of saying this is "For each $n \in \mathbb{N}$, $n^2 - n + 3 \neq 0$ or there exists at least two natural numbers n such that $n^2 - n + 3 = 0$."

2.5 Counterexamples

How can we show that a statement of the form $\forall x, P(x)$ is false? Or equivalently, how can we show that the negation of $\forall x, P(x)$ is true? By Theorem 2.1, this simply means we need to show that $\exists x, \neg P(x)$ is true. If we can find a value for x such that $\neg P(x)$ is true, then we have a ounterexample and have shown that $\forall x, P(x)$ is false. Intuitively for example, suppose that P is the predicate "is wearing a red shirt", then a counterexample to the statement "everyone is wearing a red shirt" is the statement "found someone, not wearing a red shirt".

Definition 2.5. If $P(x)$ is a propositional function and x is a member of the set A, then a **counterexample** to $\forall x \in A, P(x)$ is a member c of the set A such that $P(c)$ is false.

Example 2.11. Show that the statement "All primes are odd" is false.

Solution. The statement "All primes are odd" is written in universal quantification form as $\forall x, P(x)$ where p is the predicate "is odd" and the universe of discourse is the set of primes. It is easy to see that 2 is a counterexample because 2 is in the domain of discourse and is not prime.

2.6 Combining Quantifiers

Of course quantifiers can be nested, that is, it is possible to have a statement involving several quantifiers. Consider the following two statements:

1. There exists an integer x such that for every integer y, $x + y = 5$.
2. For every integer y there exists an integer x such that $x + y = 5$.

These statements represented in symbolic form are, respectively,

1. $\exists x \in \mathbb{Z}, [\forall y \in \mathbb{Z}, (x + y = 5)]$
2. $\forall x \in \mathbb{Z}, [\exists y \in \mathbb{Z}, (x + y = 5)]$

These statements have very different meanings. In order for statement (1)), to be true we need to demonstrate at least one x such that for any given y (in the domain of discourse) that $x + y = 5$ is true. Since we can not specify an integer x such that $x + y = 5$ is true for all integers y we see that statement (1) is false.

In order for (2) to be true, we need to be able to specify an integer y once a given integer x has been specified, such that $x + y = 5$ is true. For example, if $x = 3$, then $y = 2$, then $3 + 2 + 5$ is true. However this is just one value for x, in order for (2) to be true, we need to specify an integer y *for any given integer* x. We can specify an integer y when x is given just use $y = 5 - x$. Since, if we are given an integer x, we know that $y = 5 - x$ is also an integer and $x + y = x + (5 - x) = 5$. Thus we see that statement (2) is true.

The reader is encourage to practice writing out the negation of the definition of a limit.

Example 2.12 (Definition of Limit)**.** Recall from calculus, that the definition of a limit of a real-valued function is:

> For every real number $\epsilon > 0$ there exists a real number $\delta > 0$ such that $|f(x) - L| < \epsilon$ whenever $0 < |x - a| < \delta$.

Express the definition of a limit using quantifiers.

Solution. This definition of limit can be phrased in term of quantifiers by

$$\forall \epsilon, \exists \delta, \forall x, (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon)$$

where the universe of discourse for the variables ϵ and δ is the set of positive real numbers and for x is the set of real numbers.

Example 2.13. Find the negation of the statement

$$\exists x \in \mathbb{N}, \forall y \in \mathbb{N}, (xy = y) \tag{2.4}$$

Solution. This statement has the form

$$\exists x, [\forall y, P(x, y)]$$

where $P(x, y)$ represents the propositional function $xy = y$. We find the negation to be:

$$\begin{aligned} \neg[\exists x, [\forall y, P(x, y)]] &\equiv \forall x, [\neg[\forall y, P(x, y)]] \\ &\equiv \forall x, [\exists y, [\neg P(x, y)] \end{aligned}$$

So the negation of (2.4) is

$$\forall x \in \mathbb{N}, [\exists y \in N, (xy \neq y)].$$

The next example uses the logical equivalence $p \rightarrow q \equiv p \wedge \neg q$ and DeMorgan's Law.

Example 2.14. Find the negation of the statement

$$\forall x, \forall y, [x < y \rightarrow \exists z, (x < z \wedge z < y)] \tag{2.5}$$

If the domain of discourse for x, y and z is $\mathbb{R}$, then is this statement true or false?

Solution. This statement has the form

$$\forall x, \forall y, [P(x,y) \to \exists z, [Q(x,z) \wedge R(y,z)]$$

where $P(x,y)$, $Q(x,z)$, and $R(x,y)$ represent the propositional functions $x < y$, $x < z$, and $z < y$, respectively. We find the negation to be:

$$\begin{aligned}
&\neg[\forall x, \forall y, [P(x,y) \to \exists z, [Q(x,z) \wedge R(y,z)]] \\
&\qquad \equiv \exists x, \neg[\forall y, [P(x,y) \to \exists z, [Q(x,z) \wedge R(y,z)]] \\
&\qquad \equiv \exists x, \exists y, \neg[P(x,y) \to \exists z, [Q(x,z) \wedge R(y,z)] \\
&\qquad \equiv \exists x, \exists y, [P(x,y) \wedge \neg[\exists z, [Q(x,z) \wedge R(y,z)] \\
&\qquad \equiv \exists x, \exists y, [P(x,y) \wedge [\forall z, \neg[Q(x,z) \wedge R(y,z)] \\
&\qquad \equiv \exists x, \exists y, [P(x,y) \wedge [\forall z, [\neg Q(x,z) \vee \neg R(y,z)]
\end{aligned}$$

So the (working) negation of (2.5) is

$$\exists x, \exists y, [(x < y) \wedge (\forall z, (x \geq z \vee z \geq y)]$$

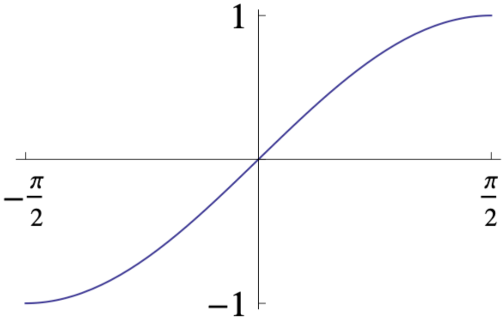

Figure 2.1: The sine function on $[-\pi/2, \pi, 2]$.

Example 2.15. Let $P(x,y)$ be the statement

If $x < y$, then $\sin x < \sin y$.

The domain of discourse is the closed interval $I = [-\frac{\pi}{2}, \frac{\pi}{2}]$. Determine which of the following statements

$$\exists x, \exists y, P(x,y) \quad \exists x, \forall y, P(x,y) \quad \forall x, \exists y, P(x,y) \quad \forall x, \forall y, P(x,y)$$

are true and which are false.

Solution. The first statement $\exists x \in I, \exists y \in I, P(x,y)$ is true. To see this simply let $x = 0$ and $y = \pi/2$ because $0 < 1$ and $\sin 0 = 0 < 1 = \sin \pi/2$.

The second statement $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, P(x, y)$ is true. To see this let $x = -\pi/2$, and then notice that $\forall y \in I, P(-\pi/2, y)$ is a true statement. That is,

$$\forall y \in I, \text{ if } -\frac{\pi}{2} < y, \text{ then } -1 < \sin y$$

is true. Recall the graph of the sine function restricted to the domain of I (see Figure 2.1).

The third statement $\forall x \in I, \exists y \in I, P(x, y)$ is true. We can not prove this statement is true with one value for x. Let $x \in I$ be an arbitrary element in I. Now that x is given we can set $y = x$. Then $P(x, y)$ is a true implication since it has a false hypothesis.

The fourth statement $\forall x \in I, \forall y \in I, P(x, y)$ is true. Again we can not prove this statement is true with one value for x. Moreover, for any given value of x, the value of y must also be arbitrary. Let $x \in I$ be an arbitrary element in I. If $y \leq x$, then the implication $P(x, y)$ is true by a false hypothesis; and thus the statement $\forall x \in I, \exists y \in I, P(x, y)$ is true in this case. If $x < y$, then the hypothesis in the implication $P(x, y)$ is true, but in fact the conclusion in $P(x, y)$ is also true since the sine function is increasing on I. Therefore, no matter what x in I is given we see that $P(x, y)$ is true for all y in I.

2.7 Inference Rules for Quantified Statements

Before we begin proving theorems, we need to discuss the inference rules for quantified statements. However, before we do so, the reader is encourage to complete Exercise 3.29, that is, write out each incidence axiom in symbolic form and also write the negation of each one in both symbolic and English form.

Suppose that $\exists x \in U$, $P(x)$ is true, where U is the domain of discourse. By Definition 2.3, $P(x)$ is true for some x in U. Thus, there exists $c \in U$ such that $P(c)$ is true. Hence we have shown that the argument

$$\frac{\exists x, P(x)}{\therefore P(c) \text{ for some element } c \in U}$$

is valid. Now suppose that $\forall x \in U$, $P(x)$ is true. By Definition 2.4, $P(x)$ is true for every x in U. In particular, if $c \in U$, then $P(c)$ is true. Hence we have shown that the argument

$$\frac{\forall x, P(x)}{\therefore P(c) \text{ if } c \in U}$$

is valid. The reader should write careful arguments to justify the other two inference rules. All four are listed below.

Table 2.1: Inference Rules for Universe

Inference Rules for Universe U	Name
$\forall x, P(x)$ $\therefore P(c)$ if $c \in U$	Universal instantiation
$P(c)$ for an arbitrary $c \in U$ $\therefore \forall x, P(x)$	Universal generalization
$\exists x, P(x)$ $\therefore P(c)$ for some element $c \in U$	Existential instantiation
$P(c)$ for some element $c \in U$ $\therefore \exists x, P(x)$	Existential generalization

2.8 Exercises

Exercise 2.1. Write the negation for each statement.

1. $\forall x, p(x) \wedge q(x)$
2. $\forall x, p(x) \vee q(x)$
3. $\forall x, p(x) \rightarrow q(x)$
4. $\forall x, p(x) \leftrightarrow q(x)$
5. $\forall x, \neg p(x)$

Exercise 2.2. Write the negation for each statement.

1. $\exists x, p(x) \wedge q(x)$
2. $\exists x, p(x) \vee q(x)$
3. $\exists x, p(x) \rightarrow q(x)$
4. $\exists x, p(x) \leftrightarrow q(x)$
5. $\exists x, \neg p(x)$

Let $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the natural numbers, integers, the rational numbers, the real numbers and the complex numbers, respectively.

Exercise 2.3. Decide which of the following propositions are true and which are false.

1. $\exists\ x \in \mathbb{Q}, x^3 + 3 = 0.$
2. $\exists\ x \in \mathbb{R}, x^3 + 3 = 0.$
3. $\exists\ x \in \mathbb{C}, x^3 + 3 = 0.$
4. $\exists!\ x \in \mathbb{Q}, x^3 + 3 = 0.$
5. $\exists!\ x \in \mathbb{R}, x^3 + 3 = 0.$
6. $\exists!\ x \in \mathbb{C}, x^3 + 3 = 0.$

Exercise 2.4. Decide which of the following propositions are true and which are false.

1. $\forall\ x \in \mathbb{N}, \exists\ y \in \mathbb{N}, x \leq y$
2. $\forall\ x \in \mathbb{Z}, \exists\ y \in \mathbb{Z}, x \leq y$
3. $\exists\ x \in \mathbb{Q}, \exists\ y \in \mathbb{N}, x \leq y$
4. $\exists\ x \in \mathbb{N}, \forall\ y \in \mathbb{N}, x \leq y$
5. $\forall\ x \in \mathbb{Z}, \forall\ y \in \mathbb{Z}, x \leq y$
6. $\exists\ x \in \mathbb{Q}, \forall\ y \in \mathbb{N}, x \leq y$

Exercise 2.5. Rewrite the following propositions symbolically with the quantifiers explicit and in the correct place.

1. For every two distinct points A and B there exists a unique line l incident with A and B.
2. For every line l there exist at least two distinct points incident with l.
3. There exist three distinct points with the property that no line is incident with all three of them.

Exercise 2.6. If the statement is written in symbols, then rewrite the statement using words; and conversely. For each also write its negation in both symbols and words.

1. $(\exists\, x \in \mathbb{Z})(\forall\, y \in \mathbb{Z})(x + y = 0)$
2. There exists an integer x such that for all real numbers y the sum of x and y is zero.
3. There exists an integer y such that for all rational numbers x the sum of x and y is zero.
4. There exists a natural number x such that for all integers y the sum of x and y is zero.
5. There exists an natural number y such that for all natural numbers x the sum of x and y is zero.
6. $(\forall\, x \in \mathbb{N})(\exists\, y \in \mathbb{N})(xy = x)$
7. There exists an integer x such that for all real numbers y the product of x and y is x.
8. There exists an integer y such that for all real numbers x the product of x and y is x.
9. There exists a natural number x such that for all integers y the product of x and y is x.
10. There exists an natural number y such that for all rational numbers x the product of x and y is x.

11. Given any two distinct real numbers, some rational number lies strictly between them.
12. $\forall\, x, y \in \mathbb{R}, (x \neq y \to \exists\, z \in \mathbb{Q}, x < z < y)$
13. $\exists\, x, y \in \mathbb{R}, (x \neq y \to \exists\, z \in \mathbb{Q}, x < z < y)$
14. $\exists\, x, y \in \mathbb{R}, (x \neq y \to \forall\, z \in \mathbb{Q}, x < z < y)$
15. $\forall\, x, y \in \mathbb{R}, (x \neq y \to \forall\, z \in \mathbb{Q}, x < z < y)$
16. $\exists\, x, y \in \mathbb{R}, (x \neq y \to \exists\, z \in \mathbb{Q}, x < z < y)$
17. $(\exists\, x \in \mathbb{Z})(\forall\, y \in \mathbb{Q})(x + y = 0)$
18. $(\forall\, y \in \mathbb{Z})(\exists\, x \in \mathbb{Z})(x + y = 0)$
19. $(\forall\, x \in \mathbb{N})(\exists\, y \in \mathbb{N})(xy = x)$
20. $(\exists\, y \in \mathbb{N})(\forall\, x \in \mathbb{N})(xy = x)$
21. $(\forall\, x \in \mathbb{N})(\exists\, y \in \mathbb{N})(x = y - 7)$
22. $(\exists\, y \in \mathbb{N})(\forall\, x \in \mathbb{N})(x = y - 7)$
23. $(\forall\, y \in \mathbb{N})(\forall\, x \in \mathbb{N})(y = x - 7)$
24. $(\exists\, x \in \mathbb{N})(\exists\, y \in \mathbb{N})(y = x - 7)$
25. For all integers x and y, the numbers xy and yx are equal.
26. Given any real number x, there exists a natural number n such that $x < n$
27. Given any real number x, there exists a natural number y such that $x + y = 0$.
28. Given any nonnegative real number x, there exists a natural number y such that $y^2 = x$.
29. Given any nonzero real number x, there exists a natural number y such that $xy = 1$.
30. There exists a smallest natural number.
31. There is no largest integer.
32. Given any two distinct real numbers, some rational number lies strictly between them.
33. Given any positive real number ϵ, there exists a natural number k such that $\frac{1}{n} < \epsilon$ whenever n is a natural number greater than k.
34. For each real number ϵ, if $\epsilon > 0$ then there exists a positive real number δ such that for each number x, if $|x-2| < \delta$ then $\left|x^2 - 4\right| < \epsilon$.

Exercise 2.7. Finish the proof of Theorem 2.1.

Chapter 3

Mathematical Proofs

In addition, proofs can help us to understand complicated concepts. By breaking down an argument into small, manageable steps, we can see how each piece fits together to form a larger whole.

Finally, proofs can be aesthetically pleasing. There is a certain beauty in a well-constructed argument, just as there is beauty in a finely crafted piece of art.

We now discuss valid arguments, inference rules, and various methods of proof including direct proofs, indirect proofs, proof by contrapositive, and proof by cases.

An **argument** is defined as a statement q being asserted as a consequence of some list of statements $p_1, p_2, ..., p_k$. The statements $p_1, p_2, .., p_k$ are called the **premises** (or) **hypothesis** of the argument; and the statement q is called the **conclusion**.

Definition 3.1. A statement q is called a **propositional consequence** of statements $p_1, p_2, ..., p_k$ if and only if the single statement $(p_1 \wedge p_2 \wedge \cdots \wedge p_k) \to q$ is a tautology.

Example 3.1. Test the validity of the following arguments.

$$\begin{array}{l} p \longleftrightarrow q \\ q \vee r \\ \neg\, r \\ \hline \therefore \neg\, p \end{array} \qquad \begin{array}{l} p \vee q \\ \neg\, q \to r \\ \neg\, p \vee \neg\, r \\ \hline \therefore \neg\, p \end{array}$$

Solution. By Definition 3.1, the arguments can be shown to be valid or not by constructing a truth table for the following statements

1. $[(p \longleftrightarrow q) \wedge (q \vee r) \wedge (\neg\, r)] \longleftrightarrow (\neg p)$
2. $[(p \vee q) \wedge (\neg\, q \to r) \wedge (\neg\, p \vee \neg\, r)] \longrightarrow (\neg p)$

and determining whether or not these are tautologies. The reader should verify that the first statement is not a tautology, and so the argument in (a) is not valid. What about the second statement?

3.1 Logical Discourse

The pattern of logical discourse goes as follows:

- A collection of primitive (undefined terms) is given.
- A collection of axioms (unproven statements) about the primitive terms is also given.

- Then all of the terms of the discourse are defined by means of the primitive terms or by previously defined terms that were defined using primitive terms.

- All other statements in the system are logically deduced from the axioms. These are the theorems of the system.

In mathematical exposition, we often communicate by distinguishing different types of theorems. For example, a theorem is sometimes called a **result**. There is an air of humility in calling a theorem merely a result. Other alternatives to **theorem** are listed below.

Fact. A very minor theorem, but important enough to number and refer to latter, i.e., the statement $1 + 1 = 2$ is a fact.

Proposition. Also a minor theorem, but more important (usually more general) than a fact –but not as prestigious as a theorem.

Lemma. Often a technical theorem, which is used to help prove another more important theorem. Stating lemmas, before proving a difficult complicated theorem, is functional.

Claim. Similar to lemma but less formal. A claim will often be referred to only a small number of times, whereas a lemma may be referenced many times and is a useful result in itself. For example, stating a claim inside the proof theorem is a great way to help organize key steps in a proof.

Corollary. An important enough result to state on its own whose proof requires a previously proved theorem as its main step.

3.2 Writing Proofs

Direct Proofs

Basically, direct proofs are proofs that do not use the Law of Excluded middle tautology. In each of the following examples, we use inference rules to write a proof in column format – and we also write a paragraph proof.

Example 3.2. Given the three previously proven theorems:

- Theorem 1: $p \to q$,
- Theorem 2: $q \to r$, and
- Theorem 3: $r \to s$.

We can now prove the next theorem.

Theorem: If p then s.

Solution. We begin with a column proof.

Conclusions	Justifications
p	premise
$p \to q$	theorem 1
q	steps 1 and 2, modus ponens
$q \to r$	theorem 2
r	steps 3 and 4, modus ponens
$r \to s$	theorem 3
s	steps 5 and 6, modus ponens

We end with a paragraph proof.

> Assume p. By Theorem 1, we know q, and so by Theorem 2, we now have r. Hence by Theorem 3, we have s as needed.

Example 3.3. Prove: if $p \vee q$ and $\neg q$, then p.

Solution. We begin with a column proof.

Conclusions	Justifications
$\neg q$	premise
$p \vee q$	premise
p	disjunctive syllogism

We end with a paragraph proof:

> Assume $\neg q$ and $p \vee q$. We can not have q and $\neg q$, thus p follows immediately.

Example 3.4. Assume the following:

- Definition: a is said to be b iff $r \rightarrow s$,
- Axiom 1: $r \rightarrow q$,
- Theorem 1: If a is c then $q \rightarrow t$,
- Theorem 2: $t \rightarrow s$.

Prove the following theorem.

Theorem: If a is c then a is b.

Solution. We begin with a column proof.

Conclusions	Justifications
a is c	premise
if a is c then $q \rightarrow t$	theorem 1
$q \rightarrow t$	steps 2 and 3, modus ponens
r	premise
$r \rightarrow q$	axiom 1
q	steps 4 and 5, modus ponens
t	steps 3 and 6, modus ponens
$t \rightarrow s$	theorem 2
s	steps 7 and 8, modus ponens
$r \rightarrow s$	steps 4 through 9
a is b	definition of a is b

We end with a paragraph proof:

> Assume a is c. By Theorem 1, we have $q \rightarrow t$. To prove that a is b we assume r. Then by Axiom 1, we have q, which now yields t. By Theorem 2, it follows that s. Therefore we have shown $r \rightarrow s$ as needed.

Indirect Proofs

Example 3.5. Given the two previously proven theorems:

- Theorem 1: $\neg q \rightarrow r$,
- Theorem 2: If r then either $\neg p$ or q.

Prove the following theorem.

$$\text{Theorem: } p \to q.$$

Solution. We begin with a column proof.

Conclusions	Justifications
p	premise
$q \vee \neg q$	excluded middle
$\neg$	premise
$\neg q \to r$	theorem 1
r	steps 3 and 4, modus ponens
$r \to (\neg p \vee q)$	theorem 2
$\neg p \vee q$	steps 5 and 6, modus ponens
$p \wedge \neg q$	steps 1 and 3
$\neg(\neg p) \wedge \neg q$	double negation
$\neg(\neg p \vee q)$	step 9, De Morgan
$(\neg p \vee q) \wedge \neg(\neg p \vee q)$	steps 7 and 10, contradiction
q	steps 3 and 11, indirect proof

We end with a paragraph proof:

> Assume p. Suppose $\neg q$ for otherwise we are finished. Then r by Theorem 1. By hypothesis we cannot have $\neg p$, and so by Theorem 2, we have q as needed.

Example 3.6. Prove: if $p \leftrightarrow q$ and $q \to \neg\, p$, then $\neg\, p$.

Solution. We begin with a column proof.

Conclusions	Justifications
$p \leftrightarrow q$	premise
$(p \to q) \wedge (q \to p$	definition of ↔
$p \to q$	simplification
$q \to \neg p$	premise
$p \vee \neg p$	excluded middle
p	premise
q	steps 3 and 6, modus ponens
$\neg p$	steps 4 and 7, modus ponens
$p \wedge \neg p$	steps 6 and 9, contradiction
$\neg p$	steps 5-9, indirect proof

We end with a paragraph proof:

> Assume for a contradiction p. Since p and q are equivalent, we have q. By hypothesis, we then have $\neg p$. Since $\neg p$ and p is a contradiction, our original premise of p can not happen. Whence $\neg p$.

Example 3.7. Assume the following:

- Axiom 1: p implies either r or s,
- Theorem 1: $y \to \neg p$,
- Theorem 2: $r \to x$,
- Theorem 3: $s \to y$,
- Theorem 4: $x \to q$.

Prove the following theorem.

$$\text{Theorem: } p \to q.$$

Solution. We begin with a column proof.

Conclusions	Justifications
p	premise
$p \to (r \vee s)$	axiom 1
$r \vee s$	steps 1 and 2, modus ponens}
s	premise
$s \to y$	theorem 3
y	steps 4 and 5, modus ponens
$y \to \neg p$	theorem 1
$\neg p$	steps 6 and 7, modus ponens
$p \wedge \neg p$	steps 1 and 8, contradiction
$\neg s$	steps 4-9, indirect proof
r	steps 3 and 10, disjunctive syllogism
$r \to x$	theorem 2
x	steps 11 and 12, modus ponens
$x \to q$	theorem 4
q	steps 13 and 14, modus ponens

We end with a paragraph proof:

> Assume p. If we have s, then by Theorem 3, we have y; yet by Theorem 1 this yields $\neg p$. Since we can not have both $\neg p$ and p we see that we can not have s. Hence we have $\neg s$. By Axiom 1, we must have r. By Theorem 2, we now have x, and so by Theorem 4, we conclude with q as needed.

Proof by Contrapositive

Example 3.8. Assume the following:

- Axiom 1: $p \to \neg y$.
- Axiom 2: $\neg q \to r$.
- Theorem 1: $p \to \neg z$.
- Theorem 2: $x \to$ either q or z..
- Theorem 3: $r \to$ either x or y.

$$\text{Theorem: } \neg p \to \neg q.$$

Solution. We prove the (logical equivalent) contrapositive statement $p \to q$.
We begin with a column proof.

Conclusions	Justifications
p	premise
$p \to \neg y$	axiom 1
$\neg y$	steps 1 and 2, modus ponens
$q \vee \neg q$	excluded middle
$\neg q$	premise
$\neg q \to r$	axiom 2
r	steps 5 and 6, modus ponens
$r \to x \vee y$	theorem 3
$x \vee y$	steps 7 and 8, modus ponens
x	steps 3 and 9, disjunctive syllogism
$x \to q \vee z$	theorem 2
$q \vee z$	steps 10 and 11, modus ponens
z	premise
$p \to \neg z$	theorem 1
$z \to \neg p$	contrapositive
$\neg p$	steps 13 and 15, modus ponens
$p \wedge \neg p$	steps 1 and 16, contradiction
$\neg z$	steps 13 and 17, indirect proof
q	steps 12 and 18, disjunctive syllogism
$\neg(\neg q)$	steps 5 and 19, contradiction
q	steps 4 and 20, disjunctive syllogism

We end with a paragraph proof:

> Assume p. Then by Axiom 1 we have $\neg y$. Assume for a contradiction that $\neg q$. Then by Axiom 2 we have r, and so either x or y by Theorem 3. In case we have x, then by

> Theorem 2 we have z. Now $\neg p$ follows by Theorem 1 and so this contradiction show that x can not happen. Hence y follows. Yet now we have y and $\neg y$ and so it fact we cannot have $\neg q$. Therefore q as needed.

Proof by Cases

Example 3.9. Assume the following:

- Theorem 1: $r \to \neg p$,
- Theorem 2: $s \to \neg p$,
- Theorem 3: A complete set of logical possibilities is: r, s, and q; that is, one of the statements r, s, and q is true and only one.

Prove the following theorem.

Theorem: If p then q.

Solution. We begin with a column proof.

Conclusions	Justifications
p	premise
one and only one holds: r, s, q	theorem 3
r	premise (case 1)
$r \to \neg p$	theorem 1
$\neg p$	steps 3 and 4, modus ponens
$p \wedge \neg p$	steps 1 and 5, contradiction
$\neg r$	steps 3 and 6, indirect proof
s	premise (case 2)
$s \to \neg p$	theorem 2
$\neg p$	steps 8 and 9, modus ponens
$p \wedge \neg p$	steps T and 10, contradiction
$\neg s$	steps 8 and 11, indirect proof
q	step 2

We end with a paragraph proof:

> Assume p. By Theorem 3, there are exactly three cases two consider. If r, then we have $\neg p$ by Theorem 1 which is contrary to hypothesis. Similarly, s is contrary to hypothesis. Hence we have q as needed.

We end this section with a short discussion on how you might have seen these types of arguments (proofs) before in precalculus. We will demonstrate three ways to prove the statement:

$$\text{If } x^3 - x^2 + x - 1 = 0, \text{ then } x = 1.$$

- (**Direct Proof**) Assume $x^3 - x^2 + x - 1 = 0$. Then $(x-1)(x^2+1) = 0$, which implies that either $x - 1 = 0$ or $x^2 + 1 = 0$. But we know that $x^2 + 1 \neq 0$ (since x is real), and so it must be the case that $x - 1 = 0$. Hence $x = 1$.
- (**Proof by Contrapositive**) Assume $x \neq 1$. Then $x - 1 \neq 0$. Also, since x is real, $x^2 + 1 \neq 0$. It follows that $(x-1)(x^2+1) \neq 0$. Upon multiplication we obtain the result $x^3 - x^2 + x - 1 \neq 0$.
- (**Proof by Contradiction**) Suppose $x^3 - x^2 + x - 1$ and assume for a contradiction that $x \neq 1$. Then $x - 1 \neq 0$. Since $x^4 - x^2 + x - 1 = (x-1)(x^2+1))$ and $x - 1 \neq 0$, it must be that $x^2 + 1 = 0$. This is a contradiction because x is a real number. Therefore, we conclude $x = 1$.

3.3 Axiomatic Systems

In this chapter we discuss axiomatic systems and inference rules for quantified statements. To give an example of this process, we carry out a simple logical discourse for incidence geometry involving points, lines, and incidence.

An **axiomatic** (or **formal**) system must contain a set of technical terms that are deliberately chosen as undefined, called **undefined terms**, and are subject to the interpretation (an intuition) of the reader. All other technical terms of the system are ultimately defined by means of the undefined terms, and are called **definitions**. An axiomatic system contains a set of statements, dealing with undefined terms and definitions, that are chosen to remain unproved, and are called **axioms**.

Incidence Geometry

Below is an example of a simple axiomatic system where the terms *point*, *line*, and *incidence* only have the meaning given by a small collection of axioms.

We assume that we have a collection of points and a collection of lines. The only other assumptions we make about these points and lines, and their behavior, is given solely by the axioms.

> The goal is not to say what a point is or what a line is, but rather to discover how they behave, relatively to each other.

Axioms. Let **point**, **line**, and **incidence** be undefined terms. Collectively the following three axioms are called the **Incidence Axioms**.

(A1) For every two distinct points A and B there exists a unique line l incident with A and B, and is denoted by $l(A, B)$.

(A2) For every line l there exist at least two distinct points incident with l.

(A3) There exist three distinct points with the property that no line is incident with all three of them.

We will use the following convention: uppercase letters denote points, i.e. A, B, ...P, Q, etc, and lowercase letters denote lines, i.e. l, m, n.

Definition 3.2. Three or more points are called **collinear** if there exists a line incident with all of them. Three or more lines are called **concurrent** if there exists a point incident with all of them.

Notice the definitions of collinear and concurrent are dual notions, in the sense that they are defined the same way except that the roles of point and line are interchanged. We use the terms **noncollinear** and **nonconcurrent** to mean not collinear and not concurrent, respectively.

Lines l and m are called **equal lines** , denoted by $l = m$, if every point incident with l is also incident with m, and conversely. Lines l and m are called **parallel lines** if $l = m$ or if no point is incident with both of them. The notation $l \parallel m$ means line l is parallel to line m.

Theorem 3.1. *If l and m are distinct lines that are not parallel, then l and m have a unique point in common.*

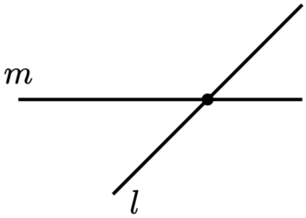

Figure 3.1: Unique point in common.

Proof. We begin with a column proof.

No.	Conclusions	Justifications
1	Lines l and m are distinct lines that are not parallel.	Hypothesis
2	Exactly one must hold: l and m either have no points in common or not	Law of Excluded Middle
3	There does not exists any points incident with both l and m.	Case 1
4	Lines l and m are parallel.	Definition of parallel
5	$\rightarrow\leftarrow$	Steps 1, 4
6	Lines l and m have points in common.	Case 2
7	Exactly one must hold: lines l and m have exactly one point in common or more.	Law of Excluded Middle
8	There exists distinct points P and Q that are both incident with both lines l and m.	Case 2.1
9	$l = m$	Axiom 1
10	$\rightarrow\leftarrow$	Step 1
11	There exists exactly one point incident with lines l and m.	Case 2.2

We end with a paragraph proof.

> Assume l and m are distinct lines that are not parallel. By definition of parallel lines, these lines must have at least one point in common. If they have another point in common, then they are the same line by Axiom 1. Therefore, they have a unique point in common.

□

Theorem 3.2. *There exist three distinct lines that are nonconcurrent.*

Proof. We begin with a column proof.

No.	Conclusions	Justifications
1	A, B, and C are distinct noncollinear points.	Axiom 3
2	There exists a line $\overleftrightarrow{AB}$ incident with A and B.	Axiom 1

No.	Conclusions	Justifications
3	There exists a line $\overleftrightarrow{BC}$ incident with B and C.	Axiom 1
4	There exists a line $\overleftrightarrow{AC}$ incident with A and C.	Axiom 1
5	$\overleftrightarrow{AB} = \overleftrightarrow{BC}$	RAA Hypothesis
6	A is incident with $\overleftrightarrow{BC}$	Definition of equality
7	A, B, and C are collinear points.	Definition of collinear
8	$\rightarrow\leftarrow$	Steps 1, 7
9	$\overleftrightarrow{AB} \neq \overleftrightarrow{BC}$	RAA Conclusion
10	$\overleftrightarrow{AB} = \overleftrightarrow{AC}$	RAA Hypothesis
11	B is incident with $\overleftrightarrow{AC}$	Definition of equality
12	A, B, and C are collinear points.	Definition of collinear
13	$\rightarrow\leftarrow$	Steps 1, 12
14	$\overleftrightarrow{AB} \neq \overleftrightarrow{AC}$	RAA Conclusion
15	$\overleftrightarrow{AC} = \overleftrightarrow{BC}$	RAA Hypothesis
16	A is incident with $\overleftrightarrow{BC}$	Definition of equality
17	A, B, and C are collinear points.	Definition of collinear
18	$\rightarrow\leftarrow$	Steps 1, 17
19	$\overleftrightarrow{AC} \neq \overleftrightarrow{BC}$	RAA Conclusion
20	Lines $\overleftrightarrow{AB}$, $\overleftrightarrow{BC}$, $\overleftrightarrow{AC}$ are three distinct lines.	Steps 9, 14, 19
21	There exists a point X incident with all three lines $\overleftrightarrow{AB}$, $\overleftrightarrow{BC}$, $\overleftrightarrow{AC}$.	RAA Hypothesis
22	One and only one must hold: $X = A$ or $X \neq A$.	Law of Excluded Middle
23	$X = A$	Case 1
24	Point A is incident with all three lines $\overleftrightarrow{AB}$, $\overleftrightarrow{BC}$, and $\overleftrightarrow{AC}$.	Steps 21, 23
25	A, B, C are collinear points.	Definition of Collinear
26	$\rightarrow\leftarrow$	Steps 1, 25
27	$X \neq A$	Case 2
28	Lines $\overleftrightarrow{AB}$ and $\overleftrightarrow{AC}$ are not parallel.	Def. of Parallel Lines
29	$X = A$	Theorem 2
30	$\rightarrow\leftarrow$	Steps 27, 29

No.	Conclusions	Justifications
31	There does not exist a point X incident with all three lines $\overleftrightarrow{AB}$, $\overleftrightarrow{BC}$, $\overleftrightarrow{AC}$.	RAA Conclusion
32	lines $\overleftrightarrow{AB}$, $\overleftrightarrow{BC}$, $\overleftrightarrow{AC}$ are nonconcurrent.	Def. of nonconcurrent

We end with a paragraph proof.

> By Axiom 3, there exists three distinct points A, B, and C and by axiom 1, we have lines $l(A,B)$, $l(B,C)$, and $l(A,C)$. If $l(A,B) = l(B,C)$, then points A, B, and C are collinear, contrary to hypothesis. Hence $l(A,B) \neq l(B,C)$. Similarly, it follows $l(B,C) \neq l(A,C)$ and $l(A,B) \neq l(A,C)$. Thus we have three distinct lines. Assume these lines are concurrent with point X. If $X = A$, then A is on all three lines and again we contradict the hypothesis. Hence $X \neq A$, and so the nonparallel lines $l(A,B)$ and $l(A,C)$ have more than one point in common. This contradicts Theorem 2, and so X can not exist. Whence these three distinct lines are nonconcurrent.

□

Theorem 3.3. *For every point, there is at least one line not passing through it.*

Proof. We begin with a column proof.

No.	Conclusions	Justifications
1	A is a point	Hypothesis
2	A is incident with every line.	RAA Hypothesis
3	There exists 3 noncollinear points E, D, F.	Axiom 3
4	There exists a line $\overleftrightarrow{ED}$ incident with E and D.	Axiom 1
5	There exists a line $\overleftrightarrow{DF}$ incident with D and F.	Axiom 1
6	One and only one must hold: $A = D$ or $A \neq D$.	Law of Excluded Middle
7	$A \neq D$	Case 1
8	A and D are incident with $\overleftrightarrow{ED}$ and $\overleftrightarrow{DF}$.	Steps 2, 4, 5

No.	Conclusions	Justifications
9	$\overleftrightarrow{ED}= \overleftrightarrow{DF}$	Axiom 1
10	F is incident with $\overleftrightarrow{ED}$.	Definition of Equal Lines
11	E, D, and F are collinear points.	Definition of collinear
12	$\rightarrow\leftarrow$	Steps 3 and 11
13	$A = D$	Case 2
14	D is incident with every line.	Steps 2, 13
15	There exists a line $\overleftrightarrow{EF}$ incident with E and F.	Axiom 1
16	D is incident with $\overleftrightarrow{EF}$.	Step 1
17	E, D, and F are collinear points.	Definition of Collinear
18	$\rightarrow\leftarrow$	Steps 3, 17
19	There exists a line not incident with A.	RAA conclusion

We end with a paragraph proof.

> Let A be an arbitrary point. Assume every line is incident with A. By Axiom 3, there exists three distinct points, say D, E, and F. Point A is not one of these points, say D. By Axiom 1, we have lines $l(E, D)$ and $l(D, F)$. Further, since A and D are distinct points and both are on $l(E, D)$ and $l(D, F)$ we have $l(E, D) = l(D, F)$, by Axiom 1. Hence E, D, and F are collinear. Therefore, point A is not incident with at least one line.

□

Peano's Axioms

Peano's Axioms $\mathbb{N}$ is a set with the following properties.

- $\mathbb{N}$ has a distinguished element which we call **1**.
- There exists a distinguished set map $s : \mathbb{N} \to \mathbb{N}$.
- The mapping s is injective.
- There does not exists an element $n \in \mathbb{N}$ such that $s(n) = 1$.
- If S is a subset of $\mathbb{N}$ with the properties: $1 \in S$ and if $n \in S$, then $s(n) \in S$, then $S = \mathbb{N}$.

We call such a set $\mathbb{N}$ to be the set of natural numbers and elements of this set to be natural numbers.

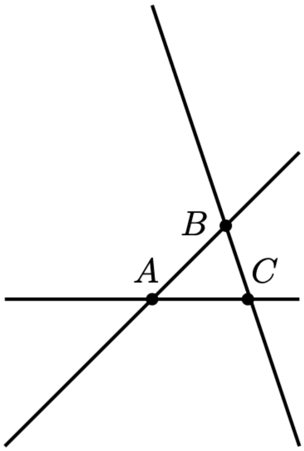

Figure 3.2: Nonconcurrent lines.

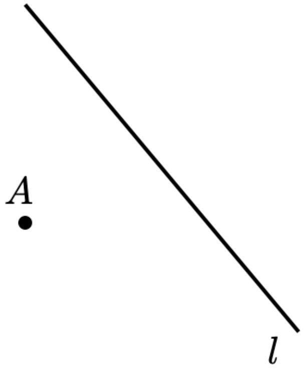

Figure 3.3: Point not on line.

Theorem 3.4. *If $n \in \mathbb{N}$ and $n \neq 1$, then there exists a unique $m \in \mathbb{N}$ such that $s(m) = n$.*

Proof. Consider the subset

$$S = \{n \in \mathbb{N} \mid n = 1 \text{ or } n = s(m), \text{ for some } m \in \mathbb{N}\}. \tag{3.1}$$

By definition, $1 \in S$. If $n \in S$, clearly $s(n) \in S$, again by definition of S. Thus by induction, we see that $S = \mathbb{N}$. Further injectivity of s implies uniqueness as claimed.

□

By **??**, the following definition of addition is well-defined.

Definition 3.3. Let *addition* be the operation $+ : X \times X \to X$ recursively defined on y by

$$x + y := \begin{cases} x & \text{if } y = 0 \\ s(x+z) & \text{if } y \in s(X) \text{ and } y = s(z) \end{cases} \tag{3.2}$$

Notice $0 + 0 = 0$ and that $x + 0 = x$, for all $x \in X$.

Lemma 3.1. *For all $x \in X$, $x + 1 = s(x)$.*

Proof. Let $x \in X$. Immediately, $x + 1 = x + s(0) = s(x + 0) = s(x)$.

□

Lemma 3.2. *For all $x \in X$, $0 + x = x$.*

Proof. We use induction on x. First, $0+1 = 0+s(0) = s(0+0) = s(0) = 1$. Assume that $0 + y = y$. We must show that $0 + s(y) = s(y)$. We have $0 + s(y) = s(0 + y) = s(y)$. Therefore, $0 + x = x$, for all $x \in X$.

□

Lemma 3.3. *For all $x, y \in X$, $s(x + y) = s(x) + y$.*

Proof. Let $x \in X$. We use induction on y. First, $s(x+0) = s(x) = s(x)+0$. Let $z \in X$ and assume that $s(x+z) = s(x)+z$. We must show that $s(x+s(z)) = s(x)+s(z)$. We have $s(x+s(z)) = s(s(x+z)) = s(s(x)+z) = s(x)+s(z)$. Therefore, $s(x+y) = s(x)+y$, for all $x, y \in X$.

□

Lemma 3.4. *For all $x, y \in X$, $x+y = y+x$.*

Proof. Let $x \in X$. We use induction on y. The case $y = 0$ follows from 3.2. Let $z \in X$ and assume that $x+z = z+x$. We must show that $x+s(z) = s(z)+x$. We have $x+s(z) = s(x+z) = s(z+x) = s(z)+x$, where the last equality follows by 3.3. Therefore, $x+y = y+x$, for all $x, y \in X$.

□

Lemma 3.5. *For all $x, y, z \in X$, $(x+y)+z = x+(y+z)$.*

Proof. Let $x, y \in X$. We use induction on z. First, $(x+y)+0 = x+y = x+(y+0)$. Let $w \in X$ and assume $(x+y)+w = x+(y+w)$, we must show $s(w)$ has the same property. In fact, $(x+y)+s(w) = s((x+y)+w) = s(x+(y+w)) = x+s(y+w) = x+(y+s(w))$ as we needed. Therefore, $(x+y)+z = x+(y+z)$, for all $x, y, z \in X$.

□

Lemma 3.6. *For all $x, y, z \in X$,*

$$x+y = z+y \implies x = z. \tag{3.3}$$

Proof. Let $x, z \in X$. We use induction on y. If $y = 0$, then (3.3) holds. Let $w \in X$ and assume that (3.3) holds for w.
We must show that $x+s(w) = z+(w)$ implies $x = z$. Notice $x+s(w) = z+s(w)$ is equivalent to $s(x+w) = s(z+w)$. Since s is injective, this implies $x+w = z+w$ as needed.

□

By **??**, the following definition of multiplication is well-defined.

Definition 3.4. We define *multiplication* $x \cdot y$, recursively on y, by

$$x \cdot 0 = 0, \qquad x \cdot s(y) = x \cdot y + x. \tag{3.4}$$

Lemma 3.7. *For all $x \in X$, $x \cdot 1 = x$.*

Proof. Let $x \in X$. Immediately, $x \cdot 1 = x \cdot s(0) = x \cdot 0 + x = 0 + x = x$.

□

Lemma 3.8. *For all $y \in X$, $0 \cdot y = 0$.*

Proof. We use induction on y. First, $0 \cdot 0 = 0$. Let $z \in X$ and assume $0 \cdot z = 0$. We must show that $0 \cdot s(z) = 0$. We have $0 \cdot s(z) = 0 \cdot z + 0 = 0 + 0 = 0$. Therefore, $0 \cdot y = 0$, for all $y \in X$.

□

Lemma 3.9. *For all $x, y \in X$, $s(x) \cdot y = x \cdot y + y$.*

Proof. Let $x \in X$. We use induction on y. First, $s(x) \cdot 0 = 0 = 0 + 0 = x \cdot 0 + 0$. Let $z \in X$ and assume $s(x) \cdot z = x \cdot z + z$. We must show that $s(x) \cdot s(z) = x \cdot s(z) + s(z)$. We have $s(x) \cdot s(z) = s(x) \cdot z + s(x) = x \cdot z + z + (x + 1) = x \cdot z + x + (z + 1) = x \cdot s(z) + s(z)$. Therefore, $s(x) \cdot y = x \cdot y + y$, for all $x, y \in X$.

□

Lemma 3.10. *For all $x, y \in X$, $x \cdot y = y \cdot x$.*

Proof. Let $x \in X$. We use induction on y. First, $x \cdot 0 = 0 = 0 \cdot x$. Let $z \in X$ and assume $x \cdot z = z \cdot x$. We must show that $x \cdot s(z) = s(z) \cdot x$. We have $x \cdot s(z) = x \cdot z + x = z \cdot x + x = s(z) \cdot x$. Therefore, $x \cdot y = y \cdot x$, for all $x, y \in X$.

□

Lemma 3.11. *For all $x, y, z \in X$, $(x + y) \cdot z = x \cdot z + y \cdot z$.*

Proof. Let $x, y \in X$. We use induction on z. Clearly, $(x+y)\cdot 0 = x\cdot 0+y\cdot 0$. Let $w \in X$ and assume $(x + y) \cdot w = x \cdot w + y \cdot w$. We must show that $(x + y) \cdot s(w) = x \cdot s(w) + y \cdot s(w)$. We have

$$\begin{aligned}(x + y) \cdot s(w) &= (x + y) \cdot w + (x + y) = x \cdot w + y \cdot w + (x + y)\\ &= (x \cdot w + x) + (y \cdot w + y) = x \cdot s(w) + y \cdot s(w)\end{aligned}$$

which follow by the commutative and associative laws for addition. Therefore, $(x + y) \cdot z = x \cdot z + y \cdot z$, for all $x, y, z \in X$.

□

Lemma 3.12. *For all $x, y, z \in X$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.*

Proof. Let $x, y \in X$. We use induction on z. Clearly, $(x \cdot y) \cdot 0 = x \cdot (y \cdot 0)$. Let $w \in X$ and assume $(x \cdot y) \cdot w = x \cdot (y \cdot w)$. We must show that $(x \cdot y) \cdot s(w) = x \cdot (y \cdot s(w))$. We have

$$\begin{aligned}(x \cdot y) \cdot s(w) &= (x \cdot y) \cdot w + (x \cdot y) = x \cdot (y \cdot w) + (x \cdot y)\\ &= x \cdot (y \cdot w + y) = x \cdot (y \cdot s(w))\end{aligned}$$

which follow from the commutative law of multiplication and the distributive law. Therefore, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, for all $x, y, z \in X$.

□

Lemma 3.13. *For all $x, y \in X$,*

$$x > y \textit{ if and only if } x = y + u \textit{ for some } 0 \neq u \in X. \tag{3.5}$$

Proof. We use induction on y. The case for $y = 0$ is clear. Let $z \in X$. Assume 3.5 holds for z, for all $x \in X$. We will prove that

$$t > s(z) \Leftrightarrow t = s(z) + v \text{ for some } 0 \neq v \in X.$$

Assume $t > s(z)$. Then $t > s(z) > z$ and so by hypothesis, there exists $0 \neq v \in X$ such that $t = z + v$. Since s is onto, let $v = s(u)$. Then $t = z + v = z + s(u) = s(z + u) = s(z) + u$. If $u = 0$, then $t = s(z)$ contrary to hypothesis.

To prove conversely, assume $t = s(z) + v$ for some nonzero element v. If $t = s(z)$, then $v = 0$ contrary to hypothesis. Suppose $t < s(z)$. Case: $t > z$. Then $z < t < s(z)$ which can not happen. Case: $t = z$. Then $z = s(z) + v$ and so $s(z) = z + 1 = s(z) + v + 1$. Hence $0 = v + 1 = v + s(0) = s(v + 0) = s(v)$ which implies $v = 1$ since s is injective. Hence

$0 = 1 + 1$, this absurdity implies that this case can not happen. Case: $t > z$. Then $s(z) + v < z$ and so $x = z + v < s(z + v) = s(z) + v < z$. By induction hypothesis $x > z$. Therefore, this case cannot happen either. All cases considered, it now follows that $t > s(z)$. Whence, 3.5 holds for all $x, y \in X$.

□

Lemma 3.14. *For all $w, x, y, z \in X$, if $w < x$ and $y < z$, then $w + y < x + z$.*

Proof. Assume $w < x$ and $y < z$. Then there exists nonzero s and t such that $x = w + s$ and $z = y + t$. Then $x + z = w + y + (s + t)$ and so by 3.13, $w + y < x + z$.

□

Lemma 3.15. *For all $x, y, z \in X$,*

$$x \cdot y = x \cdot z, x \neq 0 \implies y = z. \tag{3.6}$$

Proof. Assume $x \cdot y = x \cdot z$. If $y < z$ then there exists $w > 0$ such that $z = y + w$. Then $x \cdot y = x \cdot z = x \cdot (y + w) = x \cdot y + x \cdot w$. By 3.6, we have $x \cdot w = 0$. Since $x \neq 0$ and $w \neq 0$, let $x = s(u)$ and $w = s(t)$. Then $x \cdot w = x \cdot s(t) = x \cdot t + s(u) = s(x \cdot t + u) \neq 0$. Hence, we find that $y < z$ cannot happen. Similarly, the case for $y > z$ cannot happen, and thus $y = z$.

□

Lemma 3.16. *For all $x, y, z \in X$, if $x < y$ and $0 < z$, then $xz < yz$.*

Proof. Assume $x < y$ and $0 < z$. Then there exist nonzero s such that $y = x + s$. Then $yz = (x + s)z = xz + sz$ If $sz = 0$, then $yz = xz$. By 3.15, we have $y = x$, contrary to hypothesis. Therefore, $sx \neq 0$ and so we have $xz < yz$.

□

3.4 Exercises

Exercise 3.1. Using the Incidence Axioms do each of the following.

1. Write each Incidence Axiom in symbolic form.
2. Write the negation of each Incidence Axiom in symbolic form.
3. Write the negation of each Incidence Axiom in words.

Exercise 3.2. Write careful arguments to explain why each inference rule Table 2.1 for quantified statements is valid.

Exercise 3.3. Prove each of the following statements using the Incidence Axioms. First write a column proof and then write a paragraph proof.

1. For every line l, $l = l$.
2. For every line l and every line m, if $l = m$ then $m = l$.
3. For every line l, m, and n, if $l = m$ and $m = n$, then $l = n$.

Exercise 3.4. Prove each of the following statements using the Incidence Axioms. First write a column proof and then write a paragraph proof.

1. There exists at least one line.
2. There exists at least two lines.
3. There exists at least three points.
4. There exists at least three lines.
5. Every point is on at least one line.

Exercise 3.5. Prove each of the following statements using the Incidence Axioms. First write a column proof and then write a paragraph proof.

1. For every line l, there is at least one point not lying on l.
2. For every point A, there exist at least two distinct lines through A.
3. If C is on $l(A, B)$ and distinct from A and B, then $l(C, A) = l(B, C) = l(A, B)$
4. If $l(A, B) = l(A, C)$ and B and C are distinct, then $l(A, B) = l(B, C)$.
5. If l is any line, then there exists lines m and n such that l, m, and n are distinct and both m and n have a point in common with l.
6. If A is any point, then there exist points B and C such that A, B, and C are noncollinear.
7. If A and B are two distinct points, then there exists a point C such that A, B, and C are noncollinear.

Exercise 3.6. Determine which of the following sentences or pairs of sentences are propositions. For those that are not, explain why not.

1. A bird has two legs or an insect has six legs.
2. The lake water is boiling hot.
3. Does ice float?
4. Do pigs tell lies?
5. This sentence has four errors.
6. The following sentence is false. The preceding sentence is true.

Exercise 3.7. Write a truth table for each of the following propositional forms.

1. $p \vee (q \wedge \neg p)$
2. $p \wedge \neg(p \wedge p)$
3. $(p \vee q) \wedge (p \wedge c)$
4. $(\neg p \vee q) \wedge (r \vee \neg q)$
5. $(p \vee \neg(r \wedge \neg q)) \wedge \neg p$
6. $(p \vee \neg q) \wedge (q \wedge \neg r)$

Exercise 3.8. Determine whether the following given propositional forms is a tautology, a contradiction, or neither. Justify.

1. $(p \wedge \neg q) \wedge (q \vee \neg p)$
2. $(q \vee \neg p) \vee (r \wedge \neg q)$
3. $(p \wedge \neg r) \vee (r \wedge \neg q)$
4. $\neg(q \vee r \vee \neg p) \wedge (p \wedge r \wedge \neg q)$
5. $(p \vee (q \wedge r)) \vee (q \vee \neg r)$

Exercise 3.9. Decide which of the following propositions that follow are true and which are false. If a proposition is false, provide a counterexample to it.

1. $\forall x \in \mathbb{N}, x^2 + 3x + 2 \geq 0$
2. $\forall x \in \mathbb{Z}, x^2 + 3x + 2 \geq 0$
3. $\forall x \in \mathbb{Q}, x^2 + 3x + 2 \geq 0$
4. $\forall x \in \mathbb{R}, x^2 + 3x + 2 \geq 0$

Exercise 3.10. Write a working negation of each of the following statements. If the statement is in words, write the negation in words; if it is symbols, write the negation in symbols.

1. Every integer is even or odd.
2. Every line segment has a unique midpoint.
3. $\forall \epsilon > 0, \exists\ K \in \mathbb{N}, \forall n, m \in \mathbb{N}$ s.t. $((n > K \wedge m > K) \to |x_n - x_m| < \epsilon)$
4. Every natural number has a prime divisor.
5. There is no largest integer.
6. $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}$ s.t. $m > n$

Exercise 3.11. Let x be a positive integer and define the following propositional functions:

$$p(x) : x \text{ is prime}, \qquad q(x) : x \text{ is even}, \qquad r(x) : x > 2.$$

Write out each statement in words.

1. $\exists x, p(x)$
2. $\exists x, [p(x) \wedge q(x)]$
3. $\forall x, r(x)$
4. $\forall x, [r(x) \to (p(x) \vee q(x))]$
5. $\forall x, [(p(x) \wedge q(x)) \to \neg r(x)]$
6. $\exists x, [p(x) \wedge (q(x) \vee r(x))]$

Exercise 3.12. Find the working negation (negation in simplest form) of each formula.

1. $\forall x, [p(x) \vee q(x)]$
2. $\forall x, [\exists y, (p(x, y) \to q(x, y))]$
3. $\exists x, [(\forall x, p(x, y) \to q(x, y)) \wedge \exists z, r(x, z)]$
4. $\forall x, \forall y, [p(x, y) \to q(x, y)]$

Exercise 3.13. Let x be an integer and use the following propositional functions

- $p(x)$: x is even
- $q(x)$: x is odd
- $r(x)$: $x^2 < 0$

to show that formulas u and v are not logically equivalent.

1. $u : \forall x, [p(x) \vee q(x)]; \quad v : [\forall x, p(x)] \vee [\forall x, q(x)]$
2. $u : \exists x, [p(x) \wedge q(x)]; \quad v : [\exists x, p(x)] \wedge [\exists x, q(x)]$
3. $u : \forall x, [p(x) \to q(x)]; \quad v : [\forall x, p(x)] \to [\forall x, q(x)]$
4. $u : \exists x, [p(x) \to r(x)]; \quad v : [\exists x, p(x)] \to [\exists x, r(x)]$

Exercise 3.14. Let A be a set. Verify that

1. $\exists x \in A, [p(x) \vee q(x)] \equiv [\exists x \in A, p(x)] \vee [\exists x \in A, q(x)]$
2. $\forall x \in A, [p(x) \wedge q(x)] \equiv [\forall x \in A, p(x)] \wedge [\forall x \in A, q(x)]$
3. $\exists x \in A, [p(x) \rightarrow q(x)] \equiv [\exists x \in A, P(x)] \rightarrow [\exists x \in A, q(x)]$

Exercise 3.15. Assume the domain of discourse is the set of integers and determine which of the following statements are true and which are false. Explain your answers.

1. $\forall x, \forall y, x = y$
2. $\forall x, \exists y, xy = 1$
3. $\exists x, \forall y, xy = y$
4. $\forall x, \forall y, \exists z, xy = z$
5. $\forall x, \forall y, xy = yx$
6. $\forall x, \exists y, xy = x$
7. $\forall x, \exists x, \forall z, xy = z$

Exercise 3.16. Assume the domain of discourse is the set of integers and write the negation of the statement without using any negative words. Then explain if the statement is true or not.

1. $\exists!\, n, n^2 = 4$
2. $\exists! n, n$ has exactly two positive divisors
3. $\exists! n, n < 100$ and $n^2 > 50$

Exercise 3.17. Verify the following argument is valid by constructing a truth table. Write a column proof. Write a paragraph proof.

$$\begin{array}{l} p \vee q \\ \neg\, q \rightarrow r \\ \neg\, p \vee \neg\, r \\ \hline \therefore p \end{array}$$

Exercise 3.18. Another logical connective is called the *exclusive or* and is denoted by $\underline{\vee}$. It is defined by the following table:

p	q	$p \underline{\vee} q$
T	T	F
T	F	T
F	T	T
F	F	F

1. Prove that $\veebar$ obeys the commutative and associative properties.
2. Prove that $p \veebar q \equiv (p \wedge \neg q) \vee ((\neg q) \wedge y)$.
3. Prove that $p \veebar q \equiv (p \vee q) \wedge (\neg(q \wedge y))$.
4. Explain why (2) and (3) are important to know.

Explain why $\veebar$ is called the exclusive or.

Exercise 3.19. Use the method of contradiction to prove the following.

1. $\sqrt{3}$ is irrational,
2. $\sqrt[5]{3}$ is irrational.

Exercise 3.20. Let x be a real number. Use the method of contradiction to prove:

$$\text{If } x^3 + 4x = 0, \text{ then } x = 0.$$

Exercise 3.21. Use a counterexample to disprove the statement

$$\text{If } p \text{ is an odd prime, then } p^2 + 4 \text{ is prime.}$$

Exercise 3.22. Let q, q, and r denote the following statements:

- p: Sam knows who to write proofs.
- q: Sam knows who to find counterexamples.
- r: Sam has taken Math 3300.

Express, as simple as possible, each formula in words.

1. $r \leftrightarrow (p \vee q)$
2. $r \rightarrow \neg q$
3. $r \wedge \neg p$
4. $q \leftrightarrow (r \wedge \neg p)$
5. $(p \wedge q) \vee \neg r$
6. $p \wedge (r \rightarrow q)$

Exercise 3.23. Find and simplify the negation of each formula.

1. $p \wedge q \wedge r$
2. $p \rightarrow (q \rightarrow r)$
3. $p \rightarrow (q \vee r)$
4. $p \wedge (p \rightarrow q) \wedge (q \rightarrow r)$
5. $[p \wedge (q \rightarrow r)] \vee (\neg q \wedge p)$

6. $p \leftrightarrow q$
7. $p \wedge (q \vee r)$
8. $\neg p \wedge (q \to p)$

Exercise 3.24. Verify each of the following logical equivalencies.

1. $[(p \wedge q) \to r] \equiv [p \to (q \to r)]$
2. $[(p \vee q) \to r] \equiv [(p \to r) \wedge (q \to r)]$
3. $[p \to (q \wedge r)] \equiv [(p \to q) \wedge (p \to r)]$
4. $[p \to (q \vee r)] \equiv [(p \wedge \neg r) \to q]$

Exercise 3.25. Verify if the argument is valid.

1. $$\begin{array}{l} p \to q \\ \neg\, r \to \neg\, q \\ \hline \therefore \neg\, r \to \neg\, p \end{array}$$

2. $$\begin{array}{l} p \longleftrightarrow q \\ p \\ \hline \therefore q \end{array}$$

3. $$\begin{array}{l} p \vee q \\ \neg\, p \\ \hline \therefore q \end{array}$$

4. $$\begin{array}{l} p \wedge q \\ \neg\, p \to q \\ \hline \therefore \neg\, q \end{array}$$

5. $$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

6. $$\begin{array}{l} p \to q \\ \neg\, q \\ \hline \therefore p \to r \end{array}$$

7. $$\begin{array}{l} p \to q \\ q \\ \hline \therefore p \end{array}$$

8. $$\begin{array}{l} p \to q \\ \neg\, p \\ \hline \therefore \neg\, q \end{array}$$

9. $$\begin{array}{l} p \to q \\ \neg\, q \to \neg\, r \\ \hline \therefore r \to p \end{array}$$

10. $$\begin{array}{l} p \to q \\ \neg\, p \to \neg\, q \\ p \wedge \neg\, r \\ \hline \therefore s \end{array}$$

Exercise 3.26. Write a column proof for each of the arguments in Exercise 3.25 that are valid.

Exercise 3.27. Write a paragraph proof for each of the arguments in Exercise 3.25 that are valid.

Exercise 3.28. Write both a column proof and a paragraph proof.

1. Given the four previously proven theorems:
   - Theorem 1: $\neg p \wedge q$,
   - Theorem 2: $r \to p$,
   - Theorem 3: $\neg r \to s$.
   - Theorem 4: $s \to t$.

Prove the next theorem: Theorem: t.

2. Given the three previously proven theorems:
   - Theorem 1: $p \to q$,
   - Theorem 2: $\neg p \to r$, and
   - Theorem 3: $r \to s$.

Prove the next theorem: Theorem: $\neg q \to s$.

Exercise 3.29. Using the Incidence Axioms do each of the following.

1. Write each Incidence Axiom in symbolic form.
2. Write the negation of each Incidence Axiom in symbolic form.
3. Write the negation of each Incidence Axiom in words.

Exercise 3.30. Write careful arguments to explain why each inference rule Table 2.1 for quantified statements is valid.

Exercise 3.31. Prove each of the following statements using the Incidence Axioms. First write a column proof and then write a paragraph proof.

1. For every line l, $l = l$.
2. For every line l and every line m, if $l = m$ then $m = l$.
3. For every line l, m, and n, if $l = m$ and $m = n$, then $l = n$.

Exercise 3.32. Prove each of the following statements using the Incidence Axioms. First write a column proof and then write a paragraph proof.

1. There exists at least one line.
2. There exists at least two lines.
3. There exists at least three points.
4. There exists at least three lines.

5. Every point is on at least one line.

Exercise 3.33. Prove each of the following statements using the Incidence Axioms. First write a column proof and then write a paragraph proof.

1. For every line l, there is at least one point not lying on l.
2. For every point A, there exist at least two distinct lines through A.
3. If C is on $l(A, B)$ and distinct from A and B, then $l(C, A) = l(B, C) = l(A, B)$
4. If $l(A, B) = l(A, C)$ and B and C are distinct, then $l(A, B) = l(B, C)$.
5. If l is any line, then there exists lines m and n such that l, m, and n are distinct and both m and n have a point in common with l.
6. If A is any point, then there exist points B and C such that A, B, and C are noncollinear.
7. If A and B are two distinct points, then there exists a point C such that A, B, and C are noncollinear.

Exercise 3.34. Determine which of the following sentences or pairs of sentences are propositions. For those that are not, explain why not.

1. A bird has two legs or an insect has six legs.
2. The lake water is boiling hot.
3. Does ice float?
4. Do pigs tell lies?
5. This sentence has four errors.
6. The following sentence is false. The preceding sentence is true.

Exercise 3.35. Write a truth table for each of the following propositional forms.

1. $p \vee (q \wedge \neg p)$
2. $p \wedge \neg(p \wedge p)$
3. $(p \vee q) \wedge (p \wedge c)$
4. $(\neg p \vee q) \wedge (r \vee \neg q)$
5. $(p \vee \neg(r \wedge \neg q)) \wedge \neg p$
6. $(p \vee \neg q) \wedge (q \wedge \neg r)$

Exercise 3.36. Determine whether the following given propositional forms is a tautology, a contradiction, or neither. Justify.

1. $(p \wedge \neg q) \wedge (q \vee \neg p)$

2. $(q \vee \neg p) \vee (r \wedge \neg q)$
3. $(p \wedge \neg r) \vee (r \wedge \neg q)$
4. $\neg(q \vee r \vee \neg p) \wedge (p \wedge r \wedge \neg q)$
5. $(p \vee (q \wedge r)) \vee (q \vee \neg r)$

Exercise 3.37. Decide which of the following propositions that follow are true and which are false. If a proposition is false, provide a counterexample to it.

1. $\forall x \in \mathbb{N}, x^2 + 3x + 2 \geq 0$
2. $\forall x \in \mathbb{Z}, x^2 + 3x + 2 \geq 0$
3. $\forall x \in \mathbb{Q}, x^2 + 3x + 2 \geq 0$
4. $\forall x \in \mathbb{R}, x^2 + 3x + 2 \geq 0$

Exercise 3.38. Write a working negation of each of the following statements. If the statement is in words, write the negation in words; if it is symbols, write the negation in symbols.

1. Every integer is even or odd.
2. Every line segment has a unique midpoint.
3. $\forall \epsilon > 0, \exists\ K \in \mathbb{N}, \forall n, m \in \mathbb{N}$ s.t. $((n > K \wedge m > K) \rightarrow |x_n - x_m| < \epsilon)$
4. Every natural number has a prime divisor.
5. There is no largest integer.
6. $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}$ s.t. $m > n$

Exercise 3.39. Let x be a positive integer and define the following propositional functions:

$$p(x) : x \text{ is prime}, \qquad q(x) : x \text{ is even}, \qquad r(x) : x > 2.$$

Write out each statement in words.

1. $\exists x, p(x)$
2. $\exists x, [p(x) \wedge q(x)]$
3. $\forall x, r(x)$
4. $\forall x, [r(x) \rightarrow (p(x) \vee q(x))]$
5. $\forall x, [(p(x) \wedge q(x)) \rightarrow \neg r(x)]$
6. $\exists x, [p(x) \wedge (q(x) \vee r(x))]$

Exercise 3.40. Find the working negation (negation in simplest form) of each formula.

1. $\forall x, [p(x) \vee q(x)]$

2. $\forall x, [\exists y, (p(x, y) \to q(x, y))]$
3. $\exists x, [(\forall x, p(x, y) \to q(x, y)) \wedge \exists z, r(x, z)]$
4. $\forall x, \forall y, [p(x, y) \to q(x, y)]$

Exercise 3.41. Let x be an integer and use the following propositional functions

- $p(x)$: x is even
- $q(x)$: x is odd
- $r(x)$: $x^2 < 0$

to show that formulas u and v are not logically equivalent.

1. $u : \forall x, [p(x) \vee q(x)]; \quad v : [\forall x, p(x)] \vee [\forall x, q(x)]$
2. $u : \exists x, [p(x) \wedge q(x)]; \quad v : [\exists x, p(x)] \wedge [\exists x, q(x)]$
3. $u : \forall x, [p(x) \to q(x)]; \quad v : [\forall x, p(x)] \to [\forall x, q(x)]$
4. $u : \exists x, [p(x) \to r(x)]; \quad v : [\exists x, p(x)] \to [\exists x, r(x)]$

Exercise 3.42. Let A be a set. Verify that

1. $\exists x \in A, [p(x) \vee q(x)] \equiv [\exists x \in A, p(x)] \vee [\exists x \in A, q(x)]$
2. $\forall x \in A, [p(x) \wedge q(x)] \equiv [\forall x \in A, p(x)] \wedge [\forall x \in A, q(x)]$
3. $\exists x \in A, [p(x) \to q(x)] \equiv [\exists x \in A, P(x)] \to [\exists x \in A, q(x)]$

Exercise 3.43. Assume the domain of discourse is the set of integers and determine which of the following statements are true and which are false. Explain your answers.

1. $\forall x, \forall y, x = y$
2. $\forall x, \exists y, xy = 1$
3. $\exists x, \forall y, xy = y$
4. $\forall x, \forall y, \exists z, xy = z$
5. $\forall x, \forall y, xy = yx$
6. $\forall x, \exists y, xy = x$
7. $\forall x, \exists x, \forall z, xy = z$

Exercise 3.44. Assume the domain of discourse is the set of integers and write the negation of the statement without using any negative words. Then explain if the statement is true or not.

1. $\exists!\, n, n^2 = 4$
2. $\exists! n, n$ has exactly two positive divisors
3. $\exists! n, n < 100$ and $n^2 > 50$

Exercise 3.45. Verify the following argument is valid by constructing a truth table. Write a column proof. Write a paragraph proof.

$$\begin{array}{l} p \vee q \\ \neg\, q \rightarrow r \\ \neg\, p \vee \neg\, r \\ \hline \therefore p \end{array}$$

Exercise 3.46. Another logical connective is called the *exclusive or* and is denoted by $\veebar$. It is defined by the following table:

p	q	$p\veebar q$
T	T	F
T	F	T
F	T	T
F	F	F

1. Prove that $\veebar$ obeys the commutative and associative properties.
2. Prove that $p\veebar q \equiv (p \wedge \neg q) \vee ((\neg q) \wedge y)$.
3. Prove that $p\veebar q \equiv (p \vee q) \wedge (\neg(q \wedge y))$.
4. Explain why (2) and (3) are important to know.

Explain why $\veebar$ is called the exclusive or.

Exercise 3.47. Use the method of contradiction to prove the following.

1. $\sqrt{3}$ is irrational,
2. $\sqrt[5]{3}$ is irrational.

Exercise 3.48. Let x be a real number. Use the method of contradiction to prove:

$$\text{If } x^3 + 4x = 0, \text{ then } x = 0.$$

Exercise 3.49. Use a counterexample to disprove the statement

$$\text{If } p \text{ is an odd prime, then } p^2 + 4 \text{ is prime.}$$

Exercise 3.50. Let q, q, and r denote the following statements:

- p: Sam knows who to write proofs.

- q: Sam knows who to find counterexamples.
- r: Sam has taken Math 3300.

Express, as simple as possible, each formula in words.

1. $r \leftrightarrow (p \vee q)$
2. $r \to \neg q$
3. $r \wedge \neg p$
4. $q \leftrightarrow (r \wedge \neg p)$
5. $(p \wedge q) \vee \neg r$
6. $p \wedge (r \to q)$

Exercise 3.51. Find and simplify the negation of each formula.

1. $p \wedge q \wedge r$
2. $p \to (q \to r)$
3. $p \to (q \vee r)$
4. $p \wedge (p \to q) \wedge (q \to r)$
5. $[p \wedge (q \to r)] \vee (\neg q \wedge p)$
6. $p \leftrightarrow q$
7. $p \wedge (q \vee r)$
8. $\neg p \wedge (q \to p)$

Exercise 3.52. Verify each of the following logical equivalencies.

1. $[(p \wedge q) \to r] \equiv [p \to (q \to r)]$
2. $[(p \vee q) \to r] \equiv [(p \to r) \wedge (q \to r)]$
3. $[p \to (q \wedge r)] \equiv [(p \to q) \wedge (p \to r)]$
4. $[p \to (q \vee r)] \equiv [(p \wedge \neg r) \to q]$

Chapter 4

Set Theory

Set theory is the study of sets, which are (informally speaking) collections of objects. The objects in a set can be anything: numbers, points in space, people, etc. Sets can be finite or infinite (more numerous?).

The basic concepts of set theory include sets, subsets, unions, intersections, power sets, products, functions, and relations. The objects in a set are called elements of the set. A subset is a set that is contained within another set. The union of two sets is the set of all elements that are in either of the two sets. The intersection of two sets is the set of all elements that are in both of the two sets. There is so much to dicusss because set theory is quite rich with ideas and results.

Set theory is a branch of mathematics that is used in many other areas of mathematics, such as geometry, algebra, and analysis. It is also used in computer science, particularly in the design and analysis of algorithms.

Set theory has a long and rich history. Some of the earliest work on sets was done by the Greek philosopher Aristotle, who studied sets of objects that could be added together to form a whole. In the late 19th century, Georg Cantor developed the axiomatic approach to set theory and made major contributions to the study of infinite sets. In the early 20th century, Kurt Gödel proved that set theory was consistent, and in the 1940s, he used set theory to prove the existence of infinitely many different types of sets.

In the axiomatic approach to set theory, sets are defined using a set of axioms, or rules. The most famous of these axioms is the Axiom of Extensionality, which states that two sets are equal if they have the same elements.

4.1 What is a set?

We leave the term **set** undefined. We also leave the term **belonging** undefined. We say x belongs to a set A and we write $x \in A$. We instead, sometimes say x is an **element** of A, or even x is a **member** of a set A. We will say that a set is a collection of objects. The **universe**, or universal set, usually denoted by U, is the set of all elements under discussion.

For example, if U consists of the elements: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10, then the equation

$$A = \{0, 1, 2, 3, 4, 5\}$$

describes a set A made up of the six elements 0, 1, 2, 3, 4, and 5.

A set is determined by its elements and not by any particular order. In other words, set A is just as easily specified by

$$A = \{5, 4, 3, 2, 1, 0\}.$$

Sets are often described by properties of the elements using the **set-builder notation**

$$\{\quad \mid \qquad\} \qquad \text{or} \qquad \{\quad : \qquad\}$$

A variable is indicated before the colon, and the properties are given after the colon. For example,

$$\{n \mid n \in \mathbb{N} \text{ and } n \text{ is odd}\}. \tag{4.1}$$

represents the set of nonnegative odd integers, i.e. the set $\{0, 1, 3, 5, 7, ...\}$. The colon is alway read and so (4.1) can be read as "the set of all n such that n is a natural number and is odd".

Throughout we use $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ to denote the set of natural numbers, the set of integers, and the set of rational numbers, respectfully. Note that we include 0 among the **natural numbers**:

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, ...\}.$$

The set of all positive, zero, or negative numbers, are called the **integers**. Numbers of the form m/n, where m, n are integers and $n \neq 0$ are called the **rational numbers** since they are ratios of integers. The set of **real numbers**, rational or not, contains all the numbers in $\mathbb{Q}$, and many others as well such as $\sqrt{2}$, $\sqrt{3}$, $\sqrt[3]{3}$, $\sqrt[5]{3}$, π, and e and so on.

The most basic property of belonging is that of **equality**. For example, if

$$A = \{x \in \mathbb{R} \mid -9 + 21x - 10x^2 = 0\}, \quad B = \left\{\frac{3}{5}, \frac{3}{2}\right\}$$

then $A = B$. To see this notice that $-9+21x-10x^2 = (2x-3)(3-5x) = 0$ precisely when $x = 3/5$ or $x = 3/2$.

4.2 Principle of Extension

Extension. Two sets are equal if and only if they contain the same elements.

Definition 4.1. Two sets A and B are called **equal**, denoted by $A = B$, provided they consist of the same elements. If A and B are not equal we write $A \neq B$.

Let A and B be sets. If every element of A is an element of B, we say A is a **subset** of B, or B **contains** A, and we write $A \subseteq B$, or $B \supseteq A$. Notice that **set inclusion** $\subseteq$ has a few nice properties. It is **reflexive**, meaning $A \subseteq A$ for any set A; and is **transitive**, meaning, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$ for all sets A, B, C.

By the principle of extension, set inclusion is also meaning $A \subseteq B$ and $B \subseteq A$ together imply $A = B$. You might have noticed that equality is also reflexive and transitive. Equality is also **symmetric**, meaning if $A = B$ then $B = A$, for all sets A, B.

4.3 Specification

The next principle is designed to produce new sets out of known ones. We use the notation $P(x)$ to mean a mathematical statement P which depends on the free variable x.

Specification. To every set A and to every condition $P(x)$ there corresponds a set B whose elements are exactly those elements x of A for which $P(x)$ holds.

By Extension, the set B in the Specification is uniquely determined. Also by Specification, the set $\{x \in A \mid x \neq x\}$, denoted by $\emptyset$, exists and is called the **empty set**. This of course assumes that there exists a set A in the first place, as we have assumed all along. Of course the empty set is a subset of every set. The next question that comes to mind is: are there enough sets to ensure that every set belongs to some set?

Let A and B be sets. If every element of A is an element of B, we say A is a **subset** of B, or sometimes we say B **contains** A, and we write $A \subseteq B$, or $B \supseteq A$. For example, $\{1, 4, a\} \subseteq \{0, 1, 3, 4, a, b\}$ or as another example the inclusions hold $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

Definition 4.2. A set A is called a **subset** of a set B, denoted by $A \subseteq B$, provided every element of A is also an element of B.

The symbol $\emptyset$ is the last letter in the Danish-Norwegian alphabet.

Definition 4.3. The unique set that has no elements is called the **empty set** and is denoted by $\emptyset$.

Recall the tautologies $p \to p$ and $((p \to q) \wedge (q \to r)) \to (p \to r)$.

Theorem 4.1. *Let A, B, and C be subsets of a universal set U.*

1. $A \subseteq A$
2. $(A \subseteq B \wedge B \subseteq C) \to A \subseteq C$.

Proof. Let x be an arbitrary element of A. Then x is in A and so $A \subseteq A$. For the second statement, assume x be an arbitrary element of A. Since $A \subseteq B$, we have $x \in B$ by definition of subset. Since $B \subseteq C$, we have $x \in C$ by definition of subset, whence $A \subseteq C$.

□

To show that $A = B$ one must prove that $x \in A \leftrightarrow x \in B$; that is, $x \in A$ if and only if $x \in B$. This is equivalent to proving that $x \in A \to x \in B$ and $x \in B \to x \in A$. There are two parts to such a proof: first assume that $x \in A$ and show that $x \in B$ follows. Then assume, independently, that $x \in B$ and show that $x \in A$ follows.

The reader is encourage to justify each step in this proof.

Theorem 4.2. *For any two subsets A and B of a universal set U,*

$$A = B \leftrightarrow (A \subseteq B \wedge B \subseteq A). \tag{4.2}$$

Proof. We proceed as follows

$$\begin{aligned} A = B &\leftrightarrow \forall x, (x \in A \leftrightarrow x \in B) \\ &\leftrightarrow \forall x, [(x \in A \to x \in B) \wedge (x \in B \to x \in A)] \\ &\leftrightarrow [\forall x, x \in A \to x \in B] \wedge [\forall x, (x \in B \to x \in A)] \\ &\leftrightarrow (A \subseteq B) \wedge (B \subseteq A) \end{aligned}$$

as needed.

□

Theorem 4.3. *For any two subsets A and B of a universal set U,*

$$A \subseteq B \leftrightarrow \forall C(C \subseteq A \to C \subseteq B). \tag{4.3}$$

Proof. First we show that

$$\forall C, (C \subseteq A \to C \subseteq B) \to A \subseteq B. \tag{4.4}$$

Assume that for any set C, if $C \subseteq A$, then $C \subseteq B$. Since $A \subseteq A$, it follows that $A \subseteq B$ as needed. Next it must be shown that

$$A \subseteq B \to \forall C, (C \subseteq A \to C \subseteq B). \tag{4.5}$$

Assume $A \subseteq B$ and let C be any set such that $C \subseteq A$. Then we have $C \subseteq A$ and $A \subseteq B$, and so we have $C \subseteq B$.

□

Theorem 4.4. *Let A be a subset of a universal subset U. Then for all $x \in U$,*

$$x \in A \leftrightarrow \{x\} \subseteq A. \tag{4.6}$$

Proof. The proof is left for the reader as Exercise 4.20.

□

Set inclusion is also **antisymmetric** meaning $A \subseteq B$ and $B \subseteq A$ together imply $A = B$. Equality is also **symmetric**, meaning if $A = B$ then $B = A$, for all sets A, B.

Theorem 4.5. *For any two subsets A and B of a universal set U,*

1. $A = B \leftrightarrow B = A$, *and*
2. $(A \subseteq B \wedge B \subseteq A) \to A = B$.

Proof. The proof is left for the reader as Exercise 4.21.

□

4.4 Proper Subset

A subset B of a set A is said to be a proper subset of A if it is not equal to A itself. Thus all subsets of A are proper subsets except the set A itself, which is referred to as the **improper subset** of A.

Definition 4.4. A set A is called a **proper subset** of a set B provided $A \subseteq B$ and $A \neq B$. We write $A \subset B$ to denote that A is a proper subset of B.

Theorem 4.6. *For any two subsets A and B of a universal set U,*

$$A \subset B \leftrightarrow [A \subseteq B \wedge \exists x, (x \in B \wedge x \notin A)]. \tag{4.7}$$

Proof. Assume $A \subset B$. Then $A \subseteq B$ and $A \neq B$. By definition of $A \neq B$, one must hold

$$\exists x, (x \in A \wedge x \notin B) \quad \text{or} \quad \exists x, (x \in B \wedge x \notin A).$$

If the first one holds, then we have $x \in B$ and $x \notin B$, a contradiction. Hence the former holds as needed. Conversely, assume $A \subseteq B$ and $\exists x, (x \in B \wedge x \notin A)$. Then by definition of $A \neq B$, since B contains an element not in A, we have $A \neq B$. Therefore we have $A \subseteq B$ and $A \neq B$, and thus $A \subset B$.

□

4.5 Why elelmentary set theory?

In the foundations of mathematics, Russell's paradox, discovered by Bertrand Russell in 1901, showed that the naive set theory created by Georg Cantor leads to a contradiction. According to naive set theory, any definable collection is a set.

Let R be the set of all sets that are not members of themselves. If R is not a member of itself, then its definition dictates that it must contain itself, and if it contains itself, then it contradicts its own definition as the set of all sets that are not members of themselves.

This contradiction is called **Russell's paradox**. Symbolically:

$$\text{If } R = \{x \mid x \notin x\}, \text{ then } R \in R \leftrightarrow R \notin R.$$

In 1908, two ways of avoiding the paradox were proposed, Russell's type theory and the Zermelo set theory. There is a long interesting history of this problem and the reader is encourage to explore.

4.6 Axiom of Choice

In 1904, Ernst Zermelo formulated the Axiom of Choice to prove the Well-Ordering Theorem [**?**]. Of course, we now know that these two statements are logically equivalent and in fact, there are many equivalents forms Adamson (1998).

Theorem 4.7. *In Zermelo-Fraenkel set theory, the following statements are equivalent:*

1. *(Axiom of Choice) Given any set X of pairwise disjoint non-empty sets, there exists at least one set B that contains exactly one element in common with each of the sets in X. Suppes (1972)*
2. *(Well-Ordering) Every set can be well-ordered. (Cantor 1883)*

Said differently, and in particular, the Axiom of Choice guarantees that every finite collection of nonempty sets has a choice function. However, in Zermelo-Fraenkel set theory, this is easily proven using mathematical induction (Tourlakis 2003). The following statements are also weaker than the Axiom of Choice.

Harzheim (2005)

Theorem 4.8. *Every partial order can be extended to a total order and every well-founded partial order can be extended to a well-order.*

4.7 Set Operations

Power Sets

The next question that comes to mind is: is the collection of subsets of a set, a set itself? In other words, given a set A does there exist a set $\mathcal{P}$ such that if $X \subseteq A$ then $X \in \mathcal{P}$?

Definition 4.5. The set consisting of all subsets of a given set A is called the **power set** of A and is denoted by $\mathcal{P}(A)$.

Theorem 4.9. *If A is a set, then $\emptyset \in \mathcal{P}(A)$ and $A \in \mathcal{P}(A)$.*

Proof. Notice that the empty set is a subset of every set (including itself). Thus, $\emptyset \in \mathcal{P}(A)$ is immediate. The second statement follows immediately; that is, $A \subseteq A$ implies $A \in \mathcal{P}(A)$.

□

Theorem 4.10. *If A has n elements, then $\mathcal{P}(A)$ has 2^n elements.*

Proof. If $n = 0$, then A is the empty set. The only subset of the empty set is the set itself; thus the number of elements in $\mathcal{P}(A)$ is 1 which is 2^0 as needed to verify the basis step.

Assume that the statement holds for n. Let X be a set with $n+1$ elements and assume $x \in X$. We claim that exactly half of the subsets of X contain x, and half do not. To see this, notice that each subset of X that contains x can be paired uniquely with a subset obtained by removing x.

subsets of A that contain x	subsets of A that do not contain x
$\{x\}$	$\emptyset$
$\{x, y\}$	$\{y\}$
$\{x, z\}$	$\{z\}$
$\{x, y, z\}$	$\{y, z\}$

If we let Y be the set obtained from X by deleting x, Y has n elements. By the inductive hypothesis $\mathcal{Y}$ has exactly 2^n elements. But the subsets of Y are precisely the subsets of X that do not contain x. It follows that the number of elements in $\mathcal{Y}$ is one-half the number of elements in $\mathcal{X}$. Therefore, the number of elements in $\mathcal{X}$ is twice the number of elements in $\mathcal{Y}$. Whence the number of elements in $\mathcal{X}$ is 2^{n+1}.

□

Theorem 4.11. *If A is an infinite set, then $\mathcal{P}(A)$ is also.*

Proof. The proof is left for the reader as Exercise 4.1.

□

Principle of Unions

Union. For every collection of sets there exists a set that contains all the elements that belong to at least one set of the given collection.

Given a collection of sets $\mathcal{C}$ we want their union to consist of only those elements that belong to at least one of the subsets in the collection. So we apply the principle of specification to the set U and define the **union** of a collection of sets as

$$\bigcup_{X \in \mathcal{C}} X = \{x \in U \mid x \in X \text{ for some } X \text{ in } \mathcal{C}\}.$$

This set exists by the principle of specification and is unique by the principle of extension. In the case $\mathcal{C} = \{A, B\}$ we usually write

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

Theorem 4.12. *Let A, B, and C be sets. Then*

1. $A \cup \emptyset = A$,
2. $A \cup B = B \cup A$,
3. $A \cup (B \cup C) = (A \cup B) \cup C$,
4. $A \cup A = A$, *and*
5. $A \subseteq B$ *if and only if* $A \cup B = B$.

Proof. The proof is left for the reader as Exercise 4.2.

□

If A and B are sets we then define, using the principle of specification, their intersection as the set $A \cap B = \{x \in A \mid x \in B\}$. It is very easy to show the more familiar form, $A \cap B = \{x \mid x \in A \text{ or } x \in B\}$. More generally, let $\mathcal{C}$ be a non-empty collection of sets, the principle of specification allows us to define a set

$$I = \{x \in A \mid x \in X \text{ for every } X \text{ in } \mathcal{C}\}$$

where A is some set in $\mathcal{C}$. In fact the use of a set A is arbitrary (but necessary in order to use the principle of specification). Thus we are lead to the definition of the **intersection** of a collection of sets

$$\bigcap_{X \in \mathcal{C}} X = \{x \mid x \in X \text{ for all } X \text{ in } \mathcal{C}\ \}$$

where uniqueness is guaranteed by the principle of extension.

Theorem 4.13. *Let A, B, and C be sets. Then*

1. $A \cap \emptyset = \emptyset$,
2. $A \cap B = B \cap A$,
3. $A \cap (B \cap C) = (A \cap B) \cap C$,
4. $A \cap A = A$, *and*
5. $A \subseteq B$ *if and only if* $A \cap B = A$.

Proof. The proof is left for the reader as Exercise 4.3.

□

Let A and B be subsets of a set C. The between A and B, known as the of B in A, is the set defined by $A - B = \{x \in A \mid x \notin B\}$; and the **difference} between A and B, known as the of B in A, is the set defined by $A - B = \{x \in A \mid x \notin B\}$; and the \index{symmetric difference** of A and B is defined by $A + B = (A - B) \cup (B - A)$. Notice that the principle of specification guarantees existence and the principle of extension guarantees uniqueness of these sets for a given A and B. These sets are of course, by definition, also subsets of C.

The next question that comes to mind is: is the collection of subsets of C a set itself? In other words, given a set C does there exist a set $\mathcal{P}$ such that if $X \subseteq S$ then $X \in \mathcal{P}$?

Principle of Powers

Principle of Powers. For each set there exists a collection of sets that contains among its elements all the subsets of the given set.

Thus, given a set C we can form a collection of sets, denoted by $\mathcal{P}$, that contains the subsets of C. We can use the principle of specification to ensure that this set will consist only of subsets of C and the principle of extension to ensure that this set is unique. We call this set the **power set** of C, and denote it by $\mathcal{P}(S) = \{X \mid X \subseteq S\}$ or sometimes even 2^S.

The fundamental most frequently used operations of set theory are union, intersection, and difference.

In this section we discuss these operations and some of their properties.

The **union** of a collection of sets is the set of all distinct elements in the collection.

Definition 4.6. Let A and B be subsets of some universal set U. The **union** of A and B is the set $A \cup B$ defined by

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

Recall that $p \to (p \vee q)$ is a tautology. This immediately yields that for any sets A and B,

$$A \subseteq A \cup B \qquad \text{and} \qquad B \subseteq A \cup B. \tag{4.8}$$

This follows because $A \subseteq A \cup B$ is equivalent to $\forall x, x \in A \to (x \in A \vee x \in B)$ by definition of subset. Similarly for $B \subseteq A \cup B$.

Example 4.1. Let $U = \{1, 2, 3, \dots, 10\}$, $A = \{2, 4, 6\}$, $B = \{1, 3, 5, 7, 9\}$ and $C = \{5, 10\}$. Find and compare the sets: $A \cup (B \cup C)$ and $(A \cup B) \cup C$

Proof. We find $B \cup C = \{1, 3, 5, 7, 9, 10\}$ and so

$$A \cup (B \cup C) = \{1, 2, 3, 4, 5, 6, 7, 9, 10\}.$$

Also, $A \cup B = \{1, 2, 3, 4, 5, 6, 7, 9\}$ and so

$$(A \cup B) \cup C) = \{1, 2, 3, 4, 5, 6, 7, 9, 10\}.$$

Therefore we find that $A \cup (B \cup C) = (A \cup B) \cup C$.

□

Theorem 4.14. *Let A and B be subsets of some universal set U.*

1. $A \cup \emptyset = A$
2. *(* ***commutativity****)* $A \cup B = B \cup A$
3. *(* ***associativity****)* $A \cup (B \cup C) = (A \cup B) \cup C$
4. *(* ***idempotence****)* $A \cup A = A$
5. $A \subseteq B$ *if and only if* $A \cup B = B$.

Proof. We prove (1) and (5) and leave the remainder of the proof for the reader as Exercise 4.5.

(1): Let x be an arbitrary element of $A \cup \emptyset$. Then, by definition of union, either $x \in A$ or $x \in \emptyset$. Since there are no elements in $\emptyset$, we must have $x \in A$; hence $A \cup \emptyset \subseteq A$. Conversely, follows from (4.8).

(5): Assume $A \subseteq B$. We must show that $A \cup B = B$. By (4.8) we immediately see that $B \subseteq A \cup B$. To show the remaining inclusion, let $x \in A \cup B$. Then either $x \in A$ or $x \in B$. In the case that $x \in A$, then we have $x \in B$ by hypothesis. Thus, in either case we have $x \in B$, and so $A \cap B \subseteq B$. Therefore, we have shown that if $A \subseteq B$, then $A \cap B = B$.

Conversely, we now assume that $A \cup B = B$ and we wish to conclude that $A \subseteq B$. To do so, let x be an arbitrary element of A. Then $x \in A \cup B$ by (4.8), and so $x \in A \cup B = B$. Hence $A \subseteq B$ as needed.

□

The intersection of a collection of sets is the set that contains all elements, each of which are in each of the sets in the collection, and no other elements.

Principle of Intersections

Definition 4.7. Let A and B be subsets of some universal set U. The **intersection** of A and B is the set $A \cap B$ defined by

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

Theorem 4.15. *Let A and B be subsets of some universal set U.*

1. $A \cap \emptyset = \emptyset$
2. *(* ***commutativity****)* $A \cap B = B \cap A$
3. *(* ***associativity****)* $A \cap (B \cap C) = (A \cap B) \cap C$
4. *(* ***idempotence****)* $A \cap A = A$
5. $A \subseteq B$ *if and only if* $A \cap B = A$.

Proof. We prove (2) and (3) and leave the remainder of the proof for the reader as Exercise 4.6.

(2): Let x be an arbitrary element in $A \cap B$. Then

$$\begin{aligned}
& x \in A \cap B \\
& \quad \rightarrow x \in A \wedge x \in B && \text{by Definition of } \cap \\
& \quad \rightarrow x \in B \wedge x \in A && \text{by commutativity of } \wedge \\
& \quad \rightarrow x \in B \cap A && \text{by Definition of } \cap
\end{aligned}$$

Thus $x \in A \cap B \rightarrow x \in B \cap A$ and consequently

$$A \cap B \subseteq B \cap A.$$

In a similar fashion (simply reverse the implications) one may prove that $B \cap A \subseteq A \cap B$. Therefore, $A \cap B = B \cap A$.

(3): Let x be an arbitrary element in $(A \cap B) \cap C$. Then

$$\begin{aligned}
& x \in (A \cap B) \cap C \\
& \quad \rightarrow [x \in (A \cap B) \wedge x \in C] && \text{by Definition of } \cap \\
& \quad \rightarrow [(x \in A \wedge x \in B) \wedge x \in C] && \text{by Definition of } \cap \\
& \quad \rightarrow [x \in A \wedge (x \in B \wedge x \in C)] && \text{by associativity of } \wedge \\
& \quad \rightarrow [x \in A \wedge (x \in B \cap C)] && \text{by Definition of } \cap \\
& \quad \rightarrow [x \in (A \cap B) \cap C] && \text{by Definition of } \cap
\end{aligned}$$

Thus $x \in (A \cap B) \cap C \rightarrow x \in A \cap (B \cap C)$ and consequently

$$(A \cap B) \cap C \subseteq A \cap (B \cap C).$$

In a similar fashion (simply reverse the implications) one may prove that $A \cap (B \cap C) \subseteq (A \cap B) \cap C$. Therefore, $A \cap (B \cap C) = (A \cap B) \cap C$.

□

Theorem 4.16. *Let A, B, C be subsets of some universal set U.*

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

Proof. We prove (1) and leave the remainder of the proof for the reader as Exercise 4.7.

(1): Let x be an arbitrary element in $A \cap (B \cup C)$. Then

$$\begin{array}{lll}
x \in A \cap (B \cup C) & & \\
& \to [x \in A \wedge x \in B \cup C] & \text{by Definition of } \cap \\
& \to [x \in A \wedge (x \in B \vee x \in C)] & \text{by Definition of } \cup \\
& \to [(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)] & \text{by distributivity of } \wedge \\
& \to [(x \in A \cap B) \vee (x \in A \cap C)] & \text{by Definition of } \cap \\
& \to [(x \in A \cap B) \cup (A \cap C)] & \text{by Definition of } \cup
\end{array}$$

Thus $x \in A \cap (B \cup C) \to x \in (A \cap B) \cup (A \cap C)$ and consequently

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

In a similar fashion (simply reverse the implications) one may prove that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Therefore, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

□

Relative Complement

The relative complement of B with respect to a set A is the set of elements in A but not in B.

Definition 4.8. Let A and B be subsets of some universal set U. The **relative complement** of B in A is the set $A - B$ defined by

$$A - B = \{x \mid x \in A \wedge x \notin B\}.$$

The relative complement of B in A is also denoted by $A \quad B$.

When all sets under consideration are considered to be subsets of a given set U, the absolute **complement** of A is the set of all elements in U but not in A, and is denoted by A', that is, the complement of a set A is defined by

$$A' = \{x \in U \mid x \notin A\}.$$

To be redundant, by definition $A' = U - A$.

Example 4.2. Let $S = \{a, b, c\}$, $T = \{1, a\}$, and $V = \{1, 2, 3, c\}$. Find and compare the sets, $(S - T) - V$ and $S - (T - V)$.

Proof. We find $S - T = \{b, c\}$ and $T - V = \{a\}$, and so $(S - T) - V = \{b\}$ and $S - (T - V) = \{b, c\}$. Thus, $(S - T) - V \subseteq S - (T - V)$.

□

De Morgan's Laws

Theorem 4.17. *Let A and B be subsets of some universal set U.*

1. $(A \cup B)' = A' \cap B'$
2. $(A \cap B)' = A' \cup B'$.

Proof. We prove (1) and leave the remainder of the proof for the reader as Exercise 4.8. Let x be an arbitrary element in $(A \cup B)'$. Then

$$\begin{array}{ll} x \in (A \cup B)' & \\ \quad \rightarrow [x \notin A \cup B] & \text{by Definition of complement} \\ \quad \rightarrow [\neg(x \in A \cup B)] & \text{by Definition of } \notin \\ \quad \rightarrow [\neg(x \in A \vee x \in B)] & \text{by Definition of } \cup \\ \quad \rightarrow [\neg(x \in A) \wedge \neg(x \in B)] & \text{DeMorgan's Law} \\ \quad \rightarrow [x \notin A \wedge x \notin B] & \text{by Definition of } \notin \\ \quad \rightarrow [x \in A' \wedge x \in B'] & \text{by Definition of complement} \\ \quad \rightarrow [x \in A' \cap B'] & \text{by Definition of } \cap \end{array}$$

Thus $x \in (A \cup B)' \rightarrow x \in A' \cap B'$ and consequently $(A \cup B)' \subseteq x \in A' \cap B'$. In a similar fashion (simply reverse the implications) one may prove that $A' \cap B' \subseteq (A \cup B)'$. Therefore, $(A \cup B)' = A' \cap B'$.

□

Theorem 4.18. *Let A and B be subsets of some universal set U.*

1. $(A')' = A$
2. $\emptyset' = U$
3. $U' = \emptyset$
4. $A \cap A' = \emptyset$
5. $A \cup A' = U$
6. $A - B = A \cap B'$

Proof. The proof is left for the reader as Theorem 4.18.

□

Theorem 4.19. *Let A and B be subsets of some universal set U.*

1. *$A \subseteq B$ if and only if $B' \subseteq A'$*
2. *$A \subseteq B$ if and only if $A - B = \emptyset$*

Proof. We prove (1) and leave the remainder of the proof for the reader as Exercise 4.9. Assume $A \subseteq B$ and let x be an arbitrary element in B'. Thus, $x \notin B$. Assume for a contradiction that $x \in A$. By hypothesis, we have $x \in B$ and $x \notin B$. Thus, $x \in A'$ must occur. Conversely, assume $B' \subseteq A'$ and let x be an arbitrary element of A. Assume for a contradiction that $x \in B'$. By hypothesis, we have $x \in A$ and $x \notin A$. Thus, $x \in B$ must occur.

□

Symmetric Difference

The symmetric difference of two sets is the set of elements which are in either of the sets and not in their intersection.

Definition 4.9. If A and B are sets, we define the **symmetric difference** of A and B by

$$A \bigtriangleup B = (A - B) \cup (B - A).$$

Theorem 4.20. *Let A and B be subsets of some universal set U. Then*

$$A \bigtriangleup B = (A \cup B) - (A \cap B). \tag{4.9}$$

Proof. Let x be an arbitrary element of $A \triangle B$. Then

$$\begin{aligned}
&x \in A \triangle B \\
&\qquad \to x \in (A - B) \cup (B - A) \\
&\qquad \to x \in A - B \vee x \in B - A \\
&\qquad \to (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A) \\
&\qquad \to (x \in B \wedge x \notin A) \vee (x \in A \wedge x \notin B) \\
&\qquad \to [(x \in A \wedge x \notin A) \vee (x \in B \wedge x \notin A)] \\
&\qquad\qquad\qquad \vee [(x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin B)] \\
&\qquad \to [(x \in A \vee x \in B) \wedge x \notin A)] \vee [(x \in A \vee x \in B) \wedge x \notin B)] \\
&\qquad \to (x \in A \vee x \in B) \wedge (x \notin A \vee x \notin B) \\
&\qquad \to (x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B) \\
&\qquad \to x \in (A \cup B) \wedge \neg(x \in A \cap B) \\
&\qquad \to x \in (A \cup B) \wedge x \notin A \cap B \\
&\qquad \to x \in (A \cup B) - (A \cap B)
\end{aligned}$$

The justification of the above steps and the remainder of the proof is left for the reader as Exercise 4.10.

□

Theorem 4.21. *Let A, B, and C be subsets of some universal set U.*

1. $A \triangle B = B \triangle A$
2. $A \triangle (B \triangle C) = (A \triangle B) \triangle C$
3. $A \triangle \emptyset = A$
4. $A \triangle A = \emptyset$

Proof. The proof is left for the reader as Exercise 4.11.

□

Theorem 4.22. *Let A and B be sets. Then*

1. $A + B = B + A$,
2. $A + (B + C) = (A + B) + C$,
3. $A + \emptyset = A$, *and*
4. $A + A = \emptyset$.

Proof. The proof is left for the reader as Exercise 4.12.

□

A collection of sets is called **disjoint** if they have no elements in common.

Definition 4.10. If A and B are sets and $A \cap B = \emptyset$, then A and B are **disjoint sets** .

Theorem 4.23. *Let A and B be subsets of some universal set U. Then A and B are disjoint if and only if $A \cup B = A \bigtriangleup B$.*

Proof. The proof is left for the reader as Exercise 4.13.

□

Principle of Pairing

Principle of Pairing. For any two sets there exists a set that they both belong to.

For example, suppose a and b are sets that are elements of the set A, then by the principle of specification the set $\{a, b\} := \{x \in A \mid x = a \text{ or } x = b\}$ exists, and by the principle of extension is unique. This set is called the **pair** (or **unordered pair**) formed by a and b. Given any set a we have the pair $\{a, a\}$ which is usually just denoted by $\{a\}$, and is called the **singleton set** of a.

Let $\mathcal{C}$ denote a collection of sets. By the following principle we can define the set U consisting of those elements x such that if $x \in X$ for some $X \in \mathcal{C}$, then $x \in U$.

An ordered pair (a, b) is a pair of mathematical objects. The order in which the objects appear in the pair is significant: the ordered pair (a, b) is different from the ordered pair (b, a) unless $a = b$. (In contrast, the unordered pair $\{a, b\}$ equals the unordered pair $\{b, a\}$.)

Cartesian Product

Definition 4.11. Given any two sets A and B, the **Cartesian product** of A and B is the set $A \times B$ defined by

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

Theorem 4.24. *If A, B, and C are sets, then*

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

2. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
3. $A \times (B - C) = (A \times B) - (A \times C)$
4. $A \times (B \triangle C) = (A \times B) \triangle (A \times C)$

Proof. The proof is left for the reader as Exercise 4.14.

□

The idea of ordered pair can be extended to more than two elements. Given n elements $a_1, a_2, \dots, a_n$, where $n \geq 3$, we can define the **ordered** n-tuple $(a_1, a_2, \dots a_n)$, in which a_1 is the first element, a_2 is the second element, and so on, and a_n is the n-th element. We can now generalize the idea of Cartesian product.

Definition 4.12. Given any n sets $A_1, A_2, \dots, A_n$, the Cartesian product of $A_1, A_2, \dots, A_n$ is the set defined by

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i \text{ for each } i,\ 1 \leq i \leq n\}.$$

It follows immediately,

$(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n)$ if and only if $a_i = b_i$ for each i, $1 \leq i \leq n$.

Also notice that $A_1 \times A_2 \times \cdots \times A_n = \emptyset$ if and only if $A_i = \emptyset$ for some i, $1 \leq i \leq n$. For this reason, when working with Cartesian products of sets, it is normally the case that each of the sets is nonempty.

Example 4.3. Prove or disprove that

$$\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B),$$

for any sets A and B.

The **ordered pair** of a and b, with first coordinate a and second coordinate b is defined as the set $\{\{a\}, \{a, b\}\}$ and is denoted more naturally by (a, b). The reader should show that this definition is well-defined by proving the following lemma.

Lemma 4.1. *If (a, b) and (x, y) are ordered pairs and if $(a, b) = (x, y)$ then $x = a$ and $y = b$.*

Proof. The proof is left as an exercise for the reader as Exercise 4.16.

□

The next question that comes to mind is: if A and B are sets, does there exist a set that contains all the ordered pairs (a,b) with $a \in A$ and $b \in B$. Surely so; for example, $\{a\} \subseteq A$ and $\{b\} \subseteq B$, and therefore $\{a,b\} \subseteq A \cup B$. Thus, by definition, $(a,b) = \{\{a\},\{a,b\}\} \subseteq \mathcal{P}(A \cup B)$. It follows that $(a,b) \in \mathcal{P}(\mathcal{P}(A \cup B))$. We can do much better than this though.

The Cartesian product of two sets is a set of ordered pairs. Conversely, every set of ordered pairs is a subset of the Cartesian product of two sets. By the above argument, every set of ordered pairs is contained in some subset, via

$$(a,b) \in \mathcal{P}(\mathcal{P}(A \cup B)) \quad \text{whenever} \quad a \in A, b \in B.$$

By the principle of specification, we define a set

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

By the principle of extension, this set is unique; and is called the **Cartesian product** of A and B. Thus, as desired, the Cartesian product of two sets is a set of ordered pairs. Conversely, let P be a set that consists of ordered pairs and let $x \in P$. Then by definition of ordered pair $x = \{\{a\},\{a,b\}\}$ for some a and for some b. Since P is a set consisting of sets, we form the union and observe $\{a,b\} \in \cup_{X\in P} P$.

Observe further that $\cup_{X\in P} P := P'$ is a set consisting of sets, so it follows both a and b are elements of

$$U := \bigcup_{Y\in P'} \bigcup_{X\in P} P.$$

Let A and B be such that $A = B = U$. Thus P, a set of ordered pairs, is a subset of the Cartesian product of two sets, namely $U \times U$. We can use the principle of specification to refine the sets A and B, namely

$$A = \{a \in U \mid (a,b) \in P \text{ for some } b\}$$

and

$$B = \{b \in U \mid (a,b) \in P \text{ for some } a\}.$$

These sets are unique by the principle of extension and are called the **projections** of P onto the first and second coordinates, respectively.

Theorem 4.25. *Let A, B, X, and Y be sets. Then*

1. $(A \cup B) \times X = (A \times X) \cup (B \times X)$,
2. $(A \cap B) \times (X \cap Y) = (A \times X) \cap (B \times Y)$,
3. $(A - B) \times X = (A \times X) - (B \times X)$,

4. *$(A = \emptyset$ or $B = \emptyset)$ if and only if $A \times B = \emptyset$, and*
5. *If $A \times B \neq \emptyset$ then, $(A \subseteq X$ and $B \subseteq Y)$ if and only if $A \times B \subseteq X \times Y$.*

Proof. The proof is left for the reader as Exercise 4.15.

□

Finite Families

Given any n sets $A_1, A_2, \ldots, A_n$, we define their union to be the set

$$A_1 \cup A_2 \cup \cdots \cup A_n = \{x \mid x \in A_i \text{ for some } i, 1 \leq i \leq n\}.$$

and their intersection to the the set

$$A_1 \cap A_2 \cap \cdots \cap A_n = \{x \mid x \in A_i \text{ for all } i, 1 \leq i \leq n\}.$$

These sets can be written as

$$\bigcup_{i=1}^{n} A_i \qquad \text{and} \qquad \bigcap_{i=1}^{n} A_i$$

respectively.

Example 4.4. For $i \in \{1, 2, 3, \ldots, 10\}$, define

$$A_i = [-i, 10 - i].$$

Find A_1, $A_2, \ldots, A_{10}$ and then find $\bigcup_{i=1}^{10} A_i$ and $\bigcap_{i=1}^{10} A_i$.

Solution. We find that

$$A_1 = [-1, 9], \quad A_2 = [-2, 8], \quad \ldots, \quad A_{10} = [-10, 0].$$

Hence

$$\bigcup_{i=1}^{10} A_i = [-10, 9] \qquad \text{and} \qquad \bigcap_{i=1}^{10} A_i = [-1, 0]. \tag{4.10}$$

as needed.

Example 4.5. For $k \in \{1, 2, \ldots, 100\}$, define

$$B_k = \{r \in \mathbb{Q} \mid -1 \leq k \cdot r \leq 1\}.$$

Find B_k for $1 \leq k \leq 100$, compare these sets, and then find $\bigcup_{k=1}^{100} B_k$ and $\bigcap_{k=1}^{100} B_k$.

Solution. We find

$$B_1 = \{r \in \mathbb{Q} \mid -1 \leq r \leq 1\},$$

$$B_2 = \left\{\{r \in \mathbb{Q} \mid -\frac{1}{2} \leq r \leq \frac{1}{2}\right\},$$

$$\cdots \qquad \cdots$$

$$B_{100} = \left\{r \in \mathbb{Q} \mid -\frac{1}{100} \leq r \leq \frac{1}{100}\right\},$$

and so

$$B_{100} \subseteq B_{99} \subseteq B_{98} \subseteq \cdots \subseteq B_2 \subseteq B_1.$$

It follows that

$$\bigcup_{k=1}^{100} B_k = B_1 \qquad \text{and} \qquad \bigcap_{k=1}^{100} B_k = B_{100}.$$

as needed.

Families of Sets

Let I be a nonempty set, and suppose that for each element $i \in I$ there is associated a set A_i. We then call I an index set for the collection of sets $\mathcal{P}(A) = \{A_i \mid i \in I\}$.

Definition 4.13. Let I be an indexed set and suppose that $\mathcal{P}(A) = \{A_i \mid i \in I\}$ is a collection of sets. Then

1. the $\mathcal{P}(A)$ **union of the collection** is defined to be the set

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ for some } i \in I\},$$

2. the $\mathcal{P}(A)$ **intersection of the collection** is defined to be the set

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for each } i \in I\}.$$

Theorem 4.26. *Given the collection of sets $\{A_i \mid i \in \mathbb{N}\}$ the following properties hold.*

1. *If $A_i \subseteq A_{i+1}$ for all $i \in \mathbb{N}$, then $\bigcap_{i=1} A_i = A_1$.*
2. *If $A_i \supseteq A_{i+1}$ for all $i \in \mathbb{N}$, then $\bigcup_{i=1} A_i = A_1$.*

Proof. We prove (1) and leave (2) for the reader as Exercise 4.17. Let $T = \cap_{i=1} A_i = A_0$ and let x be an arbitrary element of T. Then $x \in A_i$ for each $i \in \mathbb{N}$, and this certainly implies that $x \in A_1$. So $T \in A_1$. Conversely, assume $x \in A_1$. Since $A_i \subseteq A_{i+1}$ for all $i \in \mathbb{N}$, we have that $A_1 \subseteq A_i$ for every $i \in \mathbb{N}$, and hence $x \in T$. This shows that $A_1 \subseteq T$; hence we conclude that $T = A_1$.

□

Example 4.6. Let $n \in \mathbb{N}$ and let

$$A_n = \{m \in \mathbb{Z} \mid -n \leq m \wedge 2^m \leq n\}.$$

Use Theorem 4.26 to find $\bigcap_{i=1}^{\infty} A_i$ and $\bigcup_{i=1}^{\infty} A_i$.

Solution. We find that

$$\begin{aligned} A_1 &= \{-1, 0\}, & A_2 &= \{-2, -1, 0, 1\}, \\ A_3 &= \{-3, -2, -1, 0, 1\}, & A_4 &= \{-3, -2, -1, 0, 1, 2\} \end{aligned}$$

and so on. Note that $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$. Hence by Theorem 4.26, we have

$$\bigcap_{n=1}^{\infty} A_n = A_1$$

The reader should verify that $\bigcup_{n=1}^{\infty} A_n = \mathbb{Z}$.

Example 4.7. Let $I = (0, 1)$, and for $i \in I$, define $A_i = (-i, i)$. Find $\bigcap_{i \in I} A_i$ and $\bigcup_{i \in I} A_i$.

Solution. For example,

$$A_{1/2} = \left(-\frac{1}{2}, \frac{1}{2}\right) \qquad \text{and} \qquad A_{\sqrt{2}/3} = \left(-\frac{\sqrt{2}}{3}, \frac{\sqrt{2}}{3}\right).$$

Notice that if $0 < i < j < 1$, then $\{0\} \subset A_i \subset A_j \subset (-1, 1)$. It follows that

$$\bigcup_{i \in I} A_i = (-1, 1) \qquad \text{and} \qquad \bigcap_{i \in I} A_i = \{0\}$$

by Theorem 4.26.

Theorem 4.27 (Extended DeMorgan Laws). *Let $\{A_i \mid i \in I\}$ be a collection of sets indexed by I. Then*

1. $\left(\bigcup_{i \in I} A_i\right)' = \bigcap_{i \in I} A_i'$
2. $\left(\bigcap_{i \in I} A_i\right)' = \bigcup_{i \in I} A_i'$

Proof. We prove(1) and leave (2) for the reader as Exercise 4.18. Let x be an arbitrary element in $(\cup_{i\in I} A_i)'$. Then

$$\begin{aligned}
&x \in (\cup_{i\in I} A_i)' \\
&\quad \to [x \notin \cup_{i\in I} A_i] && \text{by Definition of complement} \\
&\quad \to [\neg(x \in \cup_{i\in I} A_i)] && \text{by Definition of } \notin \\
&\quad \to [\neg(\exists i \in I, x \in A_i)] && \text{by Definition of } \cup \\
&\quad \to [\forall i \in I, x \notin A_i] && \text{by logic rule} \\
&\quad \to [\forall i \in I, x \in A_i'] && \text{by Definition of complement} \\
&\quad \to [x \in \cap_{i\in I} A_i'] && \text{by Definition of } \cap
\end{aligned}$$

Thus $x \in \cap_{i\in I} A_i'$ and consequently

$$(\cup_{i\in I} A_i)' \subseteq x \in \cap_{i\in I} A_i'.$$

In a similar fashion (simply reverse the implications) one may prove the reverse containment. Therefore, we conclude

$$(\cup_{i\in I} A_i)' = \cap_{i\in I} A_i'.$$

as desired.

□

Let I be a nonempty set, and suppose that for each element $i \in I$ there is associated a set A_i. We then call I an index set for the collection of sets $\mathcal{A} = \{A_i \mid i \in I\}$.

Definition 4.14. Let I be an indexed set and suppose that $\mathcal{A} = \{A_i \mid i \in I\}$ is a collection of sets. Then

1. the union of the collection $\mathcal{A}$ is defined to be the set

$$\bigcup_{i\in I} A_i = \{x \mid x \in A_i \text{ for some } i \in I\},$$

2. the intersection of the collection $\mathcal{A}$ is defined to be the set

$$\bigcap_{i\in I} A_i = \{x \mid x \in A_i \text{ for each } i \in I\}.$$

Theorem 4.28 (Ascending and Descending Chains of Sets)**.** *Given the collection of sets $\{A_i \mid i \in \mathbb{N}\}$ the following properties hold.*

1. *If $A_i \subseteq A_{i+1}$ for all $i \in \mathbb{N}$, then $\bigcap_{i=1} A_i = A_1$.*

2. If $A_i \supseteq A_{i+1}$ for all $i \in \mathbb{N}$, then $\bigcup_{i=1} A_i = A_1$.

Proof. We prove (1) and leave (2) for the reader as Exercise 4.19.

Let $T = \cap_{i=1} A_i = A_0$ and let x be an arbitrary element of T. Then $x \in A_i$ for each $i \in \mathbb{N}$, and this certainly implies that $x \in A_1$. Sp $T \in A_1$.

Conversely, assume $x \in A_1$. Since $A_i \subseteq A_{i+1}$ for all $i \in \mathbb{N}$, we have that $A_1 \subseteq A_i$ for every $i \in \mathbb{N}$, and hence $x \in T$. This shows that $A_1 \subseteq T$; hence we conclude that $T = A_1$.

□

4.8 Exercises

Exercise 4.1. Prove Theorem 4.11.

Exercise 4.2. Prove Theorem 4.12.

Exercise 4.3. Prove Theorem 4.13.

Exercise 4.4. Prove Theorem 4.18.

Exercise 4.5. Finish the proof of Theorem 4.14.

Exercise 4.6. Finish the proof of Theorem 4.15.

Exercise 4.7. Finish the proof of Theorem 4.16.

Exercise 4.8. Finish the proof of Theorem 4.17.

Exercise 4.9. Finish the proof of Theorem 4.19.

Exercise 4.10. Finish the proof of Theorem 4.20.

Exercise 4.11. Prove Theorem 4.21.

Exercise 4.12. Prove Theorem 4.22.

Exercise 4.13. Prove Theorem 4.23.

Exercise 4.14. Finish the proof of Theorem 4.24.

Exercise 4.15. Finish the proof of Theorem 4.25.

Exercise 4.16. Prove Lemma 4.1.

Exercise 4.17. Finish the proof of Theorem 4.26.

Exercise 4.18. Finish the proof of Theorem 4.27.

Exercise 4.19. Finish the proof of Theorem 4.28.

Exercise 4.20. Prove Theorem 4.4.

Exercise 4.21. Prove Theorem 4.5.

Chapter 5

Functions and Relations

The set theory of functions is a powerful tool for solving mathematical problems, as it allows us to represent relationships between variables in a concise and exact way. It also provides a way to reason about these relationships and to prove results about them. Further, the set theory of functions is a fundamental tool in many branches of mathematics, including algebra, analysis, and topology. It is also used in physics and engineering, and in the study of computer algorithms.

First we need to understand the basic concepts related to functions. In particular, we need to know what a function is, and what its domain, codmain, and range are. So in other words, a function is a set of ordered pairs (x, y) such that each x corresponds to a unique y. The set of all x-values is called the domain, and the set of all y-values is called the codomain. However, not every element in the codomain will be paired with an element in the domain.

It is important to note that a function does not have to be a mathematical formula. Any relationship between two sets can be considered a function. For example, we could define a function between the set of all countries and the set of all languages as follows:

$$f(x) = \{y \mid y \text{ is a language spoken in country } x\}.$$

In this function, every country corresponds to a set of languages spoken in that country. This shows that functions can be very general relationships between two sets.

In fact, the notion of a set function is simply a generalization of the concept of a family of sets. Given any set X, we can create a family of sets by taking any collection of subsets of X, where each subset is considered to be a member set. Conversely, given any family F of sets, we can define a set function $f : F \to X$ by letting $f(S)$ be the union of all the members of S. This shows that the concepts of a family of sets and a set function are intimately related.

5.1 Domain and Codomain

Let X and Y be sets, we say f is a **function** from X to Y if f is a subset of $X \times Y$ such that the domain of f is X and f has the property: if $(x, y) \in f$ and $(x, z) \in f$ then $x = z$. For each $x \in X$, the unique $y \in Y$ such that $(x, y) \in f$ is denoted by $f(x)$. The element y is called the **value** of f at the **argument** x.

If we do not specify a function with the notation $f : X \to Y$ we will use $D(f)$ and $R(f)$ to denote the domain and range of f, respectively.

5.2 Image and Preimage

Definition 5.1. Let X and Y be sets. The **image** of $A \subseteq X$ is the set

$$f(A) = \{y \in Y : \exists x \in A, y = f(x)\}.$$

Theorem 5.1. *Let $f : X \to Y$ be a function. If $A_1, A_2 \subseteq X$, then*

$$f(A_1) \cup f(A_2) = f(A_1 \cup A_2).$$

Proof. $f(A_1) \cup f(A_2) = f(A_1 \cup A_2)$:

$$\begin{aligned} y \in f(A_1) \cup f(A_2) &\Leftrightarrow y \in f(A_1) \vee y \in f(A_2) \\ &\Leftrightarrow \exists x_1 \in A_1, y = f(x_1) \vee \exists x_2 \in A_2, y = f(x_2) \\ &\Leftrightarrow \exists x \in X, (x \in A_1 \vee x \in A_2) \wedge y = f(x) \\ &\Leftrightarrow \exists x \in A_1 \cup A_2, y = f(x) \Leftrightarrow y \in f(A_1 \cup A_2) \end{aligned}$$

□

Theorem 5.2. *Let $f : X \to Y$ be a function. If $A_1, A_2 \subseteq X$, then*

$$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2).$$

Proof. $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$

$$\begin{aligned} y \in f(A_1 \cap A_2) &\implies \exists x \in A_1 \cap A_2, y = f(x) \\ &\implies \exists x \in A_1, y = f(x) \wedge \exists x \in A_2, y = f(x) \\ &\implies y \in f(A_1) \wedge y \in f(A_2) \implies y \in f(A_1) \cap f(A_2) \end{aligned}$$

□

Theorem 5.3. *Let $f : X \to Y$ be a function. If $A_1, A_2 \subseteq X$, then*

$$f(A_2) \quad f(A_1) \subseteq f(A_2 \quad A_1).$$

Proof. $f(A_2) \quad f(A_1) \subseteq f(A_2 \quad A_1)$

$$\begin{aligned} y \in f(A_2) \quad f(A_1) &\Leftrightarrow y \in f(A_2) \wedge y \notin f(A_1) \\ &\Leftrightarrow (\exists x \in A_2, y = f(x)) \wedge \neg(y \in f(A)) \\ &\Leftrightarrow (\exists x \in A_2, y = f(x)) \wedge \neg(\exists z \in A_1, y = f(z)) \\ &\Leftrightarrow (\exists x \in A_2, y = f(x)) \wedge (\forall z \in A_1, y \neq f(z)) \\ &\implies \exists x \in A_2 \quad A_1, y = f(x) \Leftrightarrow y \in f(A_2 \quad A_1) \end{aligned}$$

□

Definition 5.2. Let X and Y be sets. The **preimage** of $B \subseteq Y$ is the set

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

Theorem 5.4. *Let $f : X \to Y$ be a function. If $B_1, B_2 \subseteq Y$, then*

$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2).$$

Proof. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$

$$\begin{aligned} x \in f^{-1}(B_1 \cup B_2) &\Leftrightarrow f(x) \in B_1 \cup B_2 \\ &\Leftrightarrow f(x) \in B_1 \vee f(x) \in B_2 \\ &\Leftrightarrow x \in f^{-1}(B_1) \vee x \in f^{-1}(B_2) \\ &\Leftrightarrow x \in f^{-1}(B_1) \cup f^{-1}(B_2) \end{aligned}$$

□

Theorem 5.5. *Let $f : X \to Y$ be a function. If $B_1, B_2 \subseteq Y$, then*

$$f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2).$$

Proof. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$

$$\begin{aligned} x \in f^{-1}(B_1 \cup B_2) &\Leftrightarrow f(x) \in B_1 \cup B_2 \\ &\Leftrightarrow f(x) \in B_1 \wedge f(x) \in B_2 \\ &\Leftrightarrow f(x) \in B_1 \wedge f(x) \in B_2 \\ &\Leftrightarrow x \in f^{-1}(B_1) \wedge x \in f^{-1}(B_2) \\ &\Leftrightarrow x \in f^{-1}(B_1) \cap f^{-1}(B_2) \end{aligned}$$

□

Theorem 5.6. *Let $f : X \to Y$ be a function. If $B_1, B_2 \subseteq Y$, then*

$$f^{-1}(B_2 \quad B_1) = f^{-1}(B_2) \quad f^{-1}(B_1).$$

Proof. $f^{-1}(B_2 \quad B_1) = f^{-1}(B_2) \quad f^{-1}(B_1)$

$$\begin{aligned} x \in f^{-1}(B_2 \quad B_1) &\Leftrightarrow f(x) \in B_2 \quad B_1 \\ &\Leftrightarrow f(x) \in B_2 \wedge \neg(f(x) \in B_1) \Leftrightarrow x \in f^{-1}(B_2) \wedge \neg(x \in f^{-1}(B_1)) \\ &\Leftrightarrow x \in f^{-1}(B_2) \wedge x \notin f^{-1}(B_1) \Leftrightarrow x \in f^{-1}(B_2) \quad f^{-1}(B_1) \end{aligned}$$

□

Theorem 5.7. *Let $f : X \to Y$ be a function. Then*

$$A_1 \subseteq A_2 \subseteq X \implies f(A_1) \subseteq f(A_2).$$

Proof. $A_1 \subseteq A_2 \implies f(A_1) \subseteq f(A_2)$

$$\begin{aligned} y \in f(A_1) &\Leftrightarrow \exists x \in A_1, y = f(x) \\ &\implies \exists x \in A_2, y = f(x) \implies y \in f(A_2) \end{aligned}$$

□

Theorem 5.8. *Let $f : X \to Y$ be a function. Then*

$$A_1 \subseteq A_2 \subseteq X \implies f(A_1) \subseteq f(A_2).$$

Proof. $B_1 \subseteq B_2 \implies f^{-1}(B_1) \subseteq f^{-1}(B_2)$

$$x \in f^{-1}(B_1) \Leftrightarrow f(x) \in B_1 \Longrightarrow f(x) \in B_2 \Leftrightarrow x \in f^{-1}(B_2)$$

□

Theorem 5.9. *Let $f : X \to Y$ be a function. Then*

$$B \subseteq Y \implies f(f^{-1}(B)) \subseteq B$$

Proof. $B \subseteq Y \implies f(f^{-1}(B)) \subseteq B$

$$\begin{aligned} y \in f(f^{-1}(B)) &\Leftrightarrow \exists x \in f^{-1}(B), y = f(x) \\ &\Longrightarrow \exists x \in X, f(x) \in B \wedge y = f(x) \Longrightarrow y \in B \end{aligned}$$

□

Theorem 5.10. *Let $f : X \to Y$ be a function. Then*

$$A \subseteq X \implies A \subseteq f^{-1}(f(A)).$$

Proof. $A \subseteq X \implies A \subseteq f^{-1}(f(A))$

$$x \in A \implies \exists y \in Y, y = f(x) \Leftrightarrow y \in f(A) \implies x \in f^{-1}(f(A))$$

□

5.3 Injective and Surjective

A one-to-one function is a function in which each element in the domain corresponds to a unique element in the codomain. In other words, no two elements in the domain have the same image. An onto function is a function in which each element in the codomain has at least one pre-image. In other words, for every element in the codomain, there is at least one element in the domain that maps to it. One-to-one and onto functions are important because they allow us to uniquely identify each element in the domain, and to know that every element in the codomain has a pre-image.

Definition 5.3. Let X and Y be sets. A function $f : X \to Y$ is called **injective** if

$$\forall x_1, x_2 \in X, f(x_1) = f(x_2) \implies x_1 = x_2.$$

Theorem 5.11. *Let $f : X \to Y$ be a function. If f is injective and $A \subseteq X$, then $f|_A$ is injective.*

Proof. Let $x_1, x_2 \in A$. Then

$$f|_A(x_1) = f|_A(x_2) \Longrightarrow f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$$

shows that $f|_A$ is injective.

□

Theorem 5.12. *Let $f : X \to Y$ be a function. Then f is injective if and only if $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ for all $A_1, A_2 \subseteq X$.*

Proof. Assume f is injective. It suffices to show $f(A_1) \cap f(A_2) \subseteq f(A_1 \cap A_2)$ for all $A_1, A_2 \subseteq X$. Let $A_1, A_2 \subseteq X$. Then

$$\begin{aligned} y \in f(A_1) \cap f(A_2) &\Leftrightarrow y \in f(A_1) \wedge y \in f(A_2) \\ &\Leftrightarrow [\exists x \in A_1, y = f(x)] \wedge [\exists z \in A_2, y = f(z)] \\ &\Longrightarrow \exists x \in A_1, \exists z \in A_2, f(x) = y = f(z) \\ &\Longrightarrow \exists x \in A_1, \exists z \in A_2, x = z, y = f(x) \\ &\Longrightarrow \exists x \in A_1 \cap A_2, y = f(x) \Longrightarrow y \in f(A_1 \cap A_2) \end{aligned}$$

Conversely, assume $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$, for all $A_1, A_2 \subseteq X$. Let $x_1, x_2 \in X$ and assume $x_1 \neq x_2$. Then $\{x_1\} \cap \{x_2\} = \emptyset$. Then

$$f(\{x_1\} \cap \{x_2\}) = \emptyset = f(\{x_1\}) \cap f(\{x_2\}).$$

If $f(x_1) = f(x_2)$, then $f(x_2) \in f(\{x_1\})$ and $f(x_1) \in f(\{x_2\})$, and so $f(\{x_1\}) \cap f(\{x_2\}) \neq \emptyset$. Thus, $f(x_1) \neq f(x_2)$ and so f is injective.

□

Theorem 5.13. *Let $f : X \to Y$ be a function. Then f is injective if and only if $f(A_2 \quad A_1) = f(A_2) \quad f(A_1)$ for all $A_1, A_2 \subseteq X$.*

Proof. Assume f is injective. Let $A_1, A_2 \subseteq X$. It suffices to show $f(A_2\ \ A_1) \subseteq f(A_2)\ \ f(A_1)$. Assume $y \in f(A_2\ \ A_1)$. Then $y = f(x)$ for some $x \in A_2\ \ A_1$. Thus, $x \in A_2$ and so $y \in f(A_2)$. We claim $y \notin f(A_1)$. Suppose $y \in f(A_1)$. Then, there exists $z \in A_1$ such that $f(z) = y$. Since f is injective, $x = z$. However, $x \notin A_1$, and so the claim follows. Thus, $y \in f(A_2)\ \ f(A_1)$ as desired.

Conversely, assume $f(A_2\ \ A_1) = f(A_2)\ \ f(A_1)$ holds for all $A_1, A_2 \in X$. Let $x_1, x_2 \in X$ and assume $x_1 \neq x_2$. Then $\{x_2\}\ \ \{x_1\} = \{x_2\}$ and so

$$f(\{x_2\}\ \ \{x_1\}) = f(\{x_2\}) = f(\{x_2\})\ \ f(\{x_1\}).$$

If $f(x_1) = f(x_2)$, then $f(\{x_2\})\ \ f(\{x_1\}) = \emptyset$, contrary to $f(\{x_2\})\ \ f(\{x_1\}) = f(\{x_2\})$. Thus $f(x_1) \neq f(x_2)$ and so f is injective.

□

Theorem 5.14. *Let $f : X \to Y$ be a function. Then f is injective if and only if $f(A_1) \cap f(A_2) = \emptyset$ for all $A_1, A_2 \subseteq X$ such that $A_1 \cap A_2 = \emptyset$.*

Proof. Assume f is injective. Let $A_1, A_2 \in X$ with $A_1 \cap A_2 = \emptyset$. Assume $y \in f(A_1) \cap f(A_2)$. Then there exists $x_1 \in A_1$ and $x_2 \in A_2$ such that $y = f(x_1)$ and $y = f(x_2)$. Since f is injective, $x_1 = x_2$. Thus, $A_1 \cap A_2 \neq \emptyset$ contrary to hypothesis. Thus, $f(A_1) \cap f(A_2)$ is empty. Conversely, assume $f(A_1) \cap f(A_2) = \emptyset$ for all $A_1, A_2 \subseteq X$ with $A_1 \cap A_2 = \emptyset$. Let $x_1, x_2 \in X$ and assume $x_1 \neq x_2$. Then $\{x_1\} \cap \{x_2\} = \emptyset$. By hypothesis, $f(\{x_1\}) \cap f(\{x_2\}) = \emptyset$. Thus $f(x_1) \neq f(x_2)$ and so f is injective.

□

Theorem 5.15. *Let $f : X \to Y$ be a function. Then f is injective if and only if $A = f^{-1}(f(A))$ for all $A \subseteq X$.*

Proof. Assume f is injective. Let $A \subseteq X$. It suffices to show $f^{-1}(f(A))$. Let $x \in f^{-1}(f(A))$. Then $f(x) \in f(A)$. Then there exists $x_1 \in A$ such that $f(x_1) = f(x)$. Since f is injective, $x_1 = x$ and so $x \in A$. Conversely, assume $A = f^{-1}(f(A))$ for all $A \subseteq X$. Let $x_1, x_2 \in X$. Assume $f(x)1 = f(x_2)$. Then

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

implies $x_1 = x_2$ and so f is injective.

□

Definition 5.4. Let X and Y be sets. A function $f : X \to Y$ is called **surjective** if

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

Theorem 5.16. *Let $f : X \to Y$ be a function. If f is surjective and $A \supseteq X$, then $f|^A$ is surjective.*

Proof. Let $t \in Y$. Since f is surjective there exists $x \in X$ such that $f(x) = y$. Since $X \subseteq A$, $x \in A$ and so $f(x) = y$ with $x \in A$ implies $f|^A$ is surjective.

□

Theorem 5.17. *Let $f : X \to Y$ be a function. Then f is surjective if and only if $B = f(f^{-1}(B))$ for all $B \subseteq Y$.*

Proof. Assume f is surjective. It suffices to show $B \subseteq f(f^{-1}(B))$. Let $y \in B$. Since f is surjective. there exists $x \in X$ such that $y = f(x)$. Since $f(x) \in B$ we have $x \in f^{-1}(B)$. It follows $y = f(x) \in f(f^{-1}(B))$.

Conversely, assume $B = f(f^{-1}(B))$ for all $B \subseteq Y$. Since $\{y\} = f(f^{-1}(\{y\}))$, it follows $y = f(x)$ for some $x \in f^{-1}(\{y\})$. Let $y \in Y$. Thus, f is surjective.

□

Theorem 5.18. *If $f : X \to P(X)$ is a function, then f is not surjective.*

Proof. Let $A = \{x \in X : x \notin f(x)\}$. Assume for a contradiction that f is onto. Then there exists $x \in X$ such that $f(x) = A$. Consider both cases $x \in f(x)$ and $x \notin f(x)$:

$$\begin{aligned} x \in f(x) &\implies x \in A \implies x \notin f(x) \implies\Leftarrow \\ x \notin f(x) &\implies x \in A = f(x) \implies x \notin f(x) \implies\Leftarrow \end{aligned}$$

Thus, x can not exist with $f(x) = A$. Therefore, no $f : X \to P(X)$ is onto.

□

5.4 Composition and Inverse

The composition of functions is a way to combine two or more functions into a single function. This can be done by combining the domain and range of the functions, or by using the functions to compute new outputs. The composition of functions is a powerful tool that can be used to simplify complex problems. It is also a useful way to create new functions from existing functions. To compose two functions f and g, we apply f to the output of g. That is, we first apply g to its input, and then apply f to the resulting output. The composition of functions is denoted by $f \circ g$.

The inverse of a function is a function that "undoes" the original function. In other words, it is a function that maps each element in the codomain back to its corresponding element in the domain. It's important to note that not all functions have inverse functions. For example, the function that takes in an age and outputs whether or not the person is tall has no inverse. This is because there are many people who are the same age but have different heights. So, there is no way to take in a height and produce an age. However, functions like this are still useful; they just can't be "undone".

Theorem 5.19. *Let $f : X \to Y$ be a function. If $g : Y \to Z$ and $g \circ f$ is injective, then f is injective.*

Proof. Let $x_1, x_2 \in X$. Then

$$f(x_1) = f(x_2) \implies (g \circ f)(x_1) = (g \circ f)(x_2) \implies x_1 = x_2$$

shows that f is injective.

□

Theorem 5.20. *Let $f : X \to Y$ be a function. Then following are equivalent.*

1. *given any functions $g, h : Y \to X$, if $f \circ g = f \circ h$, then $g = h$*
2. *there exists a function $g : Y \to X$ with $g \circ f = I_X$ (f has a left inverse)*

Proof. (1)⇔(2): Assume f is injective. Let $g, h : Y \to X$ and assume $f \circ g = f \circ h$. Let $y \in Y$. Then $(f \circ g)(y) = (f \circ h)(y)$. Since f is injective it follows $g(y) = h(y)$ for all $y \in Y$. Conversely, assume $g, h : Y \to X$, $f \circ g = f \circ h \implies g = h$ holds. Let $x_1, x_2 \in X$ and assume $x_1 \neq x_2$. Assume, for a contradiction, $f(x_1) = f(x_2)$. Let $g : Y \to X$ be defined by

$g(y) = x_1$ for all $y \in Y$. Let $h : Y \to X$ be defined by $h(y) = x_2$ for all $y \in Y$. Notice

$$(f \circ g)(y) = f(g(y)) = f(x_1) = f(x_2) = (f \circ h)(y)$$

for all $y \in Y$. Thus, $f \circ g = f \circ h$, yet $g \neq h$ since $g(y) = x_1 \neq x_2 = h(y)$. Therefore, $f(x_1) \neq f(x_2)$ and so f is injective.

(2)⇔(1): Assume $X \neq \emptyset$ and also assume $f : X \to Y$ is injective. Let $y \in Y$. Either $y \in f(X)$ or $y \notin f(X)$. Define $g : Y \to X$ as follows

$$g(y) = \begin{cases} x & y \in f(X) \text{ and } f(x) = y \\ x_0 & y \notin f(X) \end{cases} \tag{5.1}$$

where x_0 is a fixed element of $X \neq \emptyset$. Then g is defined for all $y \in Y$. If $y' \in Y$ with $x_1 = g(y') \neq g(y') = x_2$, then $y' = f(x_1) \neq f(x_2) = y'$, since f is injective. Thus, f is injective implies g is a function. If $x \in X$, then

$$(g \circ f)(x) = g(f(x)) = g(y) = x, \qquad \text{for some } y \in f(X)$$

which shows $g \circ f = I_X$. Conversely, assume $f : X \to Y$ and there exists $g : Y \to X$ such that $g \circ f = I_X$. Let $x_1, x_2 \in X$ and assume $f(x_1) = f(x_2)$. Then

$$x_1 = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = x_2$$

which shows f is injective.

□

Theorem 5.21. *Let $f : X \to Y$ be a function. If f is injective and $g : Y \to Z$ is injective, then $g \circ f$ is injective.*

Proof. Let $x_1, x_2 \in X$. Then

$$(g \circ f)(x_1) = (g \circ f)(x_2) \Longrightarrow f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$$

shows that $g \circ f$ is injective.

□

Theorem 5.22. *Let $f : X \to Y$ be a function. If $g : Y \to Z$ and $g \circ f$ is surjective, then g is surjective.*

Proof. Let $z \in Z$. Then there exists $x \in X$ such that $(g \circ f)(x) = z$. Thus it follows $g(f(x)) = z$ shows, for all $z \in Z$ there exists y (namely $y = f(x)$) such that $g(y) = z$ and so g is surjective.

□

Theorem 5.23. *Let $f : X \to Y$ be a function. If f is surjective and $g : Y \to Z$ is surjective, then $g \circ f$ is surjective.*

Proof. Let $z \in Z$. Since g is surjective there exists $y \in Y$ such that $g(y) = z$. Since f is surjective there exists $x \in X$ such that $f(x) = y$. Thus $(g \circ f)(x) = z$ and so $g \circ f$ is surjective.

□

Theorem 5.24. *Let $f : X \to Y$ be a function. Then f is surjective if and only if given any functions $g, h : Y \to X$, if $g \circ f = h \circ f$, then $g = h$*

Proof. Assume f is surjective and let $g : Y \to Z$ and $h : Y \to Z$ be functions such that $g \circ f = h \circ f$. Let $y \in Y$. Since f is surjective, there exists $x \in X$ such that $y = f(x)$. Then $g(y) = g(f(X)) = h(f(x)) = h(y)$ as needed to show $g = h$.

Conversely, and for contrapositive, suppose f is not surjective. Then there exists $y_1 \in Y$ such that $y_1 = f(x)$ does not hold for all $x \in X$. Let $Z = \{a, b\}$ and let g and h be defined by $g(y) = a$ for all $a \in Y$ and

$$h(y) = \begin{cases} a & \text{if } y \neq y_1 \\ b & \text{if } y = y_1. \end{cases}$$

Then we have $g \neq h$ such that $g \circ f = h \circ f$. Thus f is not right cancelable.

□

Theorem 5.25. *Let $f : X \to Y$ be a function. Then f is surjective if and only if there exists a function $h : Y \to X$ with $f \circ h = I_Y$ (f has a right inverse).*

Proof. Then f is surjective if and only if there exists a function $h : Y \to X$ with $f \circ h = I_Y$. Assume there exist $h : Y \to X$ with $f \circ h = I_Y$. Let $b \in Y$. Then $b = (f \circ h)(b) = f(h(b)) = f(a)$ where $a \in X$, shows f is surjective.

Conversely, follows using the **Axiom of Choice**. Suppose f is surjective. Then $f^{-1}(b) \subseteq X$ is a nonempty set for every $b \in Y$. For each $b \in Y$ choose $a_b \in f^{-1}(b)$. Then the map $h : Y \to X$ defined by $h(b) = a_b$ is such that $f \circ h = I_Y$ since $(f \circ h)(y) = f(h(y)) = f(a_y) = y$.

□

If the inverse relation f^{-1} is also a function, then we say f is an **invertible function**, or just **invertible function**.

Theorem 5.26. *A function $f : X \to Y$ is invertible if and only if it is injective. If f is invertible then f^{-1} is also invertible and $(f^{-1})^{-1} = f$.*

Proof. Let f be invertible, then f^{-1} is a function. It follows that $f^{-1}(f(x)) = x$ for all $x \in X$. If $x_1, x_2 \in X$ and $f(x_1) = f(x_2)$, we get $f^{-1}(f(x_1)) = f^{-1}(f(x_2))$ and $x_1 = x_2$. So f is injective. Let f be injective. If $a = f^{-1}(y_1)$ and $a = f^{-1}(y_2)$ we have $y_1 = f(a)$ and $y_2 = f(a)$. Therefore, $y_1 = y_2$ and we have proven that f^{-1} is a function. We know that $(f^{-1})^{-1} = f$ by previous theorem and so f^{-1} is also invertible.

□

Definition 5.5. Let X and Y be sets. A function f is called **bijective**, if f is both injective and surjective.

Theorem 5.27. *Let $f : X \to Y$ be a function. Then f is bijective if and only if there exists a unique function $f' : Y \to X$ such that both $f' \circ f = I_X$ and $f \circ f' = I_Y$.*

Proof. If f is bijective, then f is injective and surjective; and thus there exists functions g and h such that $g \circ f = I_X$ and $f \circ h = I_Y$. Notice

$$g = g \circ I_Y = g \circ (f \circ h) = (g \circ f) \circ h = I_X \circ h = h$$

showing $f' := g = h$ as needed. Conversely, follows from the statements above.

□

Theorem 5.28. *Let $f : X \to Y$ be a function. If f and $g : Y \to Z$ are bijections, then $g \circ f$ is a bijection and*

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

Proof. If f and f are bijections, then $g \circ f$ is a bijection and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Therefore, the inverse of a function $f : X \to Y$ is a function $f^{-1} : Y \to X$ if and only if f is a bijection. Since f and g are bijections, $f^{-1} : Y \to X$ and $g^{-1} : Z \to Y$ are functions. Hence, $f^{-1} \circ g^{-1} : Z \to X$ is a function. It follows that, $g \circ f$ is injective and surjective, and so a bijection. Thus $(g \circ f)^{-1} : Z \to X$ is also a function. Let $z \in Z$. Since f and g are surjections there exists $x \in X$ and $y \in Y$ such that

$$g(y) = z \qquad \text{and} \qquad f(x) = y, \tag{5.2}$$

respectively. Written in inverse function notation, $y = g^{-1}(z)$ and $x = f^{-1}(y)$. By substitution, $x = f^{-1}(g^{-1}(z)) = (f^{-1} \circ g^{-1})(z)$. Notice it also follows from (5.2) that $(g \circ f)(x) = g(f(x)) = g(y) = z$. Written in inverse function notation we obtain $(g \circ f)^{-1}(z) = x$.

□

5.5 Relations

Binary relations are defined as a set of ordered pairs, where each element in the pair is from a set. In other words, binary relations involve set(s) of elements, which we will call the *left* set and the *right* set. The relationship between the two elements in each ordered pair is what we call the **relation**.

Binary relations allow us to study the relationships between sets.

For example, let's say we have a set of all the countries in the world, which we will call C, and a set of all the capitals of those countries, which we will call P. We can then define a binary relation R between C and P as follows:

$$R = \{(c, p) \mid c \in C \text{ and } p \in P \text{ and } c \text{ is the capital of } p\}.$$

In other words, R is the set of all ordered pairs (c, p) such that c is a country and p is its capital.

Binary relations can be classified according to various properties. The most common properties are composition, inverse, image, and preimage.

Image. Given a relation R and a set A, the image of A under R is the set

$$\{y \mid \exists x \in A \text{ such that } (x, y) \in R\}.$$

Preimage. Given a relation R and a set B, the preimage of B under R is the set

$$\{x \mid \exists y \in B \text{ such that } (x, y) \in R\}.$$

Composition. Given two relations R and S, their composition RS is the relation that consists of all ordered pairs (x, z) such that there exists a y such that $(x, y) \in R$ and $(y, z) \in S$.

Inverse. Given a relation R, the inverse of R is the relation that consists of all ordered pairs (y, x) such that $(x, y) \in R$.

Binary relations can be represented in various ways, such as tables, graphs, and sets of ordered pairs. In order to understand binary relations, it is important to be familiar with all the different representations.

Tables. A binary relation can be represented using a table with two columns, where the left column represents the left set and the right column represents the right set. The entries in the table are the ordered pairs that make up the relation.

Graphs. A binary relation can also be represented using a graph, where the left set is represented by the vertices and the right set is represented by the edges. The edges are labeled with the elements of the right set, and each edge goes from the vertex that represents the left element of the ordered pair to the vertex that represents the right element.

Sets of ordered pairs. Finally, a binary relation can also be represented as a set of ordered pairs. This is the most common way to represent a binary relation, and it is the representation we will use most often in this book.

Binary relations are a fundamental concept in mathematics, and they can be used to model many different situations. For example, in computer science, binary relations are used to represent many different types of relationships. They can be used to represent the relationship between two pieces of *data*, or the relationship between two *nodes in a graph*. They can also be used to represent the relationship between two *points in space*, or the relationship between two people in a *social network*. Binary relations are also used in physics to represent the interactions between particles. For example, the *gravitational force* between two masses is a binary relation.

Now it's time to become familiar with the basic terminology and notation.

Let X be a set and let $X \times X = \{(a, b) : a, b \in X\}$. A (binary) relation **relation** R is a subset of $X \times X$. If $(a, b) \in R$, then we say a is **related** to b by R. It is possible to have both $(a, b) \in R$ and $(a, b') \in R$ where $b' \neq b$; that is any element in X could be related to any number of other elements of X. It is also possible to have some element that is not related to any element in X at all. We say a relation S is an **extension** of a relation R, denoted by $R \subseteq S$, whenever aRb implies aSb, for all $a, b \in X$. Just as we would with sets, we say relations R and S are equal whenever $R \subseteq S$ and $S \subseteq R$.

Definition 5.6. Let R and S be relations on X.

1. The **image** of $A \subseteq X$ under R is the set
$$R(A) = \{y \in X : \exists\, x \in A, (x, y) \in R\}.$$
2. The **preimage** of $B \subseteq X$ under R is the set
$$R^{-1}(B) = \{x \in X : \exists\, y \in B, (x, y) \in R\}.$$
3. The **composition** of R and S is the relation
$$S \circ R = \{(a, c) \in X \times X : \exists\, b \in X, (a, b) \in R \wedge (b, c) \in S\}.$$
4. The **inverse** of R is the relation
$$R^{-1} = \{(b, a) \in X \times X : (a, b) \in R\}.$$

Union, Intersection, and Complement of Relations

We define the union, intersection, and complement of two relations just as one would expect knowing elementary set theory. So the union of two relations consists of those ordered pairs of elements that are related under at least one of the two relations, and the intersection of two relations consists of those ordered pairs of elements which are related under both relations.

Definition 5.7. Let R and S be relations on a set X.The **union** and **intersection** of R and S are the relations prescribed (respectively) by
$$R \cup S = \{(a, b) : aRb \text{ or } aSb\} \quad \text{and} \quad R \cap S = \{(a, b) : aRb \text{ and } aSb\}.$$
The of R is the relation prescribed by $R^c = \{(a, b) : \neg(aRb)\}$.

We now demonstrate one way of proving a proposition holds using elementary set theory. Suppose we wish to show that
$$R \subseteq S \Leftrightarrow R \cap S = R \tag{5.3}$$
for relations R and S defined on a set X. To do so, we will prove that $R \subseteq S$ implies $R \cap S = R$, and conversely that $R \cap S = R$ implies $R \subseteq S$.

1. First we show $R \subseteq S \Rightarrow R \cap S = R$: Assume that $R \subseteq S$. Let (a, b) be an arbitrary element of $X \times X$. If $a(R \cap S)b$, then we have aRb, and so $R \cap S \subseteq R$ follows. If aRb, then aSb by hypothesis, and so $a(R \cap S)b$ follows. Therefore, we have shown $R \cap S = R$ by assuming $R \subseteq S$.

2. Conversely, we show $R \cap S = R \Rightarrow R \subseteq S$: Let (a, b) be an arbitrary element of $X \times X$. If aRb, then $a(R \cap S)b$ by hypothesis, and so aSb. Therefore we have shown $R \subseteq S$ by assuming $R \cap S = R$.

This type of reasoning illustrates the process of using basic logic and unwrapping definitions.

Theorem 5.29. *If R, S, and T be relations on a set X, there holds*

1. $R \cup (S \cup T) = (R \cup S) \cup T$
2. $R \cup S = S \cup R$
3. $R \cup (R \cap S) = R$
4. $R \cup \emptyset = R$
5. $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$
6. $R \cup R^c = X \times X$
7. $R \cap (S \cap T) = (R \cap S) \cap T$
8. $R \cap S = S \cap R$
9. $R \cap (R \cup S) = R$
10. $R \cap \ (X \times X) = R$
11. $R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$
12. $R \cap R^c = \emptyset$

Proof. For the first statement, let (x, y) be an arbitrary element of $X \times X$, then

$$x(R \cup (S \cup T))y \Leftrightarrow xRy \vee x(S \cup T)y \Leftrightarrow xRy \vee \Big(xSy \vee xTy\Big)$$
$$\Leftrightarrow \Big(xRy \vee xSy\Big) \vee xTy \Leftrightarrow x(R \cup S)y \vee xTy \Leftrightarrow x\big((R \cup S) \cup T\big)y.$$

We leave the remainder of the proof for Exercise 5.1.

□

Relative Complement and Symmetric Difference

Other operations on $\mathcal{X} \times \mathcal{X}$ can be defined using logical connectives. For example, let $\oplus$ denote the logical XOR symbol (defined by $p \oplus q$ is true if and only if p and q have different truth values), then $R \bigtriangleup S = \{(a, b) : aRb \oplus aSb\}$ prescribes the symmetric difference of relations R and S defined on a set X.

Definition 5.8. Let R and S be relations on a set X. The **relative complement** and **symmetric difference** of R and S are the relations prescribed (respectively) by

$$R - S = R \cap S^c \qquad \text{and} \qquad R \bigtriangleup S = (R - S) \cup (S - R).$$

There are several equivalent formulations of the symmetric difference, some of which will be seen in the exercises.

Theorem 5.30. *For any relations R, S, and T on a set X, there holds 1. $R \triangle S = S \triangle R$ 2. $R \triangle (S \triangle T) = (R \triangle S) \triangle T$ 3. $R \triangle \emptyset = R$ 4. $R \triangle R = \emptyset$ 5. $R \cap (S \bigtriangleup T) = (R \cap S) \bigtriangleup (R \cap T)$ 6. $(S \bigtriangleup T) \cap R = (S \cap R) \bigtriangleup (T \cap R)$*

Proof. When we consider the triple $(\mathcal{X} \times \mathcal{X}, \triangle, \cap)$ as an algebraic structure, it is an example of a Boolean ring with identity [**?**]. More precisely, $(\mathcal{X}, \triangle)$ is an abelian group with identity $\emptyset$ and $(\mathcal{X} \times \mathcal{X}, \triangle, \cap)$ is a commutative ring with identity that is Boolean.

□

Theorem 5.31. *For any relations R, S, and T on a set X, there holds*

1. *$R \bigtriangleup S \subseteq R \cup S$,*
2. *$R \cap S = \emptyset$ if and only if $R \cup S = R \bigtriangleup S$, and*
3. *$(R \bigtriangleup S) \bigtriangleup (S \bigtriangleup T) = R \bigtriangleup T$.*

Proof. (1): Since $R - S \subseteq R$ and $S - R \subseteq S$, we have $R \bigtriangleup S \subseteq R \cup S$.

(2): If R and S are disjoint, then $R = R - S$ and $S = S - R$ and so $R \triangle S = R \cup S$. Conversely, assume that $R \bigtriangleup S = R \cup S$. If $R \cap S \neq \emptyset$, then both $R - S \subset R$ and $S - R \subset S$ (proper containment); whence $R \bigtriangleup S \neq R \cup S$ contrary to hypothesis.

(3):By Theorem 5.30 we have

$$(R \bigtriangleup S) \bigtriangleup (S \bigtriangleup T) = R \bigtriangleup S \bigtriangleup S \bigtriangleup T = R \bigtriangleup \emptyset \bigtriangleup T = R \bigtriangleup T \tag{5.4}$$

as needed.

□

Composition and Inverse Relations

In particular, relations are sets and, so are the image and preimage of a relation. Here are some basic properties of relations on a set regarding image, union, intersection, and compositon.

Theorem 5.32. *Let R, S and T be relations on X. Then the following hold.*

1. $R \circ (S \circ T) = (R \circ S) \circ T$
2. $R \circ (S \cup T) = (R \circ S) \cup (R \circ T)$
3. $(S \cup T) \circ R = (S \circ R) \cup (T \circ R)$
4. $R \circ (S \cap T) \subseteq (R \circ S) \cap (R \circ T)$
5. $R \subseteq S \implies R \circ T \subseteq S \circ T$
6. $R \subseteq S \implies T \circ R \subseteq T \circ S$

Proof. The proof of each part follows.

(1) $R \circ (S \circ T) = (R \circ S) \circ T$:

$$\begin{aligned}
(x,y) \in & R \circ (S \circ T) \\
&\iff \exists z \in X, (x,z) \in S \circ T \wedge (z,y) \in R \\
&\iff \exists z \in X, [\exists w \in X, (x,w) \in T \wedge (w,z) \in S] \wedge (z,y) \in R \\
&\iff \exists w, z \in X, (x,w) \in T \wedge (w,z) \in S \wedge (z,y) \in R \\
&\iff \exists w \in X, [\exists z \in X, (w,z) \in S \wedge (z,y) \in R] \wedge (x,w) \in T \\
&\iff \exists w \in X, (x,w) \in T \wedge (w,y) \in R \circ S \\
&\iff (x,y) \in (R \circ S) \circ T
\end{aligned}$$

(2) $R \circ (S \cup T) = (R \circ S) \cup (R \circ T)$:

$$\begin{aligned}
(x,y) \in & R \circ (S \cup T) \\
&\iff \exists z \in X, (x,z) \in S \cup T \wedge (z,y) \in R \\
&\iff \exists z \in X, [(x,z) \in S \vee (x,z) \in T] \wedge (z,y) \in R \\
&\iff \exists z \in X, [(x,z) \in S \wedge (z,y) \in R] \vee [(x,z) \in T \wedge (z,y) \in R] \\
&\iff (x,y) \in R \circ S \vee (x,y) \in R \circ T \\
&\iff (x,y) \in (R \circ S) \cup (R \circ T)
\end{aligned}$$

(3) $(S \cup T) \circ R = (S \circ R) \cup (T \circ R)$:

$$\begin{aligned}
&(x,y) \in (S \cup T) \circ R \\
&\qquad \iff \exists z \in X, (x,z) \in R \wedge (z,y) \in S \cup T \\
&\qquad \iff \exists z \in X, (x,z) \in R \wedge [(z,y) \in S \vee (z,y) \in T] \\
&\qquad \iff \exists z \in X, [(x,z) \in R \wedge (z,y) \in S] \vee [(x,z) \in R \wedge (z,y) \in T] \\
&\qquad \iff (x,y) \in (S \circ R) \vee (x,y) \in (T \circ R) \\
&\qquad \iff (x,y) \in (S \circ R) \cup (T \circ R)
\end{aligned}$$

(4) $)R \circ (S \cap T) \subseteq (R \circ S) \cap (R \circ T)$:

$$\begin{aligned}
&(x,y) \in R \circ (S \cap T) \\
&\qquad \iff \exists z \in X, (x,z) \in S \cap T \wedge (z,y) \in R \\
&\qquad \iff \exists z \in X, [(x,z) \in S \wedge (x,z) \in T] \wedge (z,y) \in R \\
&\qquad \iff \exists z \in X, [(x,z) \in S \wedge (z,y) \in R] \wedge (x,z) \in T \\
&\qquad \iff \exists z \in X, [(x,z) \in S \wedge (z,y) \in R] \wedge [(x,z) \in T \wedge (z,y) \in R] \\
&\qquad \Longrightarrow [\exists z \in X, [(x,z) \in S \wedge (z,y) \in R] \wedge [\exists w \in X, (x,w) \in T \wedge (w,y) \in R] \\
&\qquad \iff (x,y) \in R \circ S \wedge (x,y) \in R \circ T \\
&\qquad \iff (x,y) \in (R \circ S) \cap (R \circ T)
\end{aligned}$$

(5) $R \subseteq S \implies R \circ T \subseteq S \circ T$:

$$\begin{aligned}
(x,y) \in R \circ T &\iff \exists z \in X, (x,z) \in T \wedge (z,y) \in R \\
&\Longrightarrow \exists z \in X, (x,z) \in T \wedge (z,y) \in S \iff (x,y) \in S \circ T
\end{aligned}$$

(6) $R \subseteq S \implies T \circ R \subseteq T \circ S$:

$$\begin{aligned}
(x,y) \in T \circ R &\iff \exists z \in X, (x,z) \in R \wedge (z,y) \in T \\
&\Longrightarrow \exists z \in X, (x,z) \in S \wedge (z,y) \in T \iff (x,y) \in T \circ S
\end{aligned}$$

The proof is now complete.

□

Here are some basic properties of relations on a set regarding preimage, union, intersection, set difference, and compositon.

Theorem 5.33. *Let R and S be relations on X. Then the following hold.*

1. $(R^{-1})^{-1} = R$
2. $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$
3. $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$

4. $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$
5. $R \subseteq S \implies R^{-1} \subseteq S^{-1}$.
6. $(R^c)^{-1} = (R^{-1})^c$
7. $(R\ \ S)^{-1} = R^{-1}\ \ S^{-1}$

Proof. The proof of each part follows.

(1) $(R^{-1})^{-1} = R$:

$$(x,y) \in (R^{-1})^{-1} \iff (y,x) \in R^{-1} \iff (x,y) \in R$$

(2) $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$:

$$\begin{aligned}(x,y) \in (R \cup S)^{-1} &\iff (y,x) \in R \cup S \iff (y,x) \in R \vee (y,x) \in S \\ &\iff (x,y) \in R^{-1} \vee (x,y) \in S^{-1} \iff (x,y) \in R^{-1} \cup S^{-1}\end{aligned}$$

(3) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$:

$$\begin{aligned}(x,y) \in (R \cap S)^{-1} &\iff (y,x) \in R \cap S \iff (y,x) \in R \wedge (y,x) \in S \\ &\iff (x,y) \in R^{-1} \wedge (x,y) \in S^{-1} \iff (x,y) \in R^{-1} \cap S^{-1}\end{aligned}$$

(4) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$:

$$\begin{aligned}(x,y) \in (R \circ S)^{-1} &\iff (y,x) \in R \circ S \\ &\iff \exists z \in X, (y,z) \in S \wedge (z,x) \in R \\ &\iff \exists z \in X, (z,y) \in S^{-1} \wedge (x,z) \in R^{-1} \\ &\iff \exists z \in X, (x,z) \in R^{-1} \wedge (z,y) \in S^{-1} \\ &\iff (x,y) \in S^{-1} \circ R^{-1}\end{aligned}$$

(5) If $R \subseteq S$, then $R^{-1} \subseteq S^{-1}$:

$$(x,y) \in R^{-1} \iff (y,x) \in R \implies (y,x) \in S \iff (x,y) \in S^{-1}$$

(6) $(R^c)^{-1} = (R^{-1})^c$:

$$\begin{aligned}(x,y) \in (R^c)^{-1} &\iff (y,x) \in R^c \iff (y,x) \in X \times X \wedge (y,x) \notin R \\ &\iff (x,y) \in X \times X \wedge (x,y) \notin R^{-1} \iff (x,y) \in (R^{-1})^c\end{aligned}$$

(7) $(R\ \ S)^{-1} = R^{-1}\ \ S^{-1}$

$$\begin{aligned}(x,y) \in (R\ \ S)^{-1} &\iff (y,x) \in R\ \ S \iff (y,x) \in R \wedge (y,x) \notin S \\ &\iff (x,y) \in R^{-1} \wedge (y,x) \notin S \iff (x,y) \in R^{-1} \wedge (x,y) \notin S^{-1} \\ &\iff (x,y) \in R^{-1}\ \ S^{-1}\end{aligned}$$

□

In the next two theorems we have basic properties involving the image, union, intersection, and set difference. And exactly when two relations are equal.

Theorem 5.34. *Let R and S be a relations on X and $A, B \subseteq X$. Then the following hold.*

1. $A \subseteq B \implies R(A) \subseteq R(B)$
2. $R(A \cup B) = R(A) \cup R(B)$
3. $R(A \cap B) \subseteq R(A) \cap R(B)$
4. $R(A) \quad R(B) \subseteq R(A \quad B)$
5. *If $R(x) = S(x)$ for all $x \in X$, then $R = S$.*

Proof. The proof of each part follows.

(1) If $A \subseteq B$, then $R(A) \subseteq R(B)$:

$$y \in R(A) \iff \exists x \in A, (x, y) \in R \implies \exists x \in B, (x, y) \in R \iff y \in R(B)$$

(2) $R(A \cup B) = R(A) \cup R(B)$:

$$\begin{aligned} y \in R(A \cup B) &\iff \exists x \in X, x \in A \cup B \wedge (x, y) \in R \\ &\iff \exists x \in X, (x \in A \vee x \in B) \wedge (x, y) \in R \\ &\iff \exists x \in A, (x, y) \in R \vee \exists x \in B, (x, y) \in R \iff y \in R(A) \cup R(B) \end{aligned}$$

(3) $R(A \cap B) \subseteq R(A) \cap R(B)$:

$$\begin{aligned} y \in R(A \cap B) &\iff \exists x \in X, x \in A \cap B \wedge (x, y) \in R \\ &\iff \exists x \in X, (x \in A \wedge x \in B) \wedge (x, y) \in R \\ &\implies \exists x \in A, (x, y) \in R \wedge \exists x \in B, (x, y) \in R \iff y \in R(A) \cap R(B) \end{aligned}$$

(4) $R(A) \quad R(B) \subseteq R(A \quad B)$:

$$\begin{aligned} y \in R(A) \quad R(B) &\iff y \in R(A) \wedge y \notin R(B) \\ &\iff \exists x \in A, (x, y) \in R \wedge \forall z \in B, (z, y) \notin R \\ &\iff \exists x \in A \quad B, (x, y) \in R \iff y \in R(A \quad B) \end{aligned}$$

(5) Assume $R(x) = S(x)$ for all $x \in X$, then

$$(x, y) \in R \iff y \in R(x) \iff y \in S(x) \iff (x, y) \in S$$

which completes the proof.

□

Why is there not a part (5) to the next theorem? Can you state and prove a part (5)? If not, can you provide a counterexample?

Theorem 5.35. *Let R be a relation on X with $A, B \subseteq X$. Then the following hold.*

1. $A \subseteq B \implies R^{-1}(A) \subseteq R^{1-}(B)$
2. $R^{-1}(A \cup B) = R^{-1}(A) \cup R^{-1}(B)$
3. $R^{-1}(A \cap B) \subseteq R^{-1}(A) \cap R^{-1}(B)$
4. $R^{-1}(A) \quad R^{-1}(B) \subseteq R^{-1}(A \quad B)$

Proof. The proof of each part follows.

(1) $A \subseteq B \implies R^{-1}(A) \subseteq R^{-1}(B)$:

$$\begin{aligned} x \in R^{-1}(A) &\iff \exists y \in A, (x, y) \in R \\ &\implies \exists y \in B, (x, y) \in R \iff x \in R^{-1}(B) \end{aligned}$$

(2) $R^{-1}(A \cup B) = R^{-1}(A) \cup R^{-1}(B)$:

$$\begin{aligned} x \in R^{-1}(A \cup B) &\iff \exists y \in A \cup B, (x, y) \in R \\ &\iff \exists y \in A, (x, y) \in R \vee \exists y \in B, (x, y) \in R \\ &\iff x \in R^{-1}(A) \vee R^{-1}(B) \iff x \in R^{-1}(A) \cup R^{-1}(B) \end{aligned}$$

(3) $R^{-1}(A \cap B) \subseteq R^{-1}(A) \cap R^{-1}(B)$:

$$\begin{aligned} x \in R^{-1}(A \cap B) &\iff \exists y \in A \cap B, (x, y) \in R \\ &\iff \exists y \in X, y \in A \wedge y \in B \wedge (x, y) \in R \\ &\implies x \in R^{-1}(A) \wedge x \in R^{-1}(B) \iff x \in R^{-1}(A) \cap x \in R^{-1}(B) \end{aligned}$$

(4) $R^{-1}(A) \quad R^{-1}(B) \subseteq R^{-1}(A \quad B)$:

$$\begin{aligned} x \in R^{-1}(A) \quad R^{-1}(B) &\iff x \in R^{-1}(A) \wedge \neg(x \in R^{-1}(B)) \\ &\iff x \in R^{-1}(A) \wedge [\forall y \in B, (x, y) \notin R] \\ &\iff \exists y \in A, (x, y) \in R \wedge [\forall y \in B, (x, y) \notin R] \\ &\implies \exists y \in A \quad B, (x, y) \in R \iff x \in R^{-1}(A \quad B) \end{aligned}$$

□

Families of Relations

In the next theorem we have a family of relations and we see how they interact with composition.

Theorem 5.36. *Let R and R_i be relations on X for $i \in I$ where I is an indexed set. Then the following hold.*

1. $R \circ \left(\bigcup_{i\in I} R_i\right) = \bigcup_{i\in I}(R \circ R_i)$
2. $\left(\bigcup_{i\in I} R_i\right) \circ R = \bigcup_{i\in I}(R_i \circ R)$

Proof. The proof of each part follows.

(1) $R \circ \left(\bigcup_{i\in I} R_i\right) = \bigcup_{i\in I}(R \circ R_i)$

$$\begin{aligned}
(x,y) \in R \circ \left(\bigcup_{i\in I} R_i\right) &\iff \exists z \in X, (x,z) \in \bigcup_{i\in I} R_i \wedge (z,y) \in R \\
&\iff \exists z \in X, \exists i \in I, (x,z) \in R_i \wedge (z,y) \in R \\
&\iff \exists i \in I, (x,y) \in R \circ R_i \\
&\iff (x,y) \in \bigcup_{i\in I}(R \circ R_i)
\end{aligned}$$

(2) $\left(\bigcup_{i\in I} R_i\right) \circ R = \bigcup_{i\in I}(R_i \circ R)$:

$$\begin{aligned}
(x,y) \in \left(\bigcup_{i\in I} R_i\right) \circ R &\iff \exists z \in X, (x,z) \in R \wedge (z,y) \in \bigcup_{i\in I} R_i \\
&\iff \exists z \in X, \exists i \in I, (x,z) \in R \wedge (z,y) \in R_i \\
&\iff (x,y) \in \bigcup_{i\in I}(R_i \circ R)
\end{aligned}$$

□

The Powers of a Relation

In the next theorem we see how powers of a relation interacts with preimage and unions.

Theorem 5.37. *Let R be a relation on X. Then the following hold.*

1. $(R^n)^{-1} = (R^{-1})^n$ *for all* $n \geq 1$
2. $R^n \cup S^n \subseteq (R \cup S)^n$ *for all* $n \geq 1$
3. $\left(\bigcup_{n\geq 1} R^n\right)^{-1} = \bigcup_{n\geq 1}(R^{-1})^n$

Proof. The proof of each part follows.

(1) By induction. The basis step is obvious: $(R^1)^{-1} = (R^{-1})^1$. In fact,

$$(R^2)^{-1} = (R \circ R)^{-1} = R^{-1} \circ R^{-1} = (R^{-1})^2.$$

The induction step is

$$(R^n)^{-1} = (R^{-1})^n \implies (R^{n+1})^{-1} = (R^{-1})^{n+1}.$$

The result now follows from the argument:

$$\begin{aligned}(x,y) \in (R^{n+1})^{-1} &\iff (y,x) \in R^{n+1}\\ &\iff \exists z \in X, (y,z) \in R \wedge (z,x) \in R^n\\ &\iff \exists z \in X, (z,y) \in R^{-1} \wedge (x,z) \in (R^n)^{-1}\\ &\iff \exists z \in X, (x,z) \in (R^n)^{-1} \wedge (z,y) \in R^{-1}\\ &\iff \exists z \in X, (x,z) \in (R^{-1})^n \wedge (z,y) \in R^{-1}\\ &\iff (x,y) \in (R^{-1})^{n+1}\end{aligned}$$

(2) $\left(\bigcup_{n\geq 1} R^n\right)^{-1} = \bigcup_{n\geq 1}(R^{-1})^n$

$$\begin{aligned}(x,y) \in \left(\bigcup_{n\geq 1} R^n\right)^{-1} &\iff (y,x) \in \bigcup_{n\geq 1} R^n\\ \iff \exists n \geq 1, (y,x) &\in R^n = R^{n-1} \circ R\\ \iff \exists n \geq 1, \exists z &\in X, (y,z) \in R \wedge (z,x) \in R^{n-1}\\ \iff \exists n \geq 1, \exists z &\in X, (z,y) \in R^{-1} \wedge (x,z) \in (R^{n-1})^{-1}\\ \iff \exists n \geq 1, \exists z &\in X, (x,z) \in (R^{n-1})^{-1} \wedge (z,y) \in R^{-1}\\ \iff \exists n \geq 1, \exists z &\in X, (x,z) \in (R^{-1})^{n-1} \wedge (z,y) \in R^{-1}\\ \iff \exists n \geq 1, (x,y) &\in (R^{-1})^n \iff (x,y) \in \bigcup_{n\geq 1}(R^{-1})^n\end{aligned}$$

(3) $R^n \cup S^n \subseteq (R \cup S)^n$ for all $n \geq 1$. The basis step is obvious. The induction step is:

$$R^n \cup S^n \subseteq (R \cup S)^n \implies R^{n+1} \cup S^{n+1} \subseteq (R \cup S)^{n+1}$$

The result holds by

$$\begin{aligned}(R \cup S)^{n+1} &= (R \cup S)^n \circ (R \cup S)\\ &\supseteq (R^n \cup S^n) \circ (R \cup S)\\ &= [(R^n \cup S^n) \circ R] \cup (R^n \cup S^n) \circ S\\ &= R^{n+1} \cup (S^n \circ R) \cup (R^n \circ S) \cup S^{n+1}\\ &\supseteq R^{n+1} \cup S^{n+1}.\end{aligned}$$

□

The next theorem will be very useful when we discuss transtive relations.

Theorem 5.38. *Let R be a relation on X. Then $(x, y) \in R^n$ if and only if there exists $x_1, x_2, x_3, \dots, x_{n-1} \in X$ such that $(x, x_1) \in R, (x_1, x_2) \in R, ..., (x_{n-1}, y) \in R$.*

Proof. Bases case, $i = 1$ is obvious. We assume the claim is true for j. Then

$$\begin{aligned}
&(x, y) \in R^{j+1} \iff (x, y) \in R^j \circ R \\
&\iff \exists x_1 \in X, (x, x_1) \in R \wedge (x_1, y) \in R^j \\
&\iff \exists x_1 \in X, (x, x_1) \in R \wedge \exists x_2, ..., x_{j-1} \in X, (x_2, x_3), ..., (x_{j-1}, y) \in R \\
&\iff \exists x_1 \in X, x_2, ..., x_{j-1} \in X, (x, x_1), (x_2, x_3), ..., (x_{j-1}, y) \in R
\end{aligned}$$

as needed to complete induction.

□

5.6 Exercises

Exercise 5.1. Finish proving Theorem 5.29.

Chapter 6

Well-founded Confluence

For example, the relation "is less than" is well-founded on the natural numbers, because there is no sequence of natural numbers that go from a smaller number to a larger number. On the other hand, the relation "is taller than" is not well-founded, because there is an infinite sequence of people (starting with someone who is very short) who are all taller than each other. Well-founded relations can be used to solve problems in a variety of fields, including economics, computer science, and physics.

In mathematics, a well-founded relation is a binary relation that satisfies the descending chain condition. In other words, it contains no infinite descending chains. In fact, these two conditions are equivalent, assuming the axiom of dependent choice.

In mathematics and computer science, recursion is a method of defining functions in which the function being defined is applied within its own definition. The most common form of recursion is fractional recursion, in which a function is defined in terms of itself divided by some well-founded relation.

In computers, recursion is used to implement procedures that iterate over data structures or perform computations on infinite sets of data. Recursive programming techniques can be used to solve problems that would be difficult or impossible to solve using other programming paradigms. However, they can also introduce errors that are difficult to debug, and they can be computationally expensive. As a result, care must be taken to use recursion judiciously. When used properly, it can be an immensely powerful tool for solving complex problems.

The well-foundedness condition is what makes recursion possible. Without it, we would not be able to define functions by recursion, and many of the things we take for granted in computer science would not be possible.

6.1 Well-Founded Relations

Definition 6.1. Let X be a set.

1. A relation R on X is called **irreflexive** if it satisfies the property
$$\forall a \in X, (a, a) \notin R.$$
2. A relation R on X is called **asymmetric** if it satisfies the property
$$\forall a, b \in X, (a, b) \in R \implies (b, a) \notin R.$$
3. A relation R on X is called **antisymmetric** if it satisfies the property
$$\forall a, b \in X, (a, b) \in R \wedge (b, a) \in R \implies a = b.$$

A $\longrightarrow$-minimal element need not be smaller than the other elements of X. For example, singleton sets of X all have $\longrightarrow$-minimal elements, namely a is a $\longrightarrow$-minimal element of $\{a\} \subseteq X$ since there does not exist $b \in \{a\}$ such that $a \longrightarrow b$ whenever $\longrightarrow$ is irreflexive.

Lemma 6.1. *If $\longrightarrow$ is a well-founded relation on X, then $\longrightarrow$ is irreflexive and antisymmetric; and hence also asymmetric.*

Proof. Assume $\longrightarrow$ is a well-founded relation on X. If $a \longrightarrow a$, then $A = \{a\} \neq \emptyset$ does not have an $\longrightarrow$-minimal element, country to hypothesis. If $a \longrightarrow b$ and $b \longrightarrow a$, then $X = \{a, b\} \neq \emptyset$ does not have a $\longrightarrow$-minimal element, contrary to hypothesis. Thus, if $\longrightarrow$ is well-founded and $a \longrightarrow b$, then $b \longrightarrow a$ can not hold and so $\longrightarrow$ is asymmetric. A relation is asymmetric if and only if it is both antisymmetric and irreflexive.

□

Lemma 6.2. *If $\longrightarrow$ is a well-founded relation on X and $\longrightarrow'$ is a subrelation of $\longrightarrow$, then $\longrightarrow'$ is well-founded on X.*

Proof. Assume $\longrightarrow$ is well-founded on X and let $\longrightarrow'$ be a subrelation of $\longrightarrow$. Let $A \neq \emptyset$ be a subset of X. Suppose A does not have a $\longrightarrow'$-minimal element. Thus for all $a \in A$ there exists $b \in A$ that $a \longrightarrow' b$ holds. Since $\longrightarrow'$ is a subrelation of $\longrightarrow$, it follows that for all $a \in A$ there exists $b \in A$ such that $a \longrightarrow b$. Thus A does not have a $\longrightarrow$-minimal element, contrary to hypothesis.

□

Definition 6.2. Let $\longrightarrow$ be a relation on X.

1. If $A \subseteq X$ and $a \in A$, then a is called a $\longrightarrow$- **minimal element** of A if there does not exist $b \in A$ such that $a \longrightarrow b$.
2. If each nonempty subset of X has a $\longrightarrow$-minimal element, then $\longrightarrow$ is called a **well-founded relation** on X.
3. If $x \in X$, then the set

$$\overrightarrow{x} = \{y \in X : x \longrightarrow y \wedge x \neq y\}$$

is called the **initial segment** of x.

Clearly, b is a $\longrightarrow$-minimal element of A if and only if $\overrightarrow{b} \cap A = \emptyset$.

Well-Founded Induction

Lemma 6.3. *A relation $\longrightarrow$ on X is well-founded if and only if the principle of $\longrightarrow$-induction holds:*

$$\forall\, A \subseteq X, \forall x \in X, (\overrightarrow{x} \subseteq A \implies x \in A) \implies A = X.$$

Proof. Assume $\longrightarrow$ is well-founded on X. Let $A \subseteq X$ and assume the following holds

$$\forall x \in X, \overrightarrow{x} \subseteq A \implies x \in A \tag{6.1}$$

Assume for a contradiction that $X \quad A$ is nonempty with $\longrightarrow$-minimial element b. Thus $\overrightarrow{b} \cap X \quad A = \emptyset$ and so it follows $\overrightarrow{b} \subseteq A$. By (6.1) we have $b \in A$ and thus $X \quad A$ is empty. Hence $A = X$.

Conversely, assume the principle of induction holds and suppose A is a nonempty subset of X with no $\longrightarrow$-minimal element. We will apply the principle of $\longrightarrow$ induction to the set $X \ A$. Let $x \in X$ and assume $\overrightarrow{x} \subseteq X \ A$. Suppose $x \in A$. Since $\overrightarrow{x} \cap A = \emptyset$ it follows x is a $\longrightarrow$-minimal element of A contrary to hypothesis. Thus, it follows $x \notin A$ and so $x \in X \quad A$. We have shown

$$\forall x \in X, \overrightarrow{x} \subseteq X \quad A \implies x \in X \quad A$$

By the principle of $\longrightarrow$-induction it follows $X \quad A = X$. Therefore, A is empty as desired.

□

Well-Founded Recursion

Definition 6.3. Let Y be a set and let $h : X \times P(Y) \to Y$ be a function. We call a function $f : X \to Y$ a $\longrightarrow$- **recursively defined function** if

$$f(x) = h(x, f(\overrightarrow{x})) \tag{6.2}$$

for all $x \in X$.

Lemma 6.4 (Well-Founded Recursion). *Let $\longrightarrow$ be a relation on X. Then the following are equivalent. 1. $\longrightarrow$ is well founded on X 2. for every set Y, there exists $\longrightarrow$-recursively defined functions from X to Y 3. $\longrightarrow$-recursively defined functions on X are unique*

Proof. This proof is not completely rigorous not finished.

(1) $\Leftrightarrow$ (2): Assume $\longrightarrow$ is well-founded on X. Let Y be a set and let $h : X \times P(Y) \to Y$. Consider functions g defined on subsets of X with values in Y. We say $R(g)$ holds if both conditions are satisfied:

- for all $x \in D(g)$, $\overrightarrow{x} \subseteq D(g)$
- for all $x \in D(g)$, $g(x) = h(x, g(\overrightarrow{x}))$

Claim: If $R(g_1)$ and $R(g_2)$ hold, then $x \in D(g_1) \cap D(g_2)$ implies $g_1(x) = g_2(x)$. The proof of this claim follows by $\longrightarrow$-induction.

Claim: Let $f = \cup\{g : R(g) \text{ holds}\}$. Clearly f is a relation with domain included in X. We claim f is a function. To prove this we have to show that if $g_1, g_2 \in \{g : R(g) \text{ holds}\}$ and $x \in D(g_1) \cap D(g_2)$, then $g_1(x) = g_2(x)$. Now $Z = D(g_1) \cap D(g_2)$ is an initial segment of $\longrightarrow$ and $\longrightarrow' = \longrightarrow \cap (Z \times Z)$ is well-founded on Z. It follows by induction on $\longrightarrow'$ that if $x \in Z$, then $g_1(x) = g_2(x)$.

Claim: f is maximal such that $R(f)$ holds. Next we claim that

$$x \in D(f) \implies f(x) = g(x, f(\overrightarrow{x})). \tag{6.3}$$

To prove (6.3) assume $x \in D(f)$. Then $x \in D(g)$ for some g such that $R(g)$ holds. It follows that

$$f(x) = g(x) = h(x, \{g(\overrightarrow{x})) = h(x, \{f(\overrightarrow{x})\}).$$

Claim: $D(f) = X$. The proof of this claim follows by $\longrightarrow$-induction. Let x be such that $\overrightarrow{x} \subseteq D(f)$. Since $D(f)$ is an initial segment of $\longrightarrow$, so is $D(f) \cup \{x\}$. Let

$$f' = f \cup \{x, g(x, f(\overrightarrow{x}))\}.$$

Then $R(f')$ holds and hence $x \in D(f)$.

Conversely, we assume the principle of definition of recursion to hold. We define a rank function

$$rk(x) = \sup_{x \longrightarrow y} rk(y).$$

It then follows that $\longrightarrow$ is well-founded since

$$x \longrightarrow y \Leftrightarrow rk(y) \in rk(x).$$

Alternatively, we can simplify the proof by assuming $\longrightarrow$ is transitive. Suppose A is a subset of X that has no minimal element, and define (by recursion applied to the characteristic function of M):

x belongs to M if and only if for every $x \longrightarrow y$, if y is in A then y is not in M.

Then for x in A, if x is in M there is a $x \longrightarrow y$ in A (since A has no minimal element) which is not in M. But then there is a $y \longrightarrow z$ in A which is in M, and since $x \longrightarrow z$ we have a contradiction. So no x in A is in M. But then every x in A is in M, so A must be empty. We thus see that given the defining property of M, the assumption that A has no minimal element, and the transitivity of $\longrightarrow$, logical manipulation allows us to conclude that A is empty.

(1) $\Leftrightarrow$ (3): Assume $\longrightarrow$ is well-founded on X. We say that $\phi : Z \to Y$ is an attempt if Z is an initial segment of X, and

$$\phi(x) = g(x, \{\phi(z) : x \longrightarrow z\}) \quad \text{for all } x \in Z.$$

If $\phi_1 : Z_1 \to Y$ and $\phi_2 : Z_2 \to Y$ are two attempts, they agree on $Z_1 \cap Z_2$ namely $\phi_1|_{Z_1 \cap Z_2} = \phi_2|_{Z_1 \cap Z_2}$. Because $X_1 \cap X_2$ is clearly an initial segment of X and if as attempts that do not agree there is some x_0 which is $\longrightarrow$-minimal in $\{x \in Z_1 \cap Z_2 : \phi_1(x) \neq \phi_2(x)\}$. But in that case we have

$$\phi_1(x_0) = g(x_0, \{\phi_0(x) : x_0 \longrightarrow x\}) = g(x_0, \{\phi_1(x) | x_0 \longrightarrow x\})$$

a contradiction.

Conversely, we will show uniqueness implies well-foundedness. Assume X is nontrivial by having two elements, say a_0 and a_1.

□

Chains

The next proposition asserts that every relation $\longrightarrow$ on X is well-founded if and only if every $\longrightarrow$-chain in X is finite.

Lemma 6.5. *Let $\longrightarrow$ be a relation on X. Then $\longrightarrow$ is well-founded if and only there are no infinitely descending $\longrightarrow$-chains.*

Proof. Assume there exists an infinite descending $\longrightarrow$-chain B. Then $B \subseteq A$ has no $\longrightarrow$-minimal element and thus $\longrightarrow$ is not well-founded. The result follows by contrapositive.

Conversely, assume for a contradiction that B is a nonempty subset of X with no $\longrightarrow$-minimal element. Then the set $A_a = \{b \in B : b \longrightarrow a\}$ is nonempty for each $a \in B$, for otherwise a would be an $\longrightarrow$-minimal element of B. The principle of choice, applied to the family $\{A_a\}_{a \in B}$, provides a function

$$f : B \longrightarrow \bigcup_{a \in B} A_a \subseteq B \text{ with } f(a) \longrightarrow a, \text{ for all } a \in B.$$

Since B is nonempty, fix $a_0 \in B$. Define the sequence $\{a_n\}_{n \in \mathbb{N}}$ recursively by $a_{n+1} = f(a_n)$ and notice this sequence forms a strictly descending $\longrightarrow$-chain. This contradicts the assumption that there are no strictly descending $\longrightarrow$-chains in X. Thus every nonempty subset of B must have a $\longrightarrow$-minimal element.

□

::: {#lem-well-founded-relation-unique function } Let X and Y be sets. Let $\longrightarrow$ be a well-founded relation on X, and let $g : X \times P(Y) \to Y$ be a function. Then there exists a unique function $f : X \to Y$ such that

$$f(x) = g(x, \{f(z) : x \longrightarrow z\})$$

for all $x \in X$. :::

Proof. We say that $\phi : Z \to Y$ is an attempt if Z is an initial segment of X, and

$$\phi(x) = g(x, \{\phi(z) : x \longrightarrow z\}) \quad \text{for all } x \in Z.$$

If $\phi_1 : Z_1 \to Y$ and $\phi_2 : Z_2 \to Y$ are two attempts, they agree on $Z_1 \cap Z_2$ namely $\phi_1|_{Z_1 \cap Z_2} = \phi_2|_{Z_1 \cap Z_2}$. Because $X_1 \cap X_2$ is clearly an initial segment of X and if as attempts that do not agree there is some x_0 which is $\longrightarrow$-minimal in $\{x \in Z_1 \cap Z_2 : \phi_1(x) \neq \phi_2(x)\}$. But in that case we have

$$\phi_1(x_0) = g(x_0, \{\phi_0(x) : x_0 \longrightarrow x\}) = g(x_0, \{\phi_1(x) | x_0 \longrightarrow x\})$$

a contradiction.

Now let $f = \cup\{\phi : \phi \text{ is an attempt}\}$, so $f(x) = \phi(x)$ if there is an attempt ϕ with $x \in D(\phi)$. It is clear that $D(f) = \cup\{D(\phi) : \phi \text{ is an attempt}\}$ is an initial segment of X, and that f satisfies $f(x) = g(x, f(z) | x \longrightarrow z)\}$ for all $x \in D(f)$. So all that remains to be shown is that $D(f) = X$.

But if $D(f) \neq X$ there is some x_0 that is $\longrightarrow$ minimal in $\{x \in X : x \notin D(f)\}$. For such an x define $\overline{f} : D(f) \cup \{x_0\} \to Y$ by

$$\overline{f}(x) = \begin{cases} f(x) & \text{if } x \in D(f) \\ g(x_0, \{f(x) : x_0 \longrightarrow x\}) & \text{if } x = x_0. \end{cases}$$

Then one would clearly have that $\overline{f}$ is an attempt, but is not a subset of f. Hence a contradiction and so $f : X \to Y$ as desired.

□

Lemma 6.6. *Let $f : X \to Y$ be a function. If $\longrightarrow_Y$ is a well-founded relation on Y, then the relation defined on X by $x \longrightarrow_X y \Leftrightarrow f(x) \longrightarrow_Y f(y)$ is well-founded.*

Proof. Any infinite descending $\longrightarrow_X$-chain leads to an infinite descending $\longrightarrow_Y$-chain.

□

Lemma 6.7. *Let $\longrightarrow$ be a relation on X. Then $\longrightarrow$ is well-founded if and only if $\longrightarrow^+$ is well-founded.*

Proof. Clearly any infinite descending chain

$$x_0 \longrightarrow^+ x_1 \longrightarrow^+ x_2 \longrightarrow^+ \cdots$$

would induce an infinite descending chain with respect to $\longrightarrow$. This follows easily since $\longrightarrow \subseteq \longrightarrow^+$ and that any subrelation of a well-founded relation is a well-founded relation. Conversely, in order to show $\longrightarrow^+$ is well-founded, assume

$$x_1 \longrightarrow^+ x_2 \longrightarrow^+ x_3 \longrightarrow^+ \cdots$$

is an infinite descending $\longrightarrow^+$-chain. Then there exists $i_j \geq 1$ such that $x_j \longrightarrow^{i_j} x_{j+1}$ for all $j \geq 1$. This implies that

$$x_1 \longrightarrow^{i_1} x_2 \longrightarrow^{i_2} x_3 \longrightarrow^{i_3} \cdots$$

is an infinite $\longrightarrow$-chain. But this contradicts the well-foundedness of $\longrightarrow$.

□

6.2 Confluent Relations

This chapter is covers reduction relations, Newmann's Lemma, Buchberger-Winkler's Property, and more.

Reduction Relation

A **reduction relation** is a binary relation with additional properties that allow us to model the idea of *reduction.* In particular, we will consider well-founded relations as a starting point. Moreover, since the transitive closure of a well-founded relation is also well-founded relation, we will also study partial order relations.

A confluent relation is a binary relation that is both left-confluent and right-confluent. In other words, for every element in the relation, there is a unique element that it can be reduced to on the left side and a unique element that it can be reduced to on the right side.

Confluent relations are used in a variety of different contexts, including computer science, mathematics, and physics. In computer science, they are used to define algorithms; in mathematics, they are used to study equations and systems of equations; in physics, they are used to model physical phenomena. Further, they are used in the study of abstract data types, formal language theory, automata theory, and compiler design.

Newman's lemma is a result in confluent relations that suggests a local confluence and confluence are equivalent whenever the relation is well-founded. The lemma is named for Max Newmann, who proved the result in 1936.

A confluent relation is one in which every pair of connected elements can be brought into a common cluster. In other words, if you have two elements that are related by the confluent relation, there must be a third element that is related to both of them. Local confluence is a weaker form of confluence that only requires every pair of connected elements to be brought into a common cluster if they share a certain property.

The lemma has important implications for confluent relations, as it provides a way to check whether a given relation is confluent or not.

Newmann's lemma has many applications in different areas of mathematics and computer science. In particular, it is used in the study of abstract data types, formal language theory, automata theory, and compiler design.

In this chapter, you'll learn about the Buchberger-Winkler Property (also called the generalized Newman's Lemma) and about abstract reduction systems.

In short, under well-foundedness, confluent means that given any two "paths" emanating from some element in the set, there is always a unique way to combine those paths so as to get back to the original element. Moreover, an abstract reduction system is simply a confluent and well-founded reduction relation on some set. The importance of abstract reduction systems lies in the fact that they can be used to model a wide variety of systems, ranging from computational systems to biological systems.

Confluence

Confluent relations are important in the study of rewriting systems, as they ensure that any two equivalent elements can be transformed into each other by repeatedly applying the rules of the system. Moreover, confluent relations have the property that any two elements that are related by R can be "reached" from each other by following a path through the relation. As a result, confluent relations play an important role in the study of rewriting systems.

We discuss confluent relations; in particular, we prove Newman's Lemma: that local confluence, confluence, the Church-Rosser property, and the unique normal forms property are all equivalent for a well-founded relation. We also give a generalization of Newman's lemma based on the Buchberger-Winkler's Property.

Let $\longrightarrow$ be a relation on X. If there exists $c \in X$ such that $a \overset{*}{\longrightarrow} c$ and $b \overset{*}{\longrightarrow} c$, then a and b are said to have a **common successor**, denoted by $a \downarrow b$. If there does not exist $b \in X$ such that $a \longrightarrow b$, then a is called a normal form of $\longrightarrow$. If $a \overset{*}{\longrightarrow} b$ and b is a normal form, then b is called a **normal form** of X.

Theorem 6.1. *Well-founded implies every element has a normal form.*

Definition 6.4. Let $\longrightarrow$ be a relation on X.

1. A relation $\longrightarrow$ is called **locally confluent** whenever $a \longrightarrow b$ and $a \longrightarrow c$ implies $b \downarrow c$, for all $a, b, c \in X$.
2. A relation $\longrightarrow$ is called **confluent** whenever $a \overset{*}{\longrightarrow} b$ and $a \overset{*}{\longrightarrow} c$ implies $b \downarrow c$, for all $a, b, c \in X$.
3. A relation $\longrightarrow$ is said to satisfy the **unique normal forms property** if $a \overset{*}{\longrightarrow} b$ and $a \overset{*}{\longrightarrow} c$ with b and c in $\longrightarrow$-normal form implies $b = c$, for all $a, b, c \in X$.
4. A relation $\longrightarrow$ is said to have the **Church-Rosser property** whenever $b \overset{*}{\longleftrightarrow} c$ implies $b \downarrow c$, for all $a, b, c \in X$.

Newman's Lemma

Theorem 6.2. *Let $\longrightarrow$ be a well-founded relation on X. Then the following properties are equivalent.*

1. *local confluence*
2. *confluence*
3. *unique normal forms*
4. *Church-Rosser property*

Proof. (1) $\Rightarrow$ (2): Assume for a contradiction that $\longrightarrow$ is locally confluent but that the set

$$T = \left\{ a \in X : \exists\, b, c \in X \text{ with } a \overset{*}{\longrightarrow} b \text{ and } a \overset{*}{\longrightarrow} c \text{ but not } b \downarrow c \right\}$$

is non-empty. Since $\longrightarrow$ is well-founded, T has a $\longrightarrow$-minimial element a. Let $b, c \in X$ with $a \overset{*}{\longrightarrow} b$ and $a \overset{*}{\longrightarrow} c$, but not $b \downarrow c$. If $a = b$ or $a = c$, then it trivially follows $b \downarrow c$. Otherwise there must exist $b', c' \in X$ (possibly $b' = b$ or $c' = c$) with

$$a \longrightarrow b' \overset{*}{\longrightarrow} b \quad \text{and} \quad a \longrightarrow c' \overset{*}{\longrightarrow} c.$$

By the local confluence of $\longrightarrow$, there exists $d \in X$ with

$$a \longrightarrow b' \overset{*}{\longrightarrow} d \quad \text{and} \quad a \longrightarrow c' \overset{*}{\longrightarrow} d.$$

By the minimality of a in T it follows $b' \notin T$, and so there exists $e \in X$ with

$$a \longrightarrow b' \overset{*}{\longrightarrow} b \overset{*}{\longrightarrow} e \quad \text{and} \quad a \longrightarrow b' \overset{*}{\longrightarrow} d \overset{*}{\longrightarrow} e.$$

Then $a \longrightarrow c' \overset{*}{\longrightarrow} d \overset{*}{\longrightarrow} e$ and again by the minimality of a in T it follows $c' \notin T$. Thus there exists $f \in X$ with

$$a \longrightarrow c' \overset{*}{\longrightarrow} d \overset{*}{\longrightarrow} e \overset{*}{\longrightarrow} f \quad \text{and} \quad a \longrightarrow c' \overset{*}{\longrightarrow} c \overset{*}{\longrightarrow} f.$$

Therefore we have shown

$$a \longrightarrow b' \overset{*}{\longrightarrow} b \overset{*}{\longrightarrow} e \overset{*}{\longrightarrow} f \quad \text{and} \quad a \longrightarrow c' \overset{*}{\longrightarrow} c \overset{*}{\longrightarrow} f.$$

and so $b \downarrow c$ which is contrary to assumption.

(2) $\Rightarrow$ (3): Let $a \overset{*}{\longrightarrow} b$ and $a \overset{*}{\longrightarrow} c$, and suppose b and c are in $\longrightarrow$-normal form. There exists $d \in X$ with $b \overset{*}{\longrightarrow} d$ and $c \overset{*}{\longrightarrow} d$, and thus $b = d = c$.

(3) $\Rightarrow$ (4): Claim: by induction on $k \in \mathbb{N}$ that for all $a, b \in X$ with $a \overset{k}{\longleftrightarrow} b$ it follows that $a \downarrow b$. The case $k = 0$ is trivial. Now let $a \overset{k+1}{\longleftrightarrow} b$,

say $a \overset{k}{\longleftrightarrow} c \longleftrightarrow b$. Then by induction hypothesis there exists $d \in X$ with $a \overset{*}{\longrightarrow} d$ and $c \overset{*}{\longrightarrow} d$. If $b \longrightarrow c$, then $a \overset{*}{\longrightarrow} d$ and $b \overset{*}{\longrightarrow} d$ and so $a \downarrow b$. For the other case, assume $c \longrightarrow b$. Let d' be a normal form of d and let b' be a normal form of b with respect to $\longrightarrow$. Then $c \overset{*}{\longrightarrow} b'$ and $c \overset{*}{\longrightarrow} d'$, and so d' and b' are normal forms of c and hence equal. Thus we have $a \overset{*}{\longrightarrow} d'$ and $b \overset{*}{\longrightarrow} d'$, which means $a \downarrow b$.

(4) ⇒ (1): If $a \longrightarrow b$ and $a \longrightarrow c$, then $b \overset{*}{\longleftrightarrow} c$, and so it follows $b \downarrow c$.

□

Corollary 6.1. *If $\longrightarrow$ is confluent and $a \overset{*}{\longleftrightarrow} b$, then*

1. *if b is in normal form, then $a \overset{*}{\longrightarrow} b$, and*
2. *if a and b are in normal form, then $a = b$.*

Proof. This proof is left as an exercise.

□

Thus we know that for confluent relations, two elements are equivalent if and only if they have a common successor.

Connected Below

In this part we follows the ideas in buchberger1983criterion.

Definition 6.5. Let $\longrightarrow$ be a relation on X.

1. If there exists $c_1, c_2, \dots, c_n \in X$ such that

$$b_1 = c_1 \longleftrightarrow c_2 \longleftrightarrow \cdots \longleftrightarrow c_n = b_2$$

   and $a \longrightarrow^+ c_i$ for $i = 1, 2, \dots, n$, then b_1 and b_2 are said to be *connected below* a, denoted by $b_1 \overset{a}{\longleftrightarrow} b_2$.
2. A relation $\longrightarrow$ on X is said to have the **Buchberger-Winkler property** whenever $a \longrightarrow b$ and $a \longrightarrow c$ implies $b \overset{a}{\longleftrightarrow} c$ for all $a, b, c \in X$.

Theorem 6.3. *Let $\longrightarrow$ be a well-founded relation on X. Then $\longrightarrow$ is confluent if and only if the Buchberger-Winkler property holds.*

Proof. Suppose $\longrightarrow$ is confluent and $a \longrightarrow b$ and $a \longrightarrow c$ for $a, b, c \in X$. Then there exists d such that $b \overset{*}{\longrightarrow} d$ and $c \overset{*}{\longrightarrow} d$. It follows that $b \overset{a}{\longleftrightarrow} c$.

Conversely, assume a, b, c are arbitrary, but fixed such that $a \overset{*}{\longrightarrow} b$ and $a \overset{*}{\longrightarrow} c$. The proof follows by induction on $\longrightarrow$. The first induction hypothesis is:

$$\forall\, a'\ (a \longrightarrow^{+} a'), \forall\, b', c'\ (\text{if } a' \overset{*}{\longrightarrow} c' \text{ and } a' \overset{*}{\longrightarrow} b', \text{ then } b' \downarrow c').$$

It is required to show $b \downarrow c$, that is $b \overset{*}{\longrightarrow} d$ and $c \overset{*}{\longrightarrow} d$ for some d. The cases $a = b$ or $a = c$ are trivial. Assume $a \neq b$ and $a \neq c$. Then there exist b_1 and c_1 such that $a \longrightarrow b_1 \overset{*}{\longrightarrow} b$ and $a \longrightarrow c_1 \overset{*}{\longrightarrow} c$. By assuming $\longrightarrow$ has the Buchberger property, there exists $e_1, e_2, \dots, e_n$ such that $b_1 = e_1 \longleftrightarrow e_2 \longleftrightarrow \cdots \longleftrightarrow e_n = c_1$ and $a \longrightarrow^{+} e_i$. we will proceed by induction on n and show: for all n, for all $e_1, e_2, \dots, e_n$:

$$\text{if} \quad e_1 \longleftrightarrow e_2 \longleftrightarrow \cdots \longleftrightarrow e_n \quad \text{with} \quad a \longrightarrow^{+} e_i, \qquad \text{then} \qquad e_1 \downarrow e_n. \quad (*)$$

Notice (*) is clear for $n = 1$. Our second induction hypothesis is: (*) is true for some n. Assume $e_1 \longleftrightarrow e_2 \longleftrightarrow \cdots \longleftrightarrow e_n \longleftrightarrow e_{n+1}$ and $a \longrightarrow^{+} e_i$ for $i = 1, 2, \dots, n+1$. By induction hypothesis 2, there exists d_1 such that $e_1 \overset{*}{\longrightarrow} d_1$ and $e_n \overset{*}{\longrightarrow} d_1$. If $e_{n+1} \longrightarrow e_n$ then $e_{n+1} \overset{*}{\longrightarrow} d_1$ and so $e_1 \downarrow e_{n+1}$. If $e_n \longrightarrow e_{n+1}$, then by induction hypothesis 1, there exists d_1' such that $d_1 \overset{*}{\longrightarrow} d_1'$ and $e_{n+1} \overset{*}{\longrightarrow} d_1'$. Thus, it follows $e_1 \downarrow e_{n+1}$ in this case as well. Therefore, (*) is proven by induction and so d_1 exists such that $e_1 \overset{*}{\longrightarrow} d_1$ and $e_n \overset{*}{\longrightarrow} d_1$ for all n. Then, $b_1 \overset{*}{\longrightarrow} d_1$, $b_1 \overset{*}{\longrightarrow} b$, and $a \longrightarrow b_1$ implies, by induction hypothesis 1, that there exists f such that $b \overset{*}{\longrightarrow} f$ and $d_1 \overset{*}{\longrightarrow} f$. It follows that, $c_1 \overset{*}{\longrightarrow} c$ and $c_1 \overset{*}{\longrightarrow} f$. Again by induction hypothesis 1, there exists d such that $f \overset{*}{\longrightarrow} d$ and $c \overset{*}{\longrightarrow} d$. Therefore, it follows $b \overset{*}{\longrightarrow} d$ and $c \overset{*}{\longrightarrow} d$.

□

Terminating

Let X be a set and $\to$ a reduction (binary relation) on X. A **chain** with respect to $\to$ is a sequence of elements $x_1, x_2, x_3, \dots$ in X such that $x_1 \to x_2$, $x_2 \to x_3$, etc. A chain with respect to $\to$ is usually written

$$x_1 \to x_2 \to x_3 \to \cdots \to x_n \to \cdots.$$

The length of a chain is the cardinality of its underlying sequence. A chain is finite if its length is finite. Otherwise, it is infinite.

Definition 6.6. A reduction $\to$ on a set X is said to be **terminating** if it has no infinite chains. In other words, every chain **terminates**.

Here are a few examples.

- If $\to$ is reflexive, or non-trivial symmetric, then it is never terminating.
- Let X be the set of all positive integers greater than 1. Define $\to$ on X so that $a \to b$ means that $a = bc$ for some $c \in X$. Then $\to$ is a terminating reduction. By the way, $\to$ is also a normalizing reduction.
- In fact, it is easy to see that a terminating reduction is normalizing: if a has no normal form, then we may form an infinite chain starting from a.
- On the other hand, not all normalizing reduction is terminating. A canonical example is the set of all non-negative integers with the reduction $\to$ defined by $a \to b$ if and only if either $a, b \neq 0$, $a \neq b$, and aj, and j arbitrary.
- The reflexive transitive closure of a terminating relation is a partial order.

A closely related concept is the descending chain condition (DCC). A reduction $\to$ on X is said to satisfy the **descending chain condition (DCC)** if the only infinite chains on X are those that are eventually constant. A chain $x_1 \to x_2 \to x_3 \to \cdots$ is eventually constant if there is a positive integer N such that for all $n \geq N$, $x_n = x_N$. Every terminating relation satisfies DCC. The converse is obviously not true, as a reflexive reduction illustrates.

Another related concept is acyclicity. Let $\to$ be a reduction on X. A chain $x_0 \to x_1 \to \cdots x_n$ is said to be cyclic if $x_i = x_j$ for some $0 \leq i < j \leq n$. This means that there is a "closed loop' ' in the chain. The reduction $\to$ is said to be **acyclic** if there are no cyclic chains with respect to $\to$. Every terminating relation is acyclic, but not conversely. The usual strict inequality relation on the set of positive integers is an example of an acyclic but non-terminating relation.

6.3 Exercises

Chapter 7

Connect Everything

7.1 Preorders

7.2 Equivalence Relations

The Reflexive, Symmetric, and Transitive Properties

Definition 7.1. Let X be a set.

1. A relation R on X is called **reflexive** if it satisfies the property
$$\forall a \in X, (a, a) \in R.$$
2. A relation R on X is called **symmetric** if it satisfies the property
$$\forall a, b \in X, (a, b) \in R \implies (b, a) \in R.$$
3. A relation R on X is called **transitive** if it satisfies the property
$$\forall a, b, c \in X, ((a, b) \in R \wedge (b, c) \in R) \implies (a, c) \in R.$$

Theorem 7.1. *Let R and S be relations on X and let $A \subseteq X$.*

1. *A relation R is reflexive if and only if $I \subseteq R$.*
2. *A relation R is symmetric if and only if $R^{-1} \subseteq R$.*
3. *A relation R is transitive if and only if $R \circ R \subseteq R$.*

Proof. The proof of each part follows.

1. If R is reflexive, then $I \subseteq R$.

$$(x,y) \in I \Leftrightarrow y = x \implies (x,y) \in R$$

Conversely, if $I \subseteq R$, then R is reflexive.

$$x \in X \implies (x,x) \in I \implies (x,x) \in R$$

2. If R is symmetric, then $R^{-1} \subseteq R$.

$$(x,y) \in R^{-1} \Leftrightarrow (y,x) \in R \implies (x,y) \in R$$

Conversely, if $R^{-1} \subseteq R$, then R is symmetric.

$$(x,y) \in R \implies (y,x) \in R^{-1} \implies (y,x) \in R$$

3. If R is transitive, then $R \circ R \subseteq R$.

$$(x,y) \in R \circ R \Leftrightarrow \exists x \in X, (x,z) \in R \wedge (z,y) \in R \implies (x,y) \in R$$

Conversely, if $R \circ R \subseteq R$, then R is transitive.

$$(x,y) \in R \wedge (y,z) \in R \implies (x,z) \in R \circ R \implies (x,z) \in R.$$

The proof is now complete.

□

Theorem 7.2. *If R and S are reflexive, then $R|_A$, R^{-1}, $S \circ R$, $R \cup S$, and $R \cap S$ are also reflexive, while R^c is not reflexive.*

Proof. We find that $R|_A$, R^{-1}, $S \circ R$, $R \cup S$, and $R \cap S$ are reflexive, whenever R and S are reflexive by the following arguments, respectively.

- $(x,x) \in R \wedge A \subseteq X \implies (x,x) \in R|_A$
- $(x,x) \in R \implies (x,x) \in R^{-1}$
- $(x,x) \in R \wedge (x,x) \in S \implies (x,x) \in S \circ R$
- $(x,x) \in R \wedge (x,x) \in S \implies (x,x) \in R \cup S$
- $(x,x) \in R \wedge (x,x) \in S \implies (x,x) \in R \cap S$

Notice that R^c is not reflexive because $I \subseteq R \implies I \not\subseteq R^c$.

□

Theorem 7.3. *If R and S are symmetric, then $R|_A$, R^c, R^{-1}, $R^{-1} \circ R$, $R \cup S$, and $R \cap S$ are also symmetric.*

Proof. If R is symmetric, then $R|_A$ is symmetric.

$$\begin{aligned}(x,y) \in R|_A &\iff (x,y) \in (A \times A) \cap R \\ &\iff (x,y) \in A \times A \wedge (x,y) \in R \iff (y,x) \in A \times A \wedge (y,x) \in R \\ &\iff (y,x) \in (A \times A) \cap R \iff (x,y) \in R|_A\end{aligned}$$

If R is symmetric, then R^c is symmetric.

$$\begin{aligned}(x,y) \in R^c &\iff (x,y) \notin R \iff \neg((x,y) \in R) \\ &\iff \neg((y,x) \in R) \iff (y,x) \notin R \iff (y,x) \in R^c\end{aligned}$$

If R is symmetric, then R^{-1} is symmetric.

$$(x,y) \in R^{-1} \iff (y,x) \in R \iff (x,y) \in R \iff (y,x) \in R^{-1}$$

If R and S are symmetric, then $R \cup S$ is symmetric.

$$\begin{aligned}(x,y) \in R \cup S &\iff (x,y) \in R \vee (x,y) \in S \\ &\iff (y,x) \in R \vee (y,x) \in S \iff (y,x) \in R \cup S\end{aligned}$$

If R and S are symmetric then the relation $R \cap S$ is symmetric.

$$\begin{aligned}(x,y) \in R \cap S &\iff (x,y) \in R \wedge (x,y) \in S \\ &\iff (y,x) \in R \wedge (y,x) \in S \iff (y,x) \in R \cap S\end{aligned}$$

If R is symmetric, then $R^{-1} \circ R$ is symmetric.

$$\begin{aligned}(x,y) \in R^{-1} \circ R &\iff \exists z \in X, (x,z) \in R \wedge (z,y) \in R^{-1} \\ &\iff \exists z \in X, (z,x) \in R^{-1} \wedge (y,z) \in R \\ &\iff \exists z \in X, (y,z) \in R \wedge (z,x) \in R^{-1} \iff (y,x) \in R^{-1} \circ R\end{aligned}$$

The proof is now complete.

□

Theorem 7.4. *Let R and S be relations on X and let $A \subseteq X$. If R and S are transitive, then $R|_A$, R^{-1}, R^2, and $R \cap S$ are also transitive, while R^c and $R \cup S$ are not transitive.*

Proof. If R is transitive, then $R|_A$ is transitive.

$$\begin{aligned}&(x,y) \in R|_A \wedge (y,z) \in R|_A \\ &\quad\iff [(x,y) \in A \times A \wedge (x,y) \in R] \wedge [(y,z) \in A \times A \wedge (y,z) \in R] \\ &\quad\iff (x,z) \in A \times A \wedge (x,z) \in R \\ &\quad\iff (x,z) \in (A \times A) \cap R \iff (x,z) \in R|_A\end{aligned}$$

If R is transitive, then R^{-1} is transitive.

$$\begin{aligned}(x,y) \in R^{-1} \wedge (y,z) \in R^{-1} &\iff (y,x) \in R \wedge (z,y) \in R \\ &\iff (z,y) \in R \wedge (y,x) \in R \iff (z,x) \in R \iff (x,z) \in R^{-1}\end{aligned}$$

If R is transitive, then R^2 is transitive.

$$\begin{aligned}&(x,y) \in R^2 \wedge (y,z) \in R^2 \\ &\iff [\exists s \in X, (x,s) \in R \wedge (s,y) \in R] \wedge [\exists t \in X, (y,t) \in R \wedge (t,z) \in R] \\ &\iff \exists s,t \in X, (x,s) \in R \wedge (s,y) \in R \wedge (y,t) \in R \wedge (t,z) \in R \\ &\iff \exists s,t \in X, (x,s) \in R \wedge (s,t) \in R \wedge (t,z) \in R \\ &\iff (x,t) \in R \wedge (t,z) \in R \iff (x,z) \in R^2\end{aligned}$$

If R and S are transitive then the relation $R \cap S$ is transitive.

$$\begin{aligned}(x,y) \in R \cap S \wedge (y,z) \in R \cap S \\ &\iff (x,y) \in R \wedge (x,y) \in S \wedge (y,z) \in R \wedge (y,z) \in S \\ &\iff (x,z) \in R \wedge (x,z) \in S \iff (x,z) \in R \cap S\end{aligned}$$

If R and S are transitive then the relation $R \cup S$ is not necessarily transitive. To see this let $X = \{a,b,c\}$, $R = \{(a,b),(b,c),(a,c)\}$ and $S = \{(b,c),(c,d),(b,d)\}$. Then R and S are transitive, however, $R \cup S$ is not transitive since $(a,b),(b,d) \in R \cup S$ yet $(a,d) \notin R \cup S$. If R is transitive then R^c is not necessarily transitive. To see this let $X = \{a,b\}$ and $R = I$. The R is transitive and $R^c = \{(a,b),(b,a)\}$ which is not transitive.

□

Definition 7.2. If a relation is reflexive, symmetric, and transitive, then it is called an **equivalence relation**.

Theorem 7.5. *Let R and S be equivalence relations on X and let $A \subseteq X$. Then $R|_A$, R^{-1}, R^2, and $R \cap S$ are also equivalence relations.*

Proof. The proof is left as Exercise 7.1.

□

Theorem 7.6. *Let R and S be relations on X and let $A \subseteq X$.*

1. *If R and S are symmetric, then $S \circ R$ is symmetric if and only if $R \circ S \subseteq S \circ R$.*
2. *If R and S are transitive and $R \circ S \subseteq S \circ R$, then $S \circ R$ is transitive, but not conversely.*
3. *If R and S are equivalence relations, then $S \circ R$ is an equivalence relation if and only if $R \circ S \subseteq S \circ R$.*

Proof. The proof of each part follows.

1. If R and S are symmetric and $R \circ S \subseteq S \circ R$, then $S \circ R$ is symmetric.

$$\begin{aligned}
(x, y) \in S \circ R &\iff \exists z \in X, (x, z) \in R \wedge (z, y) \in S \\
&\iff \exists z \in X, (z, x) \in R \wedge (y, z) \in S \\
&\iff \exists z \in X, (y, z) \in S \wedge (z, x) \in R \iff (y, x) \in R \circ S \\
&\iff (y, x) \in S \circ R
\end{aligned}$$

Conversely, assume R, S, and $S \circ R$ are symmetric, then $S \circ R = R \circ S$.

$$\begin{aligned}
(x, y) \in S \circ R &\iff (y, x) \in S \circ R \\
&\iff \exists z \in X, (y, z) \in R \wedge (z, x) \in S \\
&\iff \exists z \in X, (z, y) \in R \wedge (x, z) \in S \\
&\iff \exists z \in X, (x, z) \in S \wedge (z, y) \in R \iff (x, y) \in R \circ S
\end{aligned}$$

2. If R and S are transitive and $R \circ S \subseteq S \circ R$, then $S \circ R$ is transitive.

$$\begin{aligned}
&(x, y) \in S \circ R \wedge (y, z) \in S \circ R \\
&\iff [\exists s \in X, (x, s) \in R \wedge (s, y) \in S] \wedge [\exists t \in X, (y, t) \in R \wedge (t, z) \in S] \\
&\iff \exists s, t \in X, (x, s) \in R \wedge (s, y) \in S \wedge (y, t) \in R \wedge (t, z) \in S \\
&\iff \exists s, t, \in X, (x, s) \in R \wedge (s, t) \in R \circ S \wedge (t, z) \in S \\
&\iff \exists s, t \in X, (x, s) \in R \wedge (s, t) \in S \circ R \wedge (t, z) \in S \\
&\iff \exists s, t, w \in X, (x, s) \in R \wedge (s, w) \in R \wedge (w, t) \in S \wedge (t, z) \in S \\
&\iff \exists w \in X, (x, w) \in R \wedge (w, z) \in S \iff (x, z) \in S \circ R
\end{aligned}$$

Let $X = \{a, b, c\}$, $R = \{(a, a), (a, b)\}$, and $S = \{(b, b), (b, c)\}$. Then R and S are transitive and so is $S \circ R = \{(a, b), (a, c)\}$. However, $R \circ S = \emptyset$.

3. If R, S, and $S \circ R$ are equivalence relations on X, then $R \circ S \subseteq S \circ R$.

$$\begin{aligned}
&S \circ R \text{ is an equivalence relation} \\
&\quad \iff S \circ R \text{ is reflexive, symmetric, and transitive} \\
&\quad \implies S \circ R \text{ is symmetric } \iff R \circ S \subseteq S \circ R
\end{aligned}$$

Conversely, if R and S are equivalence relations and $R \circ S \subseteq S \circ R$, then

$S \circ R$ is an equivalence relation.

$$\begin{aligned} R \circ S \subseteq S \circ R \wedge S, R &\text{ are equivalence relations} \\ &\implies S \circ R \text{ is reflexive, symmetric, and transitive} \\ &\iff S \circ R \text{ is an equivalence relation} \end{aligned}$$

which completes the proof.

□

A beautiful concise characterization of equivalence relation is here in the next theorem.

::: {#thm-understanding-of-equivalence relation } Let R be a relation on X. Then R is an equivalence relation if and only if

$$R = I \cup R^{-1} \cup R^2.$$

:::

Proof. Let R be a relation on X. If R is reflexive, symmetric, and transitive it follows $I \subseteq R$, $R^{-1} = R$, and $R^2 = R$; and thus $I \cup R^{-1} \cup R^2 = R$. Conversely, assume R be a relation on X. If $I \cup R^{-1} \cup R^2 = R$, then $I \subseteq R$, $R^{-1} \subseteq R$, and $R^2 \subseteq R$; and therefore R is an equivalence relation.

□

Another characterization of equivalence relation is here in the next theorem.

Theorem 7.7. *Let $\sim$ be a relation on X. Then $\sim$ is an equivalence relation if and only if the following property holds:*

$$\forall\, a, b \in X, a \sim b \Leftrightarrow \forall\, c \in X, a \sim c \Leftrightarrow b \sim c. \tag{7.1}$$

Proof. Assume $\sim$ is an equivalence relation on X. Assume $a \sim b$ for arbitrary $a, b \in X$. Let $c \in X$. By symmetry and transitivity it follows that

$$a \sim c \implies c \sim a \implies c \sim b \implies b \sim c$$

and conversely, $b \sim c \implies a \sim c$ follows by transitivity. Therefore, by symmetry and transitivity we have

$$\forall a, b \in X, a \sim b \implies \forall c \in X, a \sim c \Leftrightarrow b \sim c.$$

Assume for all $c \in X$ that $a \sim c \Leftrightarrow b \sim c$. Let $c = a$. Then we have $a \sim a \Leftrightarrow b \sim a$. Since $\sim$ is reflexive, $a \sim b$ must hold. Whence,

$$\forall c \in X, (a \sim c \Leftrightarrow b \sim c) \implies a \sim b$$

as desired.

Conversely, assume the given property holds. To show reflexivity, let $a \in X$. Since, $a \sim a$ if and only if $a \sim a$, obviously holds, it follows $a \sim a$ is valid. To prove the symmetric property holds, assume $a \sim b$. Therefore the following holds, $\forall c \in X, a \sim c \Leftrightarrow b \sim c$. Equivalently, the following holds $\forall c \in X, b \sim c \Leftrightarrow a \sim c$. Thus is it obvious that, $a \sim b \implies b \sim a$ holds; and therefore $\sim$ is also symmetric. To show transitivity, let $a, b, c \in X$ and assume $a \sim b$ and $b \sim c$. Therefore the following holds,

$$[\forall c \in X, a \sim c \Leftrightarrow b \sim c] \wedge [\forall d \in X, b \sim d \Leftrightarrow c \sim d].$$

Let $e \in X$. Then the following holds,

$$a \sim e \Leftrightarrow b \sim e \Leftrightarrow c \sim e.$$

Therefore, $a \sim c$ and so $\sim$ is also transitive. In conclusion, $\sim$ is an equivalence relation.

□

Definition 7.3. If $\sim$ is an equivalence relation on X, then the set

$$[a] = \{b \in X : b \sim a\}$$

is called the **equivalence class** of a with respect to $\sim$.

Definition 7.4. A **partition** of X is a collection of pairwise disjoint nonempty sets whose union is X.

Theorem 7.8. *Let $\sim$ be a relation on X. Then $\sim$ is an equivalence relation on X if and only if the set*

$$P = \{\{b \in X : a \sim b\} : a \in X\}$$

is a partition of X with the property $\forall a, b \in X, a \sim b \Leftrightarrow \exists A \in P$ such that $a, b \in A$.

Proof. Assume $\sim$ is an equivalence relation on X. We will prove that P is a partition of X with the desired property by proving the following four statements hold.

Claim 1: X is the union of all equivalence classes of $\sim$.

Proof: Since $\sim$ is reflexive it follows that

$$x \in \bigcup_{a \in X} [a] \Leftrightarrow \exists a \in X, x \in [a] \Leftrightarrow x \in X.$$

Claim 2: For all $a, b \in X$, $[a] \cap [b] \neq \emptyset \Leftrightarrow [a] = [b]$.

Proof: Assume $[a] \cap [b] \neq \emptyset$. Since $\sim$ is symmetric and transitive, it follows

$$\begin{aligned} x \in [a] \Leftrightarrow x \sim a &\Leftrightarrow x \sim a \wedge \exists y \in [a] \cap [b] \\ &\Leftrightarrow \exists y \in X, x \sim a \wedge y \sim a \wedge y \sim b \\ &\Leftrightarrow \exists y \in X, x \sim a \wedge a \sim y \wedge y \sim b \\ &\Leftrightarrow \exists y \in X, x \sim y \wedge y \sim b \Leftrightarrow x \sim b \Leftrightarrow x \in [b] \end{aligned}$$

Assume $[a] = [b]$. Since $\sim$ is reflexive

$$a \in [a] \implies a \in [a] \wedge a \in [b] \implies a \in [a] \cap [b] \implies [a] \cap [b] \neq \emptyset$$

Claim 3: Every equivalence class of $\sim$ is nonempty.

Proof: Since $\sim$ is reflexive, it follows that

$$a \in X \implies a \sim a \implies a \in [a] \implies [a] \neq \emptyset.$$

Claim 4: For all $a, b \in X$, $a \sim b \Leftrightarrow [a] = [b]$.

Proof: Let $a, b \in X$ and assume $a \sim b$. Then it follows that

$$x \in [a] \Leftrightarrow x \sim a \Leftrightarrow x \sim b \Leftrightarrow x \in [b].$$

Thus we have that $[a] = [b]$. Conversely, assume $[a] = [b]$ for all a, b in X. Then it follows that

$$a \in [a] \implies a \in [b] \implies a \sim b.$$

and so $a \sim b$ holds. Therefore we have shown that P, the collection of equivalence class of $\sim$, is a partition on X with the desired property.

Conversely, assume $\sim$ is a relation on X and P is a partition of X with the stated property. First we notice $\sim$ is reflexive since

$$a \in X \implies a \in \bigcup_{A \in P} A \implies \exists A \in P, a \in A \implies a \sim a.$$

The symmetric property of $\sim$ follows by

$$a \sim b \implies \exists A \in P, a \in A \wedge b \in A \implies b \sim a.$$

We also notice $\sim$ is transitive by the following

$$a \sim b \wedge b \sim c \Leftrightarrow \exists a, b \in P, a, b \in A \wedge b, c \in B \Longrightarrow A = B \Leftrightarrow a \sim c.$$

In conclusion $\sim$ is an equivalence relation where $a \sim b$ is equivalent to the existence of a set $A \in P$ with $a, b \in A$, namely the equivalence class $A = [a]$.

□

7.3 Exercise

Exercise 7.1. Prove Theorem 7.5.

7.4 Reflexive Closure

Theorem 7.9. *Let R be relation on X and $A \subseteq X$. The reflexive closure of R is the relation*

$$r(R) = R \cup I.$$

Proof. Let R b a relation, then $r(R) = R \cup I$. Notice $R \cup I$ is reflexive since

$$x \in X \implies (x, x) \in I \implies (x, x) \in R \cup I.$$

Let T be a reflexive relation containing R. Then $R \cup I \subseteq T$ since

$$\begin{aligned}(x, y) \in R \cup I &\implies (x, y) \in R \vee (x, y) \in I \\ &\implies (x, y) \in T \vee (x, y) \in I \implies (x, y) \in T \cup I = T\end{aligned}$$

Since $R \subseteq R \cup I \subseteq T$ where T is an arbitrary reflexive relation containing R, it follows $r(R) = R \cup I$.

□

7.5 Symmetric Closure

Theorem 7.10. *Let R be relation on X and $A \subseteq X$. The symmetric closure of R is the relation*

$$s(R) = R \cup R^{-1}.$$

Proof. Let R b a relation, then $s(R) = R \cup R^{-1}$. Notice $R \cup R^{-1}$ is symmetric since

$$\begin{aligned}(x, y) \in R \cup R^{-1} &\implies (x, y) \in R \vee (x, y) \in R^{-1} \\ &\implies (y, x) \in R^{-1} \vee (y, x) \in R \implies (y, x) \in R^{-1} \cup R = R \cup R^{-1}\end{aligned}$$

Let T be a symmetric relation containing R. Then $R \cup R^{-1} \subseteq T$ since

$$\begin{aligned} (x,y) \in R \cup R^{-1} &\implies (x,y) \in R \vee (x,y) \in R^{-1} \\ &\implies (x,y) \in T \vee (x,y) \in R^{-1} \implies (x,y) \in T \vee (y,x) \in T \\ &\implies (x,y) \in T \vee (x,y) \in T \implies (x,y) \in T \end{aligned}$$

Since $R \subseteq R \cup R^{-1} \subseteq T$ where T is an arbitrary symmetric relation containing R, it follows $s(R) = R \cup R^{-1}$.

□

7.6 Reflexive Transitive

Theorem 7.11. *Let R be relation on X and $A \subseteq X$. The transitive closure of R and the reflexive transitive closure of R are*

$$t(R) = \bigcup_{n\geq 1} R^n. \qquad rt(R) = \bigcup_{n\geq 0} R^n.$$

respectively.

Proof. For $i > 0$ define

$$R^i = R^{i-1} \cup \{(a,b) : \exists c \in X, (a,c) \in R^{i-1} \wedge (c,b) \in R^{i-1}\}$$

The transitive closure of R, denoted by $t(R)$, is the relation $t(R) = \cup_{n\geq 1} R^n$. First notice $t(R)$ contains all powers of R and so in particular $t(R)$ contains R. Next notice that $t(R)$ is transitive since

$$\begin{aligned} (a,b) \in t(R) \wedge (b,c) \in t(R) &\implies \exists R^n, R^m, (a,b) \in R^n \wedge (b,c) \in R^m \\ &\implies (a,c) \in R^m \circ R^n \subseteq t(R) \end{aligned}$$

Let T be a transitive relation containing R. By induction it follows $R^k \subseteq T$ for all k. This is true for $k = 1$ since T contains R. Then

$$R^k \subseteq T \implies R^{k+1} = R^k \circ R \subseteq T \circ R \subseteq T \circ T = T$$

demonstrates the claim. Whence, $t(R) = \bigcup_{n\geq 1} R^n \subseteq T$ as desired.

Define $R^0 = I$, then

$$rt(R) = r\left(\bigcup_{n\geq 1} R^n\right) = \bigcup_{n\geq 1} R^n \cup I = \bigcup_{n\geq 1} R^n \cup R^0 = \bigcup_{n\geq 0} R^n.$$

which completes the proof.

□

7.7 Transitive Closure

Theorem 7.12. *Let R be a relation on X. Then R is transitive if and only if $R^n \subseteq R$, for $n \geq 1$.*

Proof. Assume R is transitive. We will prove $R^n \subseteq R$ for $n \geq 1$ by induction. The basis step is obvious. The induction step is:

$$R^n \subseteq R \implies R^{n+1} \subseteq R$$

Assume $R^n \subseteq R$ for some $n \geq 1$. Then

$$\begin{aligned}(x,y) \in R^{n+1} &\Leftrightarrow \exists z \in X, (x,z) \in R \wedge (z,y) \in R^n \\ &\Leftrightarrow \exists z \in X, (x,z) \in R \wedge (z,y) \in R \implies (x,z) \in R\end{aligned}$$

Therefore, by induction $R^n \subseteq R$, for all ≥ 1. Conversely, assume $R^n \subseteq R$, for all $n \geq 1$. Then $(x,y) \in R \wedge (y,z) \in R \implies (x,z) \in R^2 \implies (x,y) \in R$. Thus, R is transitive.

□

Theorem 7.13. *Let R be a relation on X. If R is reflexive, then $s(R)$ and $t(R)$ are reflexive.*

Proof. If R is reflexive, then $s(R)$ and $t(R)$ are reflexive, then

$$I \subseteq R \subseteq s(R) \text{ and } I \subseteq R \subseteq t(R)$$

as desired.

□

Theorem 7.14. *Let R be a relation on X. If R is symmetric, then $r(R)$ and $t(R)$ are symmetric.*

Proof. If R is symmetric, then $r(R)$ and $t(R)$ are symmetric.

$$\begin{aligned}(x,y) \in r(R) = R \cup I &\implies (x,y) \in R \vee (x,y) \in I \\ &\implies (y,x) \in R \vee (y,x) \in I \implies (y,x) \in R \cup I = r(R) \\ (x,y) \in t(R) = \bigcup_{n\geq 1} R^n &\implies \exists R^n, (x,y) \in R^n \\ &\implies \exists R^n, (y,x) \in R^n \implies (y,x) \in \bigcup_{n \geq 1} R^n = t(R)\end{aligned}$$

which completes the proof.

□

Theorem 7.15. *Let R be a relation on X. If R is transitive, then $r(R)$ is transitive; however, $s(R)$ may not be transitive.*

Proof. If R is transitive, then $r(R)$ is transitive.

$$\begin{aligned}(x,y) \in r(R) \land (y,z) \in r(R) &\implies (x,y) \in R \cup I \land (y,z) \in R \cup I \\ &\implies ((x,y) \in R \lor (x,y) \in I) \land ((y,z) \in R \lor (y,z) \in I) \\ &\implies (x,z) \in R \lor (x,z) \in I \implies (x,z) \in R \cup I = r(R)\end{aligned}$$

Let $X = \{a,b\}$ and $R = \{(a,b)\}$. Then R is transitive and $s(R) = \{(a,b),(b,a)\}$ is not transitive. Therefore, the symmetric closure of a transitive relation may not be transitive.

□

Theorem 7.16. *Let R be a relation on X. The following hold: $rt(R) = tr(R)$, $rs(R) = sr(R)$, $st(R) \subseteq ts(R)$, and $st(R) \subsetneq ts(R)$ can hold.*

Proof. The proof of each part follows.

- $rt(R) = tr(R)$:

$$tr(R) = t(R \cup I) = \bigcup_{n \geq 1} (R \cup I)^n = \left(\bigcup_{n \geq 1} R^n \right) \cup I = \bigcup_{n \geq 0} R^n = rt(R)$$

- $rs(R) = sr(R)$:

$$\begin{aligned}&rs(R) = r(R \cup R^{-1}) = I \cup R \cup R^{-1} \\ &= r(R) \cup R^{-1} = r(R) \cup (R^{-1} \cup I) = r(R) \cup r(R)^{-1} = sr(R)\end{aligned}$$

- $st(R) \subseteq ts(R)$:

Let $A = \{a,b,c\}$. Then $st(R) = \{(a,b),(b,a),(b,c),(c,b),(a,c),(c,a)\}$ and $ts(R) = A \times A$ which completes the proof.

□

7.8 Equivalence Relation Characterization

Theorem 7.17. *Let R be a relation on a set X. Then R is an equivalence relation if and only if $R = rts(R)$.*

Proof. Assume R is an equivalence relation on X. Notice $R \subseteq rts(R)$, where r, s, and t denote the reflexive, symmetric and transitive closure operators, respectively. Let T be an arbitrary equivalence relation on X containing R. Since $R \subseteq T$ and T is symmetric, if follows that $s(R) \subseteq T$. Then $ts(R) \subseteq t(T) = T$ and so $rts(R) \subseteq r(T) = T$. Thus it follows $rts(R)$ is contained in T. Since R is an equivalence relation on X containing R, it follows that $rts(R) \subseteq R$. Whence, $R = rts(R)$.

Conversely, assume R is a relation on X such that $R = rts(R)$. It is easy to check that $ts(R)$ is symmetric and that $rts(R)$ is symmetric and transitive. It follows that $rts(R)$ is an equivalence relation. Thus R is an equivalence relation.

□

Theorem 7.18. *Let $\longrightarrow$ be a relation on X with transitive closure denoted by $\overset{+}{\longrightarrow}$. Then $a \overset{+}{\longrightarrow} b$ if and only if there exists elements $a = x_1, x_2, x_3, ..., x_n = b$ in X such that $x_1 \longrightarrow x_2 \longrightarrow \cdots \longrightarrow x_n$.*

Proof. The proof is left for the reader.

□

7.9 The Kernel and Image of a Function

Theorem 7.19. *Let $f : X \to X$ be a function and let $\sim$ be the binary relation defined on X by $a \sim b$ if and only if $f(a) = f(b)$. Then $\sim$ is an equivalence relation.*

Proof. Since $f(a) = f(a)$ holds for all $a \in X$, it follows $\sim$ is reflexive. Let $a, b \in X$ and assume $a \sim b$. Then $f(b) = f(a)$, and thus $f(b) = f(a)$ also holds. Thus, $b \sim a$ and so $\sim$ is also symmetric. Let $a, b, c \in X$ and assume $a \sim b$ and $b \sim c$. Then $f(a) = f(b)$ and $f(b) = f(c)$. Thus $f(a) = f(c)$ and so $a \sim c$, which means $\sim$ is also transitive; and in conclusion an equivalence relation on X.

□

Recall, if R is a binary relation on X, then $R(x) = \{y \in X : (x, y) \in R\}$, that is $R(x)$ is the set of outputs of R for a given input x. Of course when R is a function $R(x)$ is a singleton set for each $x \in X$. In general $R(x)$ can have many elements.

Theorem 7.20. *Let R be a binary relation on X and let* $\ker(R)$ *be the relation defined on X by $(a, b) \in \ker(R)$ if and only if $R(a) = R(b)$. Then* $\ker(R)$ *is an equivalence relation.*

Proof. Since $R(a) = R(a)$ holds for all $a \in X$, it follows $\ker(R)$ is reflexive. Let $a, b \in X$ and assume $(a, b) \in \ker(R)$. Then $R(b) = R(a)$, and thus $R(b) = R(a)$ also holds. Thus, $(b, a) \in \ker(R)$ and so $\ker(R)$ is also symmetric. Let $a, b, c \in X$ and assume (a, b) and $(b, c) \in \ker(R)$. Then $R(a) = R(b)$ and $R(b) = R(c)$. Thus $R(a) = R(c)$ and so $(a, c) \in \ker(R)$, which means $\ker(R)$ is also transitive; and in conclusion an equivalence relation on X.

□

Recall, if R is a binary relation on X, then $R^{-1}(y) = \{x \in X : (x, y) \in R\}$, that is $R^{-1}(y)$ is the set of inputs of R for a given output y. In general $R(y)$ can have many elements.

Theorem 7.21. *Let R be a binary relation on X and let* $\operatorname{im}(R)$ *be the relation defined on X by $(a, b) \in \operatorname{im}(R)$ if and only if $R^{-1}(a) = R^{-1}(b)$. Then* $\operatorname{im}(R)$ *is an equivalence relation.*

Proof. Since $R^{-1}(a) = R^{-1}(a)$ holds for all $a \in X$, it follows $\operatorname{im}(R)$ is reflexive. Let $a, b \in X$ and assume $(a, b) \in \operatorname{im}(R)$. Then $R^{-1}(b) = R^{-1}(a)$, and thus $R^{-1}(b) = R^{-1}(a)$ also holds. Thus, $(b, a) \in \operatorname{im}(R)$ and so $\operatorname{im}(R)$ is also symmetric. Let $a, b, c \in X$ and assume $(a, b) \in \operatorname{im}(R)$ and $(b, c) \in \operatorname{im}(R)$. Then $R^{-1}(a) = R^{-1}(b)$ and $R^{-1}(b) = R^{-1}(c)$. Thus $R^{-1}(a) = R^{-1}(c)$ and so $(a, c) \in \operatorname{im}(R)$, which means $\operatorname{im}(R)$ is also transitive; and in conclusion an equivalence relation on X.

□

Theorem 7.22. *Let R be a binary relation on X. Then R is an equivalence relation if and only if* $\ker(R) = R$ *if and only if* $\operatorname{im}(R) = R$ *if and only if $R = R^*$.*

Proof. The proof is left as an exercise.

□

7.10 Exercises

7.11 Up-sets and Down-sets

Throughout we assume $(X, \geq)$ is an ordered set. By this we mean that X is a set and that $\geq$ is binary relation on X that is reflexive, antisymmetric, and transitive.

Definition 7.5. A subset U of X is called an **up-set** if

$$(x \in U,\ y \in X,\ \text{and } y \geq x) \implies y \in U.$$

A subset D of X is called a **down-set** if

$$(x \in D,\ y \in X,\ \text{and } x \geq y) \implies y \in D.$$

Theorem 7.23. *Let $(X, \geq)$ be an ordered set.*

1. *The union or intersection of any family of up-sets is an up-set.*
2. *The complement of an up-set is a down-set.*

Proof. (1): Let $\{U_i : i \in I\}$ be a family of up-sets. Let

$$U = \bigcup_{i \in I} U_i \quad \text{and} \quad F = \bigcap_{i \in I} U_i.$$

We will show that U is an up-set. Let $x \in U$, $y \in X$ and assume $y \geq x$. Since $x \in U$, it follows $x \in U_i$ for some i. Since U_i is an up-set, it follows $y \in U_i$. Hence $y \in U$. Next we will show F is an up-set. Let $x \in F$ and $y \in X$ and assume $y \geq x$. Since $x \in F$, it follows $x \in U_i$ for all $i \in I$. Since U_i are all up-sets, it follows $y \in U_i$ for all $i \in I$. Hence $y \in F$.

(2): Let U be an up-set and let D be the complement of U. Let $x \in D$, $y \in X$, and assume $x \geq y$. Assume $y \in U$. Since U is an up-set and $x \geq y$, if follows $x \in U$. However, $x \in U$ and $x \in D$ is a contradiction. Thus, $y \in D$ as needed.

□

Theorem 7.24. *The union or intersection of any family of down-sets is a down-set. The complement of a down-set is an up-set.*

Definition 7.6. If A is an arbitrary subset of X and $x \in X$, then we define

$$\uparrow(A) = \{y \in X : \exists\, x \in A,\, y \geq x\} \quad \text{and} \quad \uparrow(x) = \{y \in X : y \geq x\}.$$

$$\downarrow(A) = \{y \in X : \exists\, x \in A,\, x \geq y\} \quad \text{and} \quad \downarrow(x) = \{y \in X : x \geq y\},$$

to be the **up-closure of** A, **up-closure of** x, **down-closure of** A, and the **down-closure of** x, respectively. Up-sets of the form $\uparrow(x)$ are called **principal up-sets** and dually, down-sets of the form $\downarrow(x)$ are called **principal down-sets**.

Important special cases are $\uparrow(X) = X$, $\downarrow(X) = X$, $\downarrow\emptyset = \emptyset$ and $\uparrow\emptyset = \emptyset$. Clearly,

$$\forall\ x, y \in X, \quad x \geq y \iff \uparrow(x) \subseteq \uparrow y \iff \downarrow(x) \supseteq \downarrow y. \tag{7.2}$$

To see this, suppose $x \geq y$, and assume $z \in \uparrow(x)$ and $w \in \downarrow y$. Then by transitivity of $\geq$ we have $z \in \uparrow y$ and $w \in \downarrow(x)$. Conversely, both $\uparrow(x) \subseteq \uparrow y$ and $\downarrow(x) \supseteq \downarrow y$ imply that $x \geq y$ which follows by the reflexive property.

Theorem 7.25. *Assume $A \subseteq X$ and $x \in X$. Then*

1. *$\downarrow(A)$ is the smallest down-set containing A,*
2. *A is an down-set if and only if $A = \downarrow(A)$, and*
3. *$\downarrow(x) = \downarrow(x)$.*

Proof. (1): Let $x \in \downarrow(A)$, $y \in X$. Assume $x \geq y$. Since $x \in \downarrow(A)$, there exists $z \in A$ such that $z \geq x$. By transitivity $z \geq y$. Thus it follows $y \in \downarrow(A)$. Therefore, $\downarrow(A)$ is an down-set. Let D be an down-set that contains A. We will show $\downarrow(A) \subseteq D$. Let $x \in \downarrow(A)$. Then there exists $z \in A$ such that $z \geq x$. Since $z \in A$, it follows $z \in D$. Since D is an down-set, it follows that $x \in D$, as a needed.

(2): Suppose $A = \downarrow(A)$, then by part (**??**), it follows A is an down-set. Conversely, assume A is an down-set. By (**??**), $\downarrow(A)$ is the smallest down-set that contains A, so it follows $\downarrow(A) \subseteq A$ since A is an down-set and $A \subseteq A$. Let $x \in A$. By the reflexive property of $\geq$, it follows $x \geq x$, and thus $x \in \downarrow(A)$. Hence $\downarrow(A) = A$.

(3): Immediately, $y \in \downarrow(x) \iff x \geq y \iff y \in \downarrow(x)$.

□

Theorem 7.26. *Let $(X, \geq)$ be an ordered set with $A \subseteq X$ and $x \in X$.*

1. *$\uparrow(A)$ is the smallest up-set containing A.*
2. *A is an up-set if and only if $A = \uparrow(A)$.*
3. *$\uparrow(x) = \uparrow(x)$.*

Proof. (1): Let $x \in \uparrow(A)$, $y \in X$. Assume $y \geq x$. Since $x \in \uparrow(A)$, there exists $z \in A$ such that $x \geq z$. By transitivity $y \geq z$. Thus it follows $y \in \uparrow(A)$. Therefore, $\uparrow(A)$ is an up-set. Let U be an up-set that contains A. We will show $\uparrow(A) \subseteq U$. Let $x \in \uparrow(A)$. Then there exists $z \in A$ such that $x \geq z$. Since $z \in A$, it follows $z \in U$. Since U is an up-set, it follows that $x \in U$, as a needed.

(2): Suppose $A = \uparrow(A)$, then by part (**??**), it follows A is an up-set. Conversely, assume A is an up-set. By (**??**), $\uparrow(A)$ is the smallest up-set that contains A, so it follows $\uparrow(A) \subseteq A$ since A is an up-set and $A \subseteq A$. Let $x \in A$. By the reflexive property of $\geq$, it follows $x \geq x$, and thus $x \in \uparrow(A)$. Hence $\downarrow(A) = A$.

(3): Immediately, $y \in \uparrow(x) \iff y \geq x \iff y \in \uparrow(x)$.

□

Theorem 7.27. *For all $x, y \in X$,*

$$x \geq y \iff \downarrow(x) \supseteq \downarrow y \iff \uparrow(x) \subseteq \uparrow y.$$

Proof. Suppose $x \geq y$. Let $z \in \downarrow y$ then $y \geq z$. By transitivity of $\geq$ we have $x \geq z$ and thus $z \in \downarrow(x)$. Therefore we have shown, if $x \geq y$ then $\downarrow(x) \supseteq \downarrow y$. Conversely, assume $\downarrow(x) \supseteq \downarrow y$. By reflexivity of $\geq$ we have $y \in \uparrow y$ and so $y \in \downarrow(x)$, and thus $x \geq y$. Now suppose $x \geq y$. Let $z \in \uparrow(x)$. Then $z \geq x$ and so by transitivity of $\geq$ we have $z \geq y$, and therefore $z \in \uparrow y$. Conversely, assume $\uparrow(x) \subseteq \uparrow y$. Then $x \in \uparrow y$ and thus $x \geq y$.

□

Theorem 7.28. *Let $(X, \geq)$ be an ordered set with $A, B \subseteq X$.*

1. $\uparrow(A) = \uparrow(\uparrow(A))$
2. $\uparrow(A \cup B) = \uparrow(A) \ \cup \uparrow(B)$
3. $\uparrow(A \cap B) \subseteq \uparrow(A) \ \cap \uparrow(B)$
4. $\uparrow(A) = \bigcup_{x \in A} \uparrow(x)$
5. $B \supseteq A \Rightarrow \uparrow(B) \supseteq \uparrow(A)$

Proof. (1): Immediately we have $\uparrow(A) \subseteq \uparrow(\uparrow(A))$. Let $x \in \downarrow(\downarrow(A))$. Then there exists $y \in \downarrow(A)$ such that $y \geq x$ and there exists $a \in A$ such that $a \geq y \geq x$. Hence $x \in \downarrow(A)$.

(2): Let $x \in \uparrow(A \cup B)$. Then there exists $y \in A \cup B$ such that $x \geq y$. If $y \in A$, then $x \in \uparrow(A)$. If $y \in B$, then $x \in \uparrow(B)$. Hence, $x \in \uparrow(A) \ \cup \uparrow(B)$. Conversely, assume $x \in \uparrow(A) \ \cup \uparrow(B)$. If $x \in \uparrow(A)$, then there exists $a \in A$ such that $x \geq a$. Hence $a \in A \cup B$ with $x \geq a$ which yields $x \in \uparrow(A \ \cup B)$. If $x \in \uparrow(B)$, then there exists $b \in B$ such that $x \geq b$. Hence $b \in A \cup B$ with $x \geq b$ which yields $x \in \uparrow(A \ \cup B)$.

(3): Let $x \in \uparrow(A \cap B)$. Then there exists $y \in A \cap B$ such that $x \geq y$. Hence $y \in A$ with $x \geq y$ and $y \in B$ with $x \geq y$. Thus $x \in \uparrow(A)$ and $x \in \uparrow(B)$, and so $x \in \uparrow(A) \ \cap \uparrow(B)$.

(4): Let $z \in \uparrow(A)$. Then there exists $a \in A$ such that $z \geq a$. Hence it follows that $z \in \uparrow(a) \subseteq \bigcup_{x \in A} \uparrow(x)$.Conversely, assume $z \in \bigcup_{x \in A} \uparrow(x)$. Then there exists $x \in A$ such that $z \in \uparrow(x)$. Hence we have $x \in A$ with $z \geq x$. Thus it follows that $z \in \uparrow(A)$ as needed.

□

Theorem 7.29. *Let $(X, \geq)$ be an ordered set with $A, B \subseteq X$.*

1. $\downarrow(A) = \downarrow(\downarrow(A))$
2. $\downarrow(A \cup B) = \downarrow(A) \ \cup \downarrow(B)$
3. $\downarrow(A \cap B) \subseteq \downarrow(A) \ \cap \downarrow(B)$
4. $\downarrow(A) = \bigcup_{x \in A} \downarrow(x)$
5. $B \supseteq A \Rightarrow \downarrow(B) \supseteq \downarrow(A)$

7.12 Monotone Mappings

Definition 7.7. Let $(X, \leq_1)$ and $(Y, \leq_2)$ be ordered sets. A mapping $f : X \to Y$ is said to be **isotone** (**order-preserving**) whenever

$$(\forall\, x, y \in X) \quad x \leq_1 y \implies f(x) \leq_2 f(y)$$

or is said to be **antitone** (**order-reversing**) whenever

$$(\forall\, x, y \in X) \quad x \leq_1 y \implies f(x) \geq_2 f(y).$$

Furthermore, f is called **monotone** if f is either isotone or antitone.

Theorem 7.30. *For every function f on an ordered set $(X, \geq)$, we denote it to be $\uparrow$, $\downarrow$, or $\updownarrow$ according to whether it is isotone, antitone, or both. The following are some easy consequences:*

1. $\uparrow \circ \downarrow = \downarrow \circ \uparrow = \downarrow$ *(meaning that the composition of an isotone and an antitone maps is antitone),*
2. $\uparrow \circ \uparrow = \downarrow \circ \downarrow = \uparrow$ *(meaning that the composition of two isotone or two antitone maps is isotone),*
3. *f is $\updownarrow$ if and only if it is a constant on any chain in A, and if this is the case, for every $a \in A$, $f^{-1}(a)$ is a maximal chain in A.*

Proof. An exercise for the reader as Exercise 7.2.

□

7.13 Exercises

Exercise 7.2. Prove Theorem 7.30.

Theorem 7.31. *A mapping $f : X \to Y$ is isotone if and only if the inverse image of every principal down-set of Y is a down-set of X.*

Proof. The proof follows as in MR2126425. First notice that

$$\forall y \in Y, \quad x \in f^{-1}(\downarrow(y)) \Longleftrightarrow y \geq f(x). \tag{7.3}$$

Suppose that f is isotone. Let $\downarrow(y)$ be an arbitrary principal down-set of Y and let $A = f^{-1}(\downarrow(y))$. Assume $x \in A$, $z \in X$, and $x \geq z$. Since f is isotone, we have $f(x) \geq f(z)$.
Since $x \in A$ it follows by (7.3) that $y \geq f(x)$; and so we have $y \geq f(z)$ by transitivity of $\geq$. Thus $z \in A$ as needed. For conversely, notice that by reflexivity of $\geq$ and (7.3) it follows that for every $x \in X$ we have $x \in f^{-1}(\downarrow(f(x)))$. By hypothesis, $f^{-1}(\downarrow(f(x)))$ is a down-set of X; so if $y \in X$ is such that $x \geq y$ we have $y \in f^{-1}(\downarrow(f(x)))$. By (7.3), it follows that $f(x) \geq f(y)$ and therefore f is isotone.

□

Theorem 7.32. *If X, Y are ordered sets and if $f : X \to Y$ is any mapping then the following statements are equivalent.*

1. *f is isotone;*

2. the inverse image of every principal down-set of Y is a down-set of X;

3. the inverse image of every principal up-set of Y is an up-set of X.

Proof. (1)⇔(2): Suppose that f is isotone. Let $y \in Y$ and let $A = f^{\leftarrow}(y^{\downarrow})$. If $A \neq \emptyset$ assume $x \in A$. Then for every $z \in X$ with $z \leq x$ we have $f(z) \leq f(x) \leq y$ whence $z \in A$. Thus A is a down-set of X. Conversely, notice that for every $x \in X$ we have $x \in f^{\leftarrow}[f(x)^{\downarrow}]$. By (2) this is a down-set of X; so if $y \in X$ is such that $y \leq x$ we have $y \in f^{\leftarrow}[f(x)^{\downarrow}]$. If follows that $f(y) \leq f(x)$ and therefore f is isotone.

(1)⇔(2): Assume f is order preserving. Let $y \in Y$ and let $A = f^{\leftarrow}(y^{\uparrow})$ be the inverse image of a principal down-set of Y. To show A is an up-set of X, assume $x \in A$. If $z \in X$ with $z \geq x$ we have $f(z) \geq f(x) \geq y$ whence $z \in A$ as needed. Conversely assume $x \leq y$ and that (**??**) holds. Notice $x \in f^{\leftarrow}(f(x)^{\uparrow})$ holds for all $x \in X$. By assumption, $f^{\leftarrow}(f(x)^{\uparrow})$ is an up-set of X, and so it follows $y \in f^{\leftarrow}(f(x)^{\uparrow})$. Whence $f(y) \geq f(x)$ as needed.

□

Theorem 7.33. *A mapping $f : X \to Y$ is an order-isomorphism if and only if f is bijective and both f and f^{-1} are isotone.*

Proof. The proof follows as in davey2002introduction. Assume $f : X \to Y$ is a order-isomorphism. By definition f is surjective. Using the reflexive and antisymmetric properties we have

$$\begin{aligned} f(x) = f(y) &\Longleftrightarrow f(x) \geq f(y) \text{ and } f(y) \geq f(x) \\ &\Longleftrightarrow x \geq y \text{ and } y \geq x \\ &\Longleftrightarrow x = y \end{aligned}$$

Thus f is injective and so bijective. Since

$$\forall x, y \in X, \quad x = f^{-1}(f(x)) = f^{-1}(f(y)) = y \Longleftrightarrow f(x) \geq_2 f(y)$$

it follows both f and f^{-1} are isotone. Conversely, assume f is bijective and both f and f^{-1} are isotone. Obviously, f is surjective. Let $x, y \in X$. Assume $x \geq y$. Then $f(x) \geq f(y)$ since f is isotone. Now assume $f(x) \geq f(y)$. Since f^{-1} is isotone and f^{-1} is the inverse of f, we have $x = f^{-1}(f(x)) \geq y = f^{-1}(f(y))$ as needed to establish (**??**).

□

Theorem 7.34. *The mapping $\phi : X \to \mathcal{X}$ defined by*

$$\phi(x) = \downarrow(x).$$

is an order-isomorphism onto the set of all principal down-sets of X.

Proof. First notice that ϕ is a bijection to the principal down-sets:

$$\phi(x) = \phi(y) \iff \downarrow(x) = \downarrow(y) \iff y \geq x \text{ and } x \geq y \iff x = y.$$

To show that ϕ is a order-isomorphism, observe (**??**) yields $x \geq y$ if and only if $\phi(y) \subseteq \phi(x)$, and the claim follows.

□

7.14 Residuated Mappings

Let $(X, \geq)$ and $(Y, \succeq)$ be ordered sets.

Definition 7.8. A mapping $f : X \to Y$ is called *residuated* if the inverse image of every principal down-set of Y is a principal down-set of X.

Theorem 7.35. *A mapping $f : X \to Y$ is residuated if and only if it is isotone and there exists a isotone mapping $g : Y \to X$ such that*

$$\forall\, x \in X, (g \circ f)(x) \geq x \quad \textit{and} \quad \forall y \in Y, y \succeq (f \circ g)(y). \tag{7.4}$$

Proof. The proof follows as in page 6 MR2126425. Assume f is residuated. It follows that f is isotone. Notice the definition of residuated means: for all $y \in Y$ there exists $x \in X$ such that $f^{-1}(\downarrow(y)) = \downarrow(x)$. Now for every given $y \in Y$ this element x is clearly unique [if $f^{-1}(\downarrow(y)) = \downarrow(x)$ and $f^{-1}(\downarrow(y)) = \downarrow(z)$, then $z \geq x$ and $x \geq z$], so we can define a mapping $g : Y \to X$ by setting $g(y) = x$. It follows that g is isotone:

$$\begin{aligned} y_1 \succeq y_2 &\implies \downarrow(y_2) \subseteq \downarrow(y_1) \implies f^{-1}(\downarrow(y_2)) \subseteq f^{-1}(\downarrow(y_1)) \\ &\implies \downarrow(x_2) \subseteq \downarrow(x_1) \implies \downarrow(g(y_2)) \subseteq \downarrow(g(y_1)) \implies g(y_1) \geq g(y_2). \end{aligned}$$

Further it follows $g(y) \in \downarrow(g(y)) = \downarrow(x) = f^{-1}(\downarrow(y))$, and so $y \succeq (f \circ g)(y)$, for all $y \in Y$; and $x \in f^{-1}(\downarrow(f(x))) = \downarrow(g(f(x)))$ so that $(g \circ f)(x) \geq x$, for all $x \in X$. Conversely, assume f and g are isotone mappings such that (7.4) holds. Then on the one hand we have

$$y \succeq f(x) \implies g(y) \geq g(f(x)) \geq x$$

and on the other hand we have

$$g(y) \geq x \implies y \succeq f(g(y)) \succeq f(x).$$

It follows from these observations that $y \succeq f(x)$ if and only if $g(y) \geq x$. Therefore we have $f^{-1}(\downarrow(y)) = \downarrow(g(y))$. Whence f is residuated.

□

Theorem 7.36. *If $f : X \to Y$ is a residuated, then an isotone mapping that satisfies* (7.4) *is unique, and is called the* residual *of f and is denoted by f^+.*

Proof. Suppose that $g, h : Y \to X$ are each isotone mappings that satisfy (7.4). Then

$$\forall y \in Y, \quad h(y) \geq h((f \circ g)(y)) = (h \circ f)(g(y)) \geq g(y)$$

Similarly it follows $g(y) \geq h(y)$ and therefore $g = h$.

□

For every non-empty set X the residuated mappings on $\mathcal{X}$ are completely described in the following result.

Theorem 7.37. *Let X be a non-empty set and let R be a binary relation on X. Then the mapping $\zeta_R : \mathcal{X} \to \mathcal{X}$ defined by*

$$\zeta_R(A) = \{y \in X : (\exists\, x \in A)\ (x, y) \in R\}$$

is residuated. Moreover, every residuated mapping $f : \mathcal{X} \to \mathcal{X}$ is of this form for some binary relation R on X.

Proof. The proof follows as in p. 8 MR2126425.

Let $\iota : \mathcal{X} \to \mathcal{X}$ be the antitone mapping that sends each subset of X to its complement and let $\zeta_{R^{-1}} : \mathcal{X} \to \mathcal{X}$ be defined by

$$\zeta_{R^{-1}}(A) = \{y \in X : (\exists\, x \in A)\ (x, y) \in R^{-1}\}.$$

The mapping $\zeta_R^+ : \mathcal{X} \to \mathcal{X}$ defined by $\zeta_R^+ = \iota \circ \zeta_{R^{-1}} \circ \iota$ is isotone. To see this, let $A, B \in \mathcal{X}$. Then it follows that

$$\begin{aligned} A \subseteq B &\implies \iota(A) \supseteq \iota(B) \implies \zeta_{R^{-1}}(\iota(A)) \supseteq \zeta_{R^{-1}}(\iota(B)) \\ &\implies (\iota \circ \zeta_{R^{-1}})(\iota(A)) \subseteq (\iota \circ \zeta_{R^{-1}})(\iota(B)) \implies \zeta_R^+(A) \subseteq \zeta_R^+(B). \end{aligned}$$

We claim that $(\zeta_R^+ \circ \zeta_R)(A) \supseteq A$, for all $A \in \mathcal{X}$. It suffices to show $(\zeta_{R^{-1}} \circ \iota \circ \zeta_R)(A) \subseteq \iota(A)$ because then we have $(\zeta_R^+ \circ \zeta_R)(A) = (\iota \circ \zeta_{R^{-1}})(A) \supseteq A$ as required. To this end notice that

$$y \in (\zeta_{R^{-1}} \circ \iota \circ \zeta_R)(A) \implies \exists z \in (\iota \circ \zeta_R)(A), (y, z) \in R$$

Assume $y \in A$. Then $y \in A$ and $(y, z) \in R$ which yields $z \in \zeta_R(A)$. However, $z \notin \zeta_R(A)$. Hence $y \notin A$ and so $y \in \iota(A)$ as desired.

Next we claim that $(\zeta_R \circ \zeta_R^+)(A) \subseteq A$, for all $A \in \mathcal{X}$. Equivalently we show that $(\zeta_R \circ \iota \circ \zeta_{R^{-1}})(A) \subseteq \iota(A)$, for all $A \in \mathcal{X}$. Assume $y \in (\zeta_R \circ \iota \circ \zeta_{R^{-1}})(A)$ and $y \in A$. Then there exists $z \in (\iota \circ \zeta_{R^{-1}})(A)$ such that $(y, z) \in R^{-1}$. Thus, $z \in (\iota \circ \zeta_{R^{-1}})(A)$ and $z \in \zeta_{R^{-1}}(A)$. This contradiction shows that $y \notin A$ as desired.

To see that every residuated mapping $f : \mathcal{X} \to \mathcal{X}$ is of this form for some binary relation R on X, consider the relation R_f defined on X by

$$(x, y) \in R_f \iff y \in f(\{x\}).$$

Observe that $\zeta_{R_f}(\{x\}) = \{y \in X : (x, y) \in R_f\}$, so that f and ζ_{R_f} agree on singletons. Now if $k : \mathcal{X} \to \mathcal{X}$ is any residuated mapping then, since it is isotone, for every non-empty subset A of X we have

$$k(A) = k\left(\bigcup_{x \in A} \{x\}\right) = \bigcup_{x \in A} k(\{x\}). \tag{7.5}$$

To see that 7.5 holds, notice that if $B = \bigcup_{x \in A} k(\{x\})$ then clearly $k(A) \supseteq B$. On the other hand, $k(\{x\}) \subseteq B$ for every $x \in A$ and so $\{x\} \subseteq k^+(B)$ whence $A = \bigcup_{x \in A}\{x\} \subseteq k^+(B)$. and therefore $k(A) \subseteq B$. Now 7.5 applied to both f and ζ_{R_f}, together with the fact that f and ζ_{R_f} agree on singletons we now have

$$f(A) = \bigcup_{x \in A} f(\{x\}) = \bigcup_{x \in A} \zeta_{R_f}(\{x\}) = \zeta_{R_f}(A).$$

Whence we obtain $f = \zeta_{R_f}$.

□

Theorem 7.38. *The set Res(X) of residuated mappings $f : X \to X$ forms a semigroup, as does the set Res$^+(X)$ of residual mappings $f^+ : X \to X$.*

Proof. The proof follows as in p. 9 MR2126425. Clearly, $g \circ f$ and $f \circ g$ are isotone. Moreover,

$$(f^+ \circ g^+) \circ (g \circ f) \geq f^+ \circ \mathrm{id}_Y \circ f = f^+ \circ f \geq \mathrm{id}_X$$
$$(g \circ f) \circ (f^+ \circ g^+) \leq g \circ \mathrm{id}_Y \circ g^+ = g \circ g^+ \leq \mathrm{id}_Y$$

Thus by the uniqueness of residuals, $(g \circ f)^+$ exists and is $f^+ \circ g^+$. Therefore if $f : X \to Y$ and $g : Y \to X$ are residuated, then $g \circ f$ is also residuated and $(g \circ f)^+ = f^+ \circ g^+$.

□

7.15 Closure Operators

Let $(X, \geq)$ be an ordered set.

Definition 7.9. An isotone mapping $f : X \to X$ is a *closure* on X if it is such that

$$\forall\, x \in X, f(x) = (f \circ f)(x) \geq x$$

and is called a *dual closure* on X if it is such that

$$\forall\, x \in X, x \geq f(x) = (f \circ f)(x)$$

Theorem 7.39. *If X is an ordered set then $f : X \to X$ is a closure if and only if there is an ordered set Y and a residuated mapping $g : X \to Y$ such that $f = g^+ \circ g$.*

Proof. The proof follows as in [**?**, p. 10].

$\Rightarrow$: Suppose that $f : X \to X$ is a closure. Let R be the kernel of f, i.e. the equivalence relation on X defined by

$$(x, y) \in R \iff f(x) = f(y).$$

Define the relation $\sqsubseteq$ on the quotient set E/R by

$$[x]_R \sqsubseteq [y]_R \iff f(x) \leq f(y).$$

It is readily seen that $\sqsubseteq$ is an order on E/R and, since f is isotone, the natural mapping $\tau_R : X \to X/R$ is intone. Now since f is a closure every R-class has a top element, that in $[x]_R$ being $f(x)$. We can therefore define a mapping $g : E/R \to E$ by setting $g([x]_R) = f(x)$. We then have

$$\begin{cases} (g \circ \tau_R)(x) = g([x]_R) = f(x) \geq x; \\ (\tau \circ g)([x]_R) = \tau_R(f(x)) = [f(x)]_R = [x]_R. \end{cases}$$

It follows that τ is residuated with $\tau_R^+ = g$ and that $f = \tau_R^+ \circ \tau_R$.

$\Leftarrow$: Suppose conversely that there is an ordered set Y and a residuated mapping $g : X \to Y$ such that $f = g^+ \circ g$. Then on the one hand

$g^+ \circ g \geq \mathrm{id}_X$; and on the other, by **??**, $g = g \circ g^+ \circ g$, so that $g^+ \circ g = (g^+ \circ g)^2$. Since $g^+ \circ g$ is isotone it follows that $f = g^+ \circ g$ is a closure on X.

□

Theorem 7.40. *Dually, $f : X \to X$ is a dual closure if and only if there is an ordered set Y and a residuated mapping $g : X \to Y$ such that $f = g \circ g^+$.*

If $f : X \to X$ is a closure or a dual closure and if $x \in \mathrm{Im} f$ then $x = f(y)$ for some $y \in E$, whence we obtain $f(x) = f^2(y) = f(y) = x$. Consequently, we see that

$$\mathrm{Im} f = \{x \in E : f(x) = x\},$$

the set of *fixed points* of f. In short, the image of a closure is its set of fixed points.

Definition 7.10. A subset A of an ordered set X is called a (dual) closure subset if there is a (dual) closure $f : X \to X$ such that $A = \mathrm{Im} f$.

Theorem 7.41. *A subset A of an ordered set X is a closure subset of X if and only if for every $x \in X$ the set $x^\uparrow \cap A$ has a bottom element.*

Proof. The proof follows as in [**?**, p. 11]. Suppose that A is a closure subset of X and let $f : X \to X$ be a closure such that $A = \mathrm{Im} f$. Then for every $x \in X$ the set $x^\uparrow \cap A$ is not empty since clearly it contains the element $f(x)$. Moreover, if $z \in x^\uparrow \cap A$ then $x \leq z$ and $f(x) \leq f(z) = z$. Consequently $x^\uparrow \cap A$ has a bottom element, namely $f(x)$. Conversely, suppose that for every $x \in X$ the set $x^\uparrow \cap A$ has a bottom element, x_* say, and consider the mapping $f : X \to X$ given by $f(x) = x_*$. If $x \leq y$ then $x^\uparrow \supseteq y^\uparrow$ gives $x^\uparrow \cap A \supseteq y^\uparrow \cap A$ whence it follows that $x_* \leq y_*$ and so f is isotone. Moreover, since $f(x) = x_* \geq x$ for every $x \in X$ we also have $f \geq \mathrm{id}_X$. Now for any $y \in A$ we clearly have $y = y_* = f(y) \in \mathrm{Im} f$. Applying this to $f(x) = x_* \in A$ we obtain $f^2(x) = f(x)$. Hence $f^2 = f$ and so f is a closure with $\mathrm{Im} f = A$.

□

Remark. Read about quantifiers, start with [**?**, p. 12] and then see Halmos and Janowitz.

is Connections

Galois connections are mathematical structures that allow us to model the relationships between objects in a given category. In this comprehensive guide, you'll learn everything you need to know about these fascinating structures, including their properties and applications. With plenty of examples and exercises to help you along the way, this book is perfect for anyone looking to gain a deeper understanding of Galois connections.

In mathematics, a Galois connection is a structure that allows us to model the relationships between objects. In this comprehensive guide, you'll learn everything you need to know about these fascinating structures, including their properties and applications. With plenty of examples and exercises to help you along the way, this book is perfect for anyone looking to gain a deeper understanding of Galois connections.

Galois connections are a type of relationship between two sets that allows for mappings between the two sets. These mappings preserve (or reverse) certain properties, such as order or containment.

Galois connections were first studied by French mathematician Evariste Galois, who developed the theory of algebraic equations. Galois connections have since been applied to fields such as computer science and linguistics. In computer science, they are used to define data structures and algorithms. In linguistics, they are used to describe the relationship between meaning and sound in language.

Galois connections are a powerful tool for understanding relationships between sets.

Galois connections have a number of interesting properties that make them useful for modeling relationships between objects.

First, every Galois connection has an associated closure operator. This operator takes a set and returns a new set that is "closed" under the given Galois connection. That is, if you have a set A and a Galois connection between A and B, then the closure of A will be a subset of B that contains all the elements of A, plus any additional elements that can be reached from A via the given Galois connection.

Second, every Galois connection has an associated interior operator. This operator takes a set and returns a new set that is "open" under the given Galois connection. That is, if you have a set A and a Galois connection between A and B, then the interior of A will be a subset of B that contains all the elements of A, minus any elements that can't be reached from A via the given Galois connection.

Third, every Galois connection defines a partial order on its associated sets. That is, if you have a set A and a Galois connection between A and B, then the elements of A will be partially ordered by the given Galois connection.

Fourth, every Galois connection has an associated notion of distance. This distance is used to define a metric on the sets that are connected by the Galois connection. This metric allows us to measure how “far” one element is from another.

Finally, every Galois connection has an associated notion of connectedness. This allows us to determine whether two elements are “connected” by the given Galois connection.

Galois connections can be used to model a wide variety of relationships between objects. In computer science, they are used to define data structures and algorithms. In linguistics, they are used to describe the relationship between meaning and sound in language.

Galois connections are also used in category theory, a branch of mathematics that deals with the structure of objects and their relationships. In particular, Galois connections are used to define adjunctions between categories.

Finally, Galois connections can be used to study problems in physics and engineering. For example, they can be used to model the propagation of waves through a medium.

Galois connections are a powerful tool for understanding relationships between sets. This book is a complete guide to the theory of Galois connections, with plenty of examples and exercises to help you along the way.

There are two ways to construct a Galois connection. The first is to start with a closure operator and an interior operator, and then to define the associated mapping between the sets. The second is to start with a partial order and a metric, and then to define the associated closure and interior operators.

Let $(X, \preceq)$ and $(Y, \leqslant)$ be ordered sets.

Definition 7.11. If $f_* : X \to Y$ and $f^* : Y \to X$ are functions such that

$$f_*(x) \leqslant y \iff x \preceq f^*(y) \tag{7.6}$$

for all $x \in X$ and all $y \in Y$, then (f_*, f^*) is called a **Galois connection** between $(X, \preceq)$ and $(Y, \leqslant)$.

There are several definitions of Galois connections in the literature; however they are all order-isomorphic to the definition above.

Theorem 7.42. *Let $f_* : X \to Y$ and $f^* : Y \to X$ be functions. Then (f_*, f^*) is a Galois connection if and only if*

1. *both f_* and f^* are monotone,*

2. *$x \preceq (f^* \circ f_*)(x)$ for all $x \in X$, and*
3. *$(f_* \circ f^*)(y) \leqslant y$ for all $y \in Y$.*

Proof. Suppose (f_*, f^*) is a Galois connection. By (7.6) it follows

$$f_*(x) \leqslant f_*(x) \Longleftrightarrow x \preceq (f^* \circ f_*)(x).$$

Since $\leqslant$ is reflexive, $x \preceq (f^* \circ f_*)(x)$ follows immediately. Similarly, by (7.6) it follows

$$(f_* \circ f^*)(y) \leqslant y \Longleftrightarrow f^*(y) \preceq f^*(y)$$

proving that (**??**) also holds. Assume $x_1 \preceq x_2$. By (**??**) we have $x_2 \preceq (f^* \circ f_*)(x_2)$. By (7.6) it follows $f_*(x_1) \leqslant f_*(x_2)$ and so f_* is monotone. Assume $y_1 \leqslant y_2$. By (**??**) we have $(f_* \circ f^*)(y_1) \leqslant y_1$. By (7.6) it follows $f^*(y_1) \preceq f^*(y_2)$ and so f^* is also monotone.

Conversely, assume (**??**), (**??**), and (**??**) all hold. Assume $f_*(x) \leqslant y$. By (**??**) and (**??**), it follows $(f^* \circ f_*)(x) \preceq f^*(y)$ and $x \preceq (f^* \circ f_*)(x)$, respectively. By transitivity of $\preceq$, we have $x \preceq f^*(y)$ as needed. Assume $x \preceq f^*(y)$. By (**??**) and (**??**), it follows $f_*(x) \leqslant (f_* \circ f^*)(y)$ and $(f_* \circ f^*)(y) \leqslant y$. By transitivity of $\leqslant$, we have $f_*(x) \leqslant y$ as needed. Therefore, (7.6) holds and so (f_*, f^*) is a Galois connection.

□

Theorem 7.43. *Let $f_* : X \to Y$ and $f^* : Y \to X$ be mappings. Then (f_*, f^*) is a Galois connection if and only if*

$$f^*(y) \succeq x \Longleftrightarrow y \succeq f_*(x)$$

Proof. Suppose (7.6) holds. Then

$$f_*(x) \succeq f_*(x) \Longleftrightarrow (f^* \circ f_*)(x) \succeq x.$$

Since $\succeq$ is reflexive, $(f^* \circ f_*)(x) \succeq x$ follows immediately. Similarly, by (7.6) it follows

$$y \succeq (f_* \circ f^*)(y) \Longleftrightarrow f^*(y) \succeq f^*(y)$$

proving that (**??**) holds.

Assume $x_2 \succeq x_1$. By (**??**) we have $(f^* \circ f_*)(x_2) \succeq x_2 \succeq x_1$. By (7.6) it follows $f_*(x_2) \succeq f_*(x_1)$ and so f_* is isotone. Assume $y_1 \succeq y_2$. By (**??**) we have $y_1 \succeq y_2 \succeq (f_* \circ f^*)(y_2)$. By (7.6) it follows $f^*(y_1) \succeq f^*(y_2)$ and so f^* is also isotone.

Conversely, assume (**??**) holds. Assume $y \succeq f_*(x)$. It follows $f^*(y) \succeq (f^* \circ f_*)(x)$ and $(f^* \circ f_*)(x) \succeq x$ and so by transitivity of $\succeq$ we have $f^*(y) \succeq x$ as needed. Assume $f^*(y) \succeq x$. It follows $(f_* \circ f^*)(y) \succeq f_*(x)$

and $y \succeq (f_* \circ f^*)(y)$ and so by transitivity of $\succeq$ we have $y \succeq f_*(x)$ as needed. Therefore (7.6) holds and so (f_*, f^*) is a Galois connection.

□

Theorem 7.44. *If (f_*, f^*) is a Galois connection between $(X, \preceq)$ and $(Y, \leqslant)$, then*

1. $f^*(y) = \max\{x \in X : y \succeq f_*(x)\}$,
2. $f_* \circ f^* \circ f_* = f_*$,
3. *$x \in f^*(Y)$ if and only if x is a fixed point of $f^* \circ f_*$,*
4. *$f^*(Y) = (f^* \circ f_*)(X)$, and*

Proof. (**??**): Let $M = \{x \in X : y \succeq f_*(x)\}$. By (**??**) we have $f^*(y) \in M$. Let $x \in M$. Then $y \succeq f_*(x)$ and since f^* is isotone, it follows $f^*(y) \succeq (f^* \circ f_*)(x)$. By (**??**), we have $(f^* \circ f_*)(x) \succeq x$. By transitivity of $\succeq$, we have $f^*(y) \succeq x$ and thus $f^*(y)$ is the maximum of M. (**??**): By (**??**) we have $f_*(x) \succeq (f_* \circ f^* \circ f_*)(x)$. By (7.6) with $x := (f^* \circ f_*)(x)$ and $y := f_*(x)$ it follows $(f_* \circ f^* \circ f_*)(x) \succeq f_*(x)$ using that $\succeq$ is reflexive.
Since $\succeq$ is antisymmetric, it follows $f_*(x) = (f_* \circ f^* \circ f_*)(x)$ for arbitrary x. (**??**): Clearly $x \in f^*(Y)$ is equivalent to $f^*(y) = x$ for some $y \in Y$. Then

$$(f^* \circ f_*)(x) = (f^* \circ f_* \circ f^*)(y) = f^*(y) = x$$

follows by the dual of (**??**). (**??**): It follows by (**??**) that $f^*(Y) \subseteq (f^* \circ f_*)(X)$. Conversely, let $x \in (f^* \circ f_*)(X)$. Then $x = f^*(y)$ for some $y \in f_*(X) \subseteq Y$. By definition, $x \in f^*(Y)$ and so $(f^* \circ f_*)(X) \subseteq f^*(Y)$.

□

::: {#thm-galois connection-injective } If (f_*, f^*) is a Galois connection, then f_* is injective if and only if f^* is surjective if and only if $f_* \circ f^*$ is the identity. :::

Proof. By **??**, every element of X is a fixed element of $f^* \circ f_*$ if and only if $f^*(Y) = X$. Thus f^* is surjective if and only if $f^* \circ f_*$ is the identity of X. Assume $f^* \circ f_*$ is the identity of X. Then

$$f_*(x) = f_(y) \implies x = (f^* \circ f_*)(x) = (f^* \circ f_*)(y) = y$$

which shows f_* is injective. Conversely, if f_* is injective then, for arbitrary $x \in X$, $(f_* \circ f^* \circ f_*)(x) = f_*(x)$ implies $(f^* \circ f_*)(x) = x$ and so $f^* \circ f_*$ is the identity of X.

□

Theorem 7.45. *If (f_*, g) and (f_*, h) are Galois connections between $(X, \preceq)$ and $(Y, \leqslant)$, then $g = h$. Likewise, if (g, f^*) and (h, f^*) are Galois connections between $(X, \preceq)$ and $(Y, \leqslant)$, then $g = h$.*

Proof. Let $f_* : X \to Y$ and $g : Y \to X$ be a Galois connection. Also let f_* and $h : Y \to X$ be a Galois connection. By (7.6) we have the following

$$f_*(x) \leqslant y \iff x \preceq g(y)$$

$$f_*(x) \leqslant y \iff x \preceq h(y)$$

By (7.15) we have $(f_* \circ h)(y) \leqslant y \iff h(y) \preceq g(y)$.
Notice $(f_* \circ h)(y) \leqslant y$ holds by **??**.(**??**); and thus $h(y) \preceq g(y)$.
By (7.16) we have $(f_* \circ g)(y) \leqslant y \iff g(y) \preceq h(y)$.
Notice $(f_* \circ g)(y) \leqslant y$ holds by **??**.(**??**); and thus $h(y) \preceq g(y)$.
Since $\preceq$ is antisymmetric, it follows $g(y) = h(y)$ for arbitrary y. The second statement is the dual of the first and follows just as easily using **??**.(**??**).

□

Theorem 7.46. *If (f_*, f^*) is a Galois connection between $(X, \preceq)$ and $(Y, \leqslant)$, then*

1. *$f^*(y) =$ the maximum of $\{x \in X : f_*(x) \leqslant y\}$ and*
2. *$f_*(x) =$ the minimum of $\{y \in Y : x \preceq f^*(y)\}$.*

Proof. Let $M = \{x \in X : f_*(x) \leqslant y\}$. By **??**.(**??**) we have $f^*(y) \in M$.
Let $x \in M$.
Then $f_*(x) \leqslant y$ and since f^* is monotone, it follows $(f^* \circ f_*)(x) \preceq f^*(y)$.
By **??**.(**??**), we have $x \preceq (f^* \circ f_*)(x)$. By transitivity of $\preceq$, we have $x \preceq f^*(y)$ and thus $f^*(y)$ is the maximum of M. For the second statement, let $N = \{y \in Y : x \preceq f^*(y)\}$.
By **??**.(**??**) we have $f_*(x) \in N$.
Let $y \in N$. Then $x \preceq f^*(y)$ and since f_* is monotone, it follows $f_*(x) \leqslant (f_* \circ f^*)(y)$.
By **??**.(**??**), we have $(f_* \circ f^*)(y) \leqslant y$ and so by transitivity, it follows $f_*(x) \leqslant y$. Thus $f_*(x)$ is the minimum of N.

□

Theorem 7.47. *If (f_*, f^*) is a Galois connection between $(X, \preceq)$ and $(Y, \leqslant)$, then*

1. *$f_* \circ f^* \circ f_* = f_*$, $f^* \circ f_* \circ f^* = f^*$,*

2. *$x \in f^*(Y)$ if and only if x is a fixed point of $f^* \circ f_*$,*
3. *$y \in f_*(X)$ if and only if y is a fixed point of $f_* \circ f^*$,*
4. *$f^*(Y) = (f^* \circ f_*)(X)$, and $f_*(X) = (f_* \circ f^*)(Y)$.*

Proof. (**??**): Using **??**, we have $f_*(x) \leqslant (f_* \circ f^* \circ f_*)(x)$. By (7.6) with $x := (f^* \circ f_*)(x)$ and $y := f_*(x)$ it follows $(f_* \circ f^* \circ f_*)(x) \leqslant f_*(x)$ using that $\preceq$ is reflexive. Since $\leqslant$ is antisymmetric, it follows $f_*(x) = (f_* \circ f^* \circ f_*)(x)$ for arbitrary x, thus proving (**??**) holds. (**??**): By definition, $x \in f^*(Y)$ is equivalent to $f^*(y) = x$ for some $y \in Y$. Then

$$(f^* \circ f_*)(x) = (f^* \circ f_* \circ f^*)(y) = f^*(y) = x$$

follows by (**??**). (**??**): It follows by (**??**) that $f^*(Y) \subseteq (f^* \circ f_*)(X)$. Conversely, let $x \in (f^* \circ f_*)(X)$. Then $x = f^*(y)$ for some $y \in f_*(X) \subseteq Y$. By definition, $x \in f^*(Y)$ and so $(f^* \circ f_*)(X) \subseteq f^*(Y)$.

□

Theorem 7.48. *If (f_*, f^*) is a Galois connection between $(X, \preceq)$ and $(Y, \leqslant)$, then*

1. *$x \preceq f^*(y) \iff f_*(x) \leqslant (f_* \circ f^*)(y) \iff f_*(x) \leqslant y \iff (f^* \circ f_*)(x) \preceq f^*(y)$,*
2. *$f^*(x) \preceq f^*(y) \iff (f_* \circ f^*)(x) \leqslant (f_* \circ f^*)(y) \iff (f_* \circ f^*)(x) \leqslant y$*
3. *$f_*(x) \leqslant f_*(y) \iff (f^* \circ f_*)(x) \preceq (f^* \circ f_*)(y) \iff x \preceq (f^* \circ f_*)(x)$,*
4. *$f^*(x) = f^*(y) \iff (f_* \circ f^*)(x) = (f_* \circ f^*)(y)$, and*
5. *$f_*(x) = f_*(y) \iff (f^* \circ f_*)(x) = (f^* \circ f_*)(y)$.*

Proof. For the first statement we have

$$\begin{aligned} x \preceq f^*(y) &\implies f_*(x) \leqslant (f_* \circ f^*)(y) \implies f_*(x) \leqslant y \\ &\implies (f^* \circ f_*)(x) \preceq f^*(y) \implies x \preceq f^*(y) \end{aligned}$$

For the third statement we have

$$f^*(x) \preceq f^*(y) \implies (f_* \circ f_*)(x) \leqslant (f_* \circ f^*)(y) \implies (f_* \circ f_*)(x) \leqslant y$$

For the fourth statement we have

$$\begin{aligned} f^*(x) = f^*(y) &\iff f^*(x) \preceq f^*(y) \wedge f^*(y) \preceq f^*(x) \\ &\iff (f_* \circ f^*)(x) \leqslant (f_* \circ f^*)(y) \wedge (f_* \circ f^*)(y) \leqslant (f_* \circ f^*)(x) \\ &\iff (f_* \circ f^*)(x) = (f_* \circ f^*)(y) \end{aligned}$$

The remaining statements are the dual and easily proved.

□

Definition 7.12. By an **order isomorphism** from an ordered set X to another ordered set Y we shall mean an isotone bijection $f : X \to Y$ whose inverse $f^{-1} : Y \to X$ is also an isotone.

Theorem 7.49. *Ordered sets $(X, \preceq)$ and $(Y, \leqslant)$ are isomorphic if and only if there is a surjective mapping $f : X \to Y$ such that*

$$x \preceq y \iff f(x) \leqslant f(y).$$

Proof. The necessity is clear. Suppose conversely that such a surjective mapping f exists. Then f is also injective; for if $f(x) = f(y)$ then from $f(x) \leqslant f(y)$ we obtain $x \preceq y$ and from $f(y) \leqslant f(x)$ we obtain $y \preceq x$, so that $x = y$. Hence f is a bijection. Clearly, f is isotone; and so also is f^{-1}, since $x \preceq y$ can be written $f(f^{-1}))(x) \leqslant f(f^{-1})(y)$ which gives $f^{-1}(x) \preceq f^{-1}(y)$.

□

Theorem 7.50. *If (f_*, f^*) is a Galois connection between $(X, \preceq)$ and $(Y, \leqslant)$, then $f^*(Y)$ and $f_*(X)$ are order-isomorphic.*

Proof. This follows immediately from **??** and **??**.

□

Theorem 7.51. *If (f_*, f^*) is a Galois connection between $(X, \preceq)$ and $(Y, \leqslant)$, then $f^* \circ f_*$ is a closure function for X and $f_* \circ f^*$ is a co-closure function for Y.*

Proof. Let $x \in X$. Then $x \preceq (f^* \circ f_*)(x)$ follows by **??**.(**??**). Since both f^* and f_* are monotone we have, $x_1 \preceq x_2 \implies (f^* \circ f_*)(x_1) \preceq (f^* \circ f_*)(x_2)$. Thus $f^* \circ f_*$ is also monotone. By associativity of functions and **??**.(**??**) we have

$$(f^* \circ f_*) \circ (f^* \circ f_*) = f^* \circ (f_* \circ f^* \circ f_*) = f^* \circ f_*$$

as needed. The dual statement is proved just as easily.

□

By **??**, the closed elements of $f^* \circ f_*$ and $f_* \circ f^*$ are precisely the elements that are an image of some element under f^*, respectively f_*.

Theorem 7.52. *If f is a closure (respectively co-closure) function, then there is a Galois connection (f_*, f^*) such that $f = f^* \circ f_*$ (respectively $f = f_* \circ f^*$).*

Proof. Let $f : X \to X$ be a closure over $(X, \preceq)$. Let $\overline{X}$ be the set of closed elements of f that is $f(X) = \overline{X}$. We will construct a Galois connection between $\overline{X}$ and X using **??**. Let $f_* = f$, that is $f_* : X \to \overline{X}$ defined by $f_*(x) = f(x)$ for all $x \in X$. Let $f^* : \overline{X} \to X$ be the inclusion mapping, that is $f^*(x) = x$ for all $x \in \overline{X}$. Notice $f_* \circ f^*$ is the identity on $\overline{X}$ and $f^* \circ f_* = f$.

1. Notice f_* is monotone since f is monotone and that f^* is monotone since the identity is monotone.
2. Let $x \in X$. Since f is extensive, we have $x \preceq f(x)$. Thus it follows,
$$x \preceq f(x) = (f^* \circ f)(x) = (f^* \circ f_*)(x).$$
3. Let $y \in \overline{X}$. There exists $x \in X$ such that $y = f(x)$. Since f is idempotent we have
$$f(y) = (f \circ f)(y) \preceq y$$
for all $y \in \overline{X}$ as needed.

Therefore, $(f_*, f^*) = (f, f^*)$ where $f^* : \overline{X} \to X$ is the inclusion mapping is a Galois connection between $(X, \prec 0$ and $(\overline{X}, \preceq)$.

□

Remark. A Galois connection is not uniquely determined by a closure.

Theorem 7.53. *Let R be a relation between X and Y and let*

$$f_R(A) = \{b \in Y : \forall a(a \in A \implies (a, b) \in R)\} \tag{7.7}$$
$$f^R(B) = \{a \in X : \forall b(b \in B \implies (a, b) \in R)\}. \tag{7.8}$$

Then (f_R, f^R) is a Galois connection between $(P(X), \subseteq)$ and $(P(Y), \supseteq)$

Proof. Clearly, $f_R : P(X) \to P(Y)$ and $f^R : P(Y) \to P(X)$ are functions. By (7.6) we must show

$$f_R(A) \supseteq B \iff A \subseteq f^R(B) \tag{7.9}$$

for all $A \in P(X)$ and all $B \in P(Y)$. Assume $B \subseteq f_R(A)$. We will show $A \subseteq f^R(B)$. Let $x \in A$. If $y \in B$, then $y \in f_R(A)$. Then, by (**??**), it follows $(x, y) \in R$. So we have shown, $y \in B \implies (x, y) \in R$ as needed to show $x \in f^R(B)$ Conversely, assume $A \subseteq f^R(B)$. We will show $B \subseteq f_R(A)$. Let $y \in B$. If $x \in A$, then $x \in f^R(B)$.Then, by (**??**), it follows $(x, y) \in R$. So we have shown, $x \in A \implies (x, y) \in R$ as needed to show $y \in f_R(A)$. Therefore, (7.9) holds.

□

A **relation** R is a subset of $X \times Y$ where X and Y are sets. If $(a, b) \in R$, then we say a is **related** to b by R and we write aRb. Whenever $X = Y$ we say that R is a relation on X.

Definition 7.13. A relation R on a set X is called

1. **reflexive** if aRa for all $a \in X$,
2. **irreflexive** if $\neg(aRa)$ for all $a \in X$,
3. **symmetric** if aRb implies bRa for all $a, b \in X$,
4. **asymmetric** if aRb implies $\neg(bRa)$ for all $a, b \in X$,
5. **antisymmetric** if $(aRb \text{ and } bRa) \Rightarrow a = b$ for all $a, b \in X$,
6. **transitive** if $(aRb \text{ and } bRc) \Rightarrow aRc$ for all $a, b, c \in X$,
7. **antitransitive** if $(aRb \text{ and } bRc) \Rightarrow \neg(aRc)$ for all $a, b, c \in X$,
8. a **preorder** if $aRb \Leftrightarrow \big(\forall c \in X \; cRa \Rightarrow cRb\big)$ for all $a, b, c \in X$,
9. an **equivalence relation** if $aRb \Leftrightarrow \big(\forall c \in X \; cRa \Leftrightarrow cRb\big)$ for all $a, b, c \in X$.

The asymmetric part of a preorder $\succeq$ (denoted by $\succ$) is called a , i.e. $\succ$ is a strict preorder means there holds

$$\forall\, a, b \in X \qquad a \succ b \Leftrightarrow (a \succeq b \text{ and } b \not\succeq a). \tag{7.10}$$

Associated with any preorder are its and , namely (respectively) subsets of the form

$$\downarrow\!(a) = \{x \in X : a \succeq x\} \qquad \text{and} \qquad \uparrow\!(a) = \{x \in X : x \succeq a\}.$$

If $A \subseteq X$, then A is called an whenever $(x \in A,\, y \in X, \text{ and } y \succeq x) \Rightarrow y \in A$ and is called a whenever $(x \in A,\, y \in X, \text{ and } x \succeq y) \Rightarrow y \in A$. A preorder relation $\succeq$ together with the underlying set is called a and is denoted by $(X, \succeq)$. In particular, if $\succeq$ is also symmetric i.e. an equivalence relation (denoted by $\sim$), then sets of the form

$$[a] = \{x \in X : a \sim x\} = \uparrow\!(a) = \downarrow\!(a).$$

are called **equivalence classes** (we denote the collection of all equivalence class by $\overline{X}$). It is interesting that whenever we have a preorder $\succeq$ the relation $\approx$ prescribed on X by

$$\forall\, a,b \in X \qquad a \approx b \Leftrightarrow (a \succeq b \text{ and } b \succeq a) \tag{7.11}$$

is an equivalence relation. Further, we say an element a of a subset A of X is a **maximum** (resp.) **minimum** for A whenever $a \succeq x$ ($x \succeq a$) for all $x \in A$. Let $M(A)$ and $m(A)$ denote the collection of maximums and minimums of a subset A of X, respectively. In point, if either $a, b \in M(A)$ or $a, b \in m(A)$, then $a \approx b$.

Definition 7.14. A mapping $f : (X, \succeq) \to (Y, \succeq)$ between preordered sets is called

- **isotone** if $a \succeq b \Rightarrow f(a) \succeq f(b)$ for all $a, b \in X$,
- **antitone** if $a \succeq b \Rightarrow f(b) \succeq f(b)$ for all $a, b \in X$,
- **monotone** if it is either isotone or antitone.

Further, if $Y = X$, then f is called 1. **inflationary** if $f(a) \succeq a$ for all $a \in X$, 2. **deflationary** if $a \succeq f(a)$ for all $a \in X$, 3. **quasi-idempotent** if $f(a) \approx (f \circ f)(a)$ for all $a \in X$, 4. **idempotent** if $f(a) = (f \circ f)(a)$ for all $a \in X$, 5. a **closure operator** if $f(b) \succeq a \Leftrightarrow f(b) \succeq f(a)$ for all $a, b \in X$, 6. a **kernel operator** $a \succeq f(b) \Leftrightarrow f(a) \succeq f(b)$ for all $a, b \in X$.

We call a preorder relation $\geq$ on set X that is also antisymmetric a **partial order** and we say that $(X, \geq)$ is an **ordered set**. A mapping $f : X \to Y$ between ordered sets $(X, \geq)$ and $(Y, \succeq)$ is called an **isomorphism** if it is surjective and $x \geq y \Leftrightarrow f(x) \succeq f(y)$ for all $x, y \in X$; and is called a if it is surjective and $x \geq y \Leftrightarrow f(y) \succeq f(x)$ for all $x, y \in X$. A mapping $f : X \to Y$ is an isomorphism if and only if f is bijective and both f and f^{-1} are isotone. For any set X, the mapping $\phi : X \to \mathcal{X}$ prescribed by $\phi(x) = \downarrow x$ is an isomorphism onto the set of all principal down-sets of X.

It is straightforward to show that a mapping f on a preordered (ordered) set is a closure if and only if it is isotone, inflationary, and quasi-idempotent (idempotent). For example, the reflexive (symmetric, transitive) **closure** of a relation R is the intersection of all reflexive (symmetric, transitive) relations that contain R, respectively. We denote these closures by $r(R)$, $s(R)$, and $t(R)$ respectively, and we find there holds

$$r(R) = R \cup I_X, \qquad s(R) = R \cup R^{-1}, \qquad t(R) = \bigcup_{n \geq 1} R^n. \tag{7.12}$$

We say that a relation R **generates an equivalence relation** $\sim$ whenever $\sim = rts(R)$.

Definition 7.15. Let R and S be relations on sets X and Y, respectively, and let $f : X \to Y$ and $g : Y \to X$ be mappings. The pair (f, g) is called

1. a **covariant connection** between (X, R) and (Y, S), denoted by $(f, g) : (X, R) \leftrightarrow (Y, S)$ whenever $g(b)\, R\, a \Leftrightarrow b\, S\, f(a), \forall\, a \in X, \forall\, b \in Y$.
2. an **inverse covariant connection** between (X, R) and (Y, S), denoted by $(f, g) : (X, R) \leftrightarrow (Y, S)$ whenever $a\, R\, g(b) \Leftrightarrow f(a)\, S\, b, \forall\, a \in X, \forall\, b \in Y$.
3. a **contravariant connection** between (X, R) and (Y, S), denoted by $(f, g) : (X, R) \leftrightarrow (Y, S)$ whenever $g(b)\, R\, a \Leftrightarrow f(a)\, S\, b, \forall\, a \in X, \forall\, b \in Y$.
4. an **inverse contravariant connection** between (X, R) and (Y, S), denoted by $(f, g) : (X, R) \leftrightarrow (Y, S)$ whenever $a\, R\, g(b) \Leftrightarrow b\, S\, f(a), \forall\, a \in X, \forall\, b \in Y$.

Generically, we say (f, g) forms a **connection** between (X, R) and (Y, S), denoted by $(f, g) : (X, R) \leftrightarrow (Y, S)$ whenever $\leftrightarrow \in \{\leftrightarrow, \leftrightarrow, \leftrightarrow, \leftrightarrow\}$. \footnote{The notation used here in defining a connection was found in (García-Pardo et al. 2013)).

Example 7.1. If $f : X \to Y$ is a bijection then $(f, f^{-1}) : (X, =) \leftrightarrow (Y, =)$ is a connection of any type. More generally, if f is injective, then $(f, f^{-1}) : (X, =) \leftrightarrow (\mathrm{Im} f, =)$ is a connection of any type.

Example 7.2. The collection of up-sets τ^R of a preorder relation R on a nonempty set X forms an Alexandroff topology on X. Conversely, if τ is a topology on X and if R^τ denotes the relation on X prescribed by

$$b\ R^\tau a \ \Leftrightarrow\ \forall O \in \tau\, (b \in O \Rightarrow a \in O), \tag{7.13}$$

for all $a, b \in X$, then R^τ is a preorder relation on X (called the of τ). Also notice that we have mappings prescribed by

1. $f : Q(X) \to A(X), \quad f(R) = \tau^R$
2. $g : A(X) \to Q(X), \quad g(\tau) = R^\tau$

where $Q(X)$ and $A(X)$ denote the collection of all preorder relations and all Alexandroff topologies on a set X, respectively. Then for any preorder relation R on X, and any Alexandroff topology τ on X, we have

$$(g \circ f)(R) = R \qquad \text{and} \qquad (f \circ g)(\tau) = \tau. \tag{7.14}$$

In other words, there is a natural bijection where f and g are inverses of each other. Hence (f, g) forms a connection of any type and we see that preorder relations and Alexandroff topologies are essential the same. Of course the same can be said for the special case of equivalence relations and partitions.

The next four propositions are either elementary or can be found in [**?**].

Lemma 7.1. *If (f, g) and (f, h) are contravariant connections between preordered sets $(X, \geq)$ and $(Y, \succeq)$, then $g \approx h$.*

Proof. Suppose we have maps $f : X \to Y$, $g : Y \to X$, and $h : Y \to X$ such that

$$g(b) \geq a \Leftrightarrow f(a) \succeq b \qquad (\forall a \in X, \forall b \in Y) \tag{7.15}$$

$$h(b) \geq a \Leftrightarrow f(a) \succeq b \qquad (\forall a \in X, \forall b \in Y) \tag{7.16}$$

We have $(f \circ h)(b) \succeq b$ if and only if $g(b) \geq h(b)$. Notice $(f \circ h)(b) \succeq b$ holds; and thus $g(b) \geq h(b)$. We have $(f \circ g)(b) \succeq b$ if and only if $h(b) \geq g(b)$. Notice $(f \circ g)(b) \succeq b$ holds; and thus $h(b) \geq g(b)$. Hence $g(b) \approx h(b)$ for arbitrary b.

□

Lemma 7.2. *If $f : X \to Y$, $g : Y \to X$ are mappings between preordered sets $(X, \geq)$ and $(Y, \succeq)$, then the following are equivalent:*

1. *$(f, g) : (X, \geq) \leftrightarrow (Y, \succeq)$ is a contravariant connection*
2. *f and g are antitone maps, and $g \circ f$, $f \circ g$ are inflationary maps*
3. *$\downarrow f(a) = g^{-1}(\uparrow a)$, for all $a \in X$*
4. *$\downarrow g(b) = f^{-1}(\uparrow b)$, for all $b \in Y$*
5. *f is antitone and $g(b) \in M(f^{-1}(\uparrow b))$ for all $b \in Y$.*
6. *g is antitone and $f(a) \in M(g^{-1}(\uparrow a))$ for all $a \in X$.*

Proof. (1)⇒(2): Suppose $g(b) \geq a \Leftrightarrow f(a) \succeq b$ for all $a \in X$ and $b \in Y$. It follows that $(g \circ f)(a) \geq a$ and $(f \circ g)(b) \succeq b$ since $\succeq$ is reflexive. Hence $g \circ f$, $f \circ g$ are inflationary maps. Assume $a_1 \geq a_2$ for any $a_1, a_2 \in X$. We have $(g \circ f)(a_1) \geq a_1$, and so by transitivity $(g \circ f)(a_1) \geq a_2$; hence $f(a_2) \succeq f(a_1)$. Assume $b_1 \succeq b_2$ for any $b_1, b_2 \in X$. We have $(f \circ g)(b_1) \succeq b_1$, and so by transitivity $(f \circ g)(b_1) \succeq b_2$; hence $g(b_2) \geq g(b_1)$.

(2)⇒(3):
On one hand we have $f(a) \succeq b$ implies $g(b) \geq (g \circ f)(a) \geq a$ since g is

antitone and $g \circ f$ is inflationary. Conversely we have $g(b) \geq a$ implies $f(a) \succeq (f \circ g)(b) \succeq b$ since f is antitone and $f \circ g$ is inflationary. Hence $f(a) \succeq b \Leftrightarrow g(b) \geq a$ as needed to prove that $\downarrow f(a) = g^{-1}(\uparrow a)$.

(3)⇒(4):
Let $a \in X$ and $b \in Y$ be arbitrary elements. We find

$$g(b) \geq a \Leftrightarrow g(b) \in \uparrow a \Leftrightarrow b \in g^{-1}(\uparrow a) = \downarrow f(a) \Leftrightarrow f(a) \succeq b \Leftrightarrow a \in f^{-1}(\uparrow b).$$

(4)⇒(5):
Assume that $a_1 \geq a_2$ for arbitrary elements $a_1, a_2 \in X$. Since $f(a_1) \geq f(a_1)$, clearly $a_1 \in f^{-1}(\uparrow f(a_1))$.Further, since $f^{-1}(\uparrow f(a_1)) = \downarrow g(f(a_1))$ and $a_1 \geq a_2$, it follows that $a_2 \in f^{-1}(\uparrow f(a_1))$. Hence $f(a_2) \succeq f(a_1)$. For the second statement, let $a \in f^{-1}(\uparrow b)$. Then by hypothesis $g(b) \geq a$, as needed.

(5)⇒(6):
Assume that $b_1 \succeq b_2$ for arbitrary elements $b_1, b_2 \in Y$. Since $g(b_1) \in f^{-1}(\uparrow b_1)$ we have $(f \circ g)(b_1) \succeq b_1 \succeq b_2$. Hence $g(b_1) \in f^{-1}(\uparrow b_2)$ and so $g(b_2) \geq g(b_1)$. Let $a \in X$ be arbitrary and assume that $b \in g^{-1}(\uparrow a)$. Then $g(b) \geq a$. Since f is antitone, we have $f(a) \succeq (f \circ g)(b) \succeq b$ since $g(b) \in f^{-1}(\uparrow b)$.

(6)⇒(1):
Assume that $g(b) \geq a$. Then $b \in g^{-1}(\uparrow a)$ and so $f(a) \succeq b$ by hypothesis. Conversely, assume that $f(a) \succeq b$. Then $g(b) \geq (g \circ f)(a) \geq a$ as needed.

□

Lemma 7.3. *If $(f, g) : (X, \geq) \leftrightarrow (Y, \succeq)$ is a connection between preordered sets then $f \circ g$ and $g \circ f$ are closures Moreover, there holds*

1. *If (f, g) is a contravariant and inverse contravariant (covariant and inverse covariant) connection, then $(g \circ f)(a) \approx a$ for all $a \in A$ and $(f \circ g)(b) \approx b$ for all $b \in B$.*
2. *If (f, g) is a (contravariant or inverse contravariant) connect and a (covariant or inverse covariant) connection, then $a_1 \geq a_2$ implies $f(a_1) \approx f(a_2)$ for all $a_1, a_2 \in X$ and $b_1 \succeq b_2$ implies $g(b_1) \approx g(b_2)$ for all $b_1, b_2 \in Y$.*

Proof. We prove this for the case of contravariant connections and leave the other cases for the reader as an exercise. Assume $(f, g) : (X, \geq) \leftrightarrow (Y, \succeq)$ is a contravariant connection. By **??**, f and g are antitone and so it follows that $f \circ g$ and $g \circ f$ are isotone. Since $f \circ g$ is inflationary we have $(f \circ g \circ f)(a) \succeq f(a)$. Since $g \circ f$ is inflationary we have $(g \circ f)(a) \geq a$ and so $f(a) \succeq (f \circ g \circ f)(a)$ since f is antitone. Hence

$$(f \circ g \circ f)(a) \approx f(a) \tag{7.17}$$

for all $a \in X$. Further since g is antitone we have $(g \circ f \circ g \circ f)(a) \succeq (g \circ f)(a)$ and $(g \circ f)(a) \succeq (g \circ f \circ g \circ f)(a)$. Thus $g \circ f$ is quasi-idempotent. Since $g \circ f$ is inflationary we have $(g \circ f \circ g)(b) \succeq g(b)$. Since $f \circ g$ is inflationary we have $(f \circ g)(b) \geq b$ and so $g(b) \succeq (g \circ f \circ g)(b)$ since g is antitone. Hence $(g \circ f \circ g)(b) \approx g(b)$ for all $b \in Y$. Further since f is antitone we have $(f \circ g \circ f \circ g)(b) \geq (f \circ g)(b)$ and $(f \circ g)(b) \succeq (f \circ g \circ f \circ g)(b)$. Thus $f \circ g$ is quasi-idempotent.

1. Suppose that (f, g) is both a contravariant and inverse contravariant connection. Since $g \circ f$ is both inflationary and deflationary, we have $(g \circ f)(a) \geq a$ and $a \geq (g \circ f)(a)$ and so $(g \circ f)(a) \approx a$. Since $f \circ g$ is both inflationary and deflationary, we have $(f \circ g)(b) \geq b$ and $b \geq (f \circ g)(b)$ and so $(f \circ g)(b) \approx b$.
2. Suppose that (f, g) is both a contravariant and a covariant connection and assume that $a_1 \geq a_2$. Since f is isotone and antitone, we have $f(a_1) \succeq f(a_2)$ and $f(a_2) \succeq f(a_1)$ as needed. If $b_1 \succeq b_2$, then since g is isotone and antitone, we have $g(b_1) \geq g(b_2)$ and $g(b_2) \geq g(b_1)$ as needed.

□

Lemma 7.4. *If $(X, \geq)$ and $(Y, \succeq)$ are preordered sets, there holds*

$$(f, g) : (X, \geq) \leftrightarrow (Y, \succeq) \Rightarrow (f_\approx, g_\approx) : (\overline{X}, \geqq) \leftrightarrow (\overline{Y}, \gtrsim) \tag{7.18}$$

where $f_\approx([a]) = [f(a)]$ for all $a \in X$, $g_\approx([b]) = [g(b)]$ for all $b \in B$, and $\leftrightarrow \in \{\leftrightarrow, \leftrightarrow, \leftrightarrow, \leftrightarrow\}$.

Proof. We prove this for the case of contravariant connections and leave the other cases for the reader as an exercise. Assume $(f, g) : (X, \geq) \leftrightarrow (Y, \succeq)$ is a contravariant connection. We are assuming that $g(b) \geq a \Leftrightarrow f(a) \succeq b$ for all $a \in X, b \in Y$. We must show that $g_\approx([b]) \geqq [a] \Leftrightarrow f_\approx([a]) \gtrsim [b]$ for all $[a] \in \overline{X}, [b] \in \overline{Y}$.

Suppose that $g_\approx([b]) \geqq [a]$. Then $[g(b)] \geqq [a]$ and so $g(b) \geq a$, hence $f(a) \succeq b$. Thus we have that $f_\approx([a]) = [f(a)] \gtrsim [b]$ as needed. Now suppose that $f_\approx([a]) \gtrsim [b]$. Then $[f(a)] \gtrsim [b]$ and so $f(a) \succeq b$, hence $g(b) \geq a$. Thus we have that $g_\approx([b]) = [g(b)] \gtrsim [a]$ as needed.

□

Contravariant Connections	
$(f,g):(X,\geq)\leftrightarrow(Y,\succeq)$	$(f,g):(X,\geq)\leftrightarrow(Y,\succeq)$
$g(b)\geq a\Leftrightarrow f(a)\succeq b$ for all $a\in X, b\in Y$	$a\geq g(b)\Leftrightarrow b\succeq f(a)$ for all $a\in X, b\in Y$
f and g are antitone maps, and $g\circ f$, $f\circ g$ are inflationary maps	f and g are antitone maps, and $g\circ f$, $f\circ g$ are deflationary maps
$\downarrow f(a)=g^{-1}(\uparrow a)$, for all $a\in X$	$\uparrow f(a)=g^{-1}(\downarrow a)$, for all $a\in X$
$\downarrow g(b)=f^{-1}(\uparrow b)$, for all $b\in Y$	$\uparrow g(b)=f^{-1}(\downarrow b)$, for all $b\in Y$
f is antitone and $g(b)\in M(f^{-1}(\uparrow b))$, for all $b\in Y$.	f is antitone and $g(b)\in m(f^{-1}(\downarrow b))$, for all $b\in Y$.
g is antitone and $f(a)\in M(g^{-1}(\uparrow a))$, for all $a\in X$.	g is antitone and $f(a)\in m(g^{-1}(\downarrow a))$, for all $a\in X$.
Covariant Connections	
$(f,g):(X,\geq)\leftrightarrow(Y,\succeq)$	$(f,g):(X,\geq)\leftrightarrow(Y,\succeq)$
$g(b)\geq a\Leftrightarrow b\succeq f(a)$ for all $a\in X, b\in Y$	$a\geq g(b)\Leftrightarrow f(a)\succeq b$ for all $a\in X, b\in Y$
f and g are isotone, $g\circ f$ is inflationary, and $f\circ g$ is deflationary	f and g are isotone, $f\circ g$ is inflationary, and $g\circ f$ is deflationary
$\uparrow f(a)=g^{-1}(\uparrow a)$, for all $a\in X$	$\downarrow f(a)=g^{-1}(\downarrow a)$, for all $a\in X$
$\downarrow g(b)=f^{-1}(\downarrow b)$, for all $b\in Y$	$\uparrow g(b)=f^{-1}(\uparrow b)$, for all $b\in Y$
f is isotone and $g(b)\in M(f^{-1}(\downarrow b))$, for all $b\in Y$.	f is isotone and $g(b)\in m(f^{-1}(\uparrow b))$, for all $b\in Y$.
g is isotone and $f(a)\in m(g^{-1}(\uparrow a))$, for all $a\in X$.	g is isotone and $f(a)\in M(g^{-1}(\downarrow a))$, for all $a\in X$.

Figure 7.1: Summary of equivalencies for connections between preorders.

Chapter 8

Concept Theory

References

Adamson, Iain T. 1998. "Equivalents of the Axiom of Choice." In *A Set Theory Workbook*, 59–62. Springer.

Cantor, Georg. 1883. "Ueber Unendliche, Lineare Punktmannichfaltigkeiten." *Math. Ann.* 21 (4): 545–91. https://doi.org/10.1007/BF01446819.

García-Pardo, F., I. P. Cabrera, P. Cordero, and Manuel Ojeda-Aciego. 2013. "On Galois Connections and Soft Computing." In *Advances in Computational Intelligence*, edited by Ignacio Rojas, Gonzalo Joya, and Joan Cabestany, 7903:224–35. Lecture Notes in Computer Science. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-38682-4_26.

Halmos, Paul R. 1974. *Naive Set Theory.* Springer-Verlag, New York-Heidelberg.

Harzheim, Egbert. 2005. *Ordered Sets.* Vol. 7. Advances in Mathematics (Springer). New York: Springer.

Jech, Thomas J. 2008. *The Axiom of Choice.* Courier Corporation.

Moore, Gregory H. 2012. *Zermelo's Axiom of Choice: Its Origins, Development, and Influence.* Courier Corporation.

Rubin, Herman, and Jean E Rubin. 1985. *Equivalents of the Axiom of Choice, II.* Elsevier.

Suppes, Patrick. 1972. "Axiomatic Set Theory, 1960." Dover edn., New York.

Szpilrajn, Edward. 1930. "Sur l'extension de l'ordre Partiel." *Fundamenta Mathematicae* 16 (1): 386–89.

Tourlakis, George. 2003. *Lectures in Logic and Set Theory: Volume 2, Set Theory.* Vol. 83. Cambridge University Press.

Index