

# Cumulative Notes

Tree

September 12, 2023

# Contents

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Naive Set Theory and Logic</b>                | <b>3</b>  |
| 1.1      | Sets . . . . .                                   | 4         |
| 1.2      | Functions . . . . .                              | 7         |
| 1.3      | Relations . . . . .                              | 9         |
| 1.4      | Least Upper Bound Property . . . . .             | 11        |
| <b>2</b> | <b>Logic</b>                                     | <b>12</b> |
| 2.1      | Notation . . . . .                               | 13        |
| 2.2      | Functions and Predicates . . . . .               | 14        |
| 2.3      | First-Order Languages . . . . .                  | 16        |
| 2.4      | Structures . . . . .                             | 17        |
| 2.5      | First-Order Theories . . . . .                   | 19        |
| 2.6      | The Characterization Problem . . . . .           | 22        |
| 2.7      | Interpretations . . . . .                        | 24        |
| <b>3</b> | <b>Topology</b>                                  | <b>25</b> |
| 3.1      | Topological Space . . . . .                      | 26        |
| 3.2      | Closed Sets . . . . .                            | 28        |
| 3.3      | Important Topologies . . . . .                   | 30        |
| 3.4      | Hausdorff Spaces . . . . .                       | 38        |
| 3.5      | Sequences (Topology) . . . . .                   | 39        |
| 3.6      | $T_i$ Axioms . . . . .                           | 40        |
| 3.7      | Continuous Function . . . . .                    | 41        |
| 3.8      | Homeomorphisms . . . . .                         | 43        |
| <b>4</b> | <b>Analysis</b>                                  | <b>44</b> |
| <b>5</b> | <b>Group Theory</b>                              | <b>45</b> |
| 5.1      | Notation . . . . .                               | 46        |
| 5.2      | Definition and Examples . . . . .                | 47        |
| 5.3      | How to Form New Groups From Given Ones . . . . . | 48        |
| 5.4      | Basic Theorems About Groups . . . . .            | 49        |
| 5.5      | Order of An Element of A Group . . . . .         | 50        |
| 5.6      | Multiplication Table . . . . .                   | 51        |
| 5.7      | Generators and Relations . . . . .               | 52        |
| 5.8      | Important Groups . . . . .                       | 53        |
| 5.9      | Homomorphisms and Isomorphisms . . . . .         | 57        |
| 5.10     | Group Actions . . . . .                          | 58        |

|  |           |
|--|-----------|
| <i>CONTENTS</i>  | 2         |
| <b>6 Ring Theory</b>   | <b>59</b> |
| <b>7 Combinatorics</b>                                       | <b>60</b> |
| 7.1 The Pigeonhole Principle . . . . .                       | 61        |
| <b>A Solutions to Shoenfield's <i>Mathematical Logic</i></b> | <b>62</b> |
| A.1 The Nature of Mathematical Logic . . . . .               | 62        |
| A.2 First-Order Theories . . . . .                           | 62        |
| <b>B Solutions to D&amp;F's <i>Abstract Algebra</i></b>      | <b>65</b> |
| B.1 Introduction to Groups . . . . .                         | 77        |
| <b>C Solutions to Munkres' <i>Topology</i></b>               | <b>81</b> |
| C.1 Set Theory and Logic . . . . .                           | 81        |

## Chapter 1

# Naive Set Theory and Logic

Axiomatic set theory is the list of axioms which define sets, on which essentially the rest of math is based. Here is given a less formal treatment called naive set theory. Taken to its logical extreme, it results in contradictions and nonsense. But it serves well enough for the purposes of most mathematicians' day-to-day work.

Incidentally, there are other solutions to these paradoxes, notably type theory and category theory. Homotopy Type Theory (HoTT) is one recent formulation which is gaining ground as an alternative foundation to mathematics.

## 1.1 Sets

### 1.1.1 Definition and Examples

**Definition 1.1.1** (Set/Elements of a Set). In naive set theory, a *set*  $A$  is a collection of objects. These objects are called the *elements* of the set. We write  $a \in A$  if  $a$  is an element of  $A$ . We write  $a \notin A$  if  $a$  is not an element of  $A$ .

**Example 1.1.1.1.**

- The *empty set* is the set which contains no elements. We denote the empty set by  $\emptyset$ .
- The set of all subsets of a set  $A$  is called the *power set of*  $A$ , and is denoted by  $\mathcal{P}(A)$ .
- The set of all integers is denoted  $\mathbb{Z}$ .

We can specify a set in two main ways. The first is to explicitly list the elements of the set within curly brackets:

$$A = \{a, b, c\}$$

The second is to consider as a set all objects which have a certain property. For example, we can specify the set  $A$  of all people as follows:

$$A = \{x \mid x \text{ is a person}\},$$

which is to be read as “The set of all  $x$  such that  $x$  is a person.”

This naive view of sets can lead to contradictions since there is no restriction on what a set can be. For example, consider Russell’s paradox: Does the set of all sets which do not contain themselves contain itself? Such contradictions are solved in axiomatic set theory by restricting what is able to be considered a set.

Sets are commonly visualized as circles or ovals, as in Figure 1.1, which depicts a set  $A$  containing elements  $a$  and  $b$ .

It is common to “equip” a set with a structure. For example, one could equip a set with a topology, as discussed in Section 3.1.

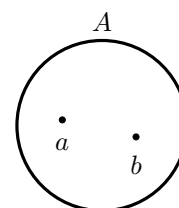


Figure 1.1: A set  $A$  which contains elements  $a$  and  $b$ .

### 1.1.2 Comparing Different Sets

- $A$  is a **subset** of  $B$  if every element of  $A$  is also an element of  $B$ , and we write  $A \subseteq B$ .  $A$  is a **proper subset** of  $B$  if  $A$  is a subset of  $B$  and  $A$  is different from  $B$ , and we write  $A \subsetneq B$ . See Figure 1.2.
- Two sets are **disjoint** if  $A \cap B = \emptyset$ .
- A set is **finite** if it is empty or if there is a bijection

$$f : A \rightarrow \{1, 2, \dots, n\}$$

for some positive integer  $n$ . (See Sec 1.2.3.) In the former case, we say that  $A$  has **cardinality** 0; in the latter case, we say that  $A$  has **cardinality**  $n$ . If a bijection exists between  $A$  and the positive integers, we say that  $f$  is **countably infinite**. If a set is finite or countably infinite, it is **countable**. If there exists a bijection between two sets, they have the same cardinality. We denote the cardinality of  $A$  by  $|A|$ . Intuitively, if you can pair up

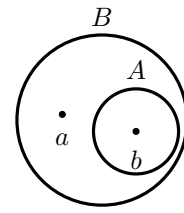


Figure 1.2: The set  $A = \{b\}$  is a proper subset of the set  $B = \{a, b\}$ .

**Remark 1.1.1.** ZXclkJZXlckLxcj...

### 1.1.3 How to Form New Sets From Given Ones

- Given some sets, we could consider the set to which each of these sets is an element. We refer to this new set as a **collection** of sets.
- Given a collection  $\mathcal{A}$  of sets, the **union** of the elements of  $\mathcal{A}$  is the set

$$\bigcup_{A \in \mathcal{A}} A = \{x \mid x \in A \text{ for at least one } A \in \mathcal{A}\}.$$

- Given a collection  $\mathcal{A}$  of sets, the **intersection** of the elements of  $\mathcal{A}$  is the set

$$\bigcap_{A \in \mathcal{A}} A = \{x \mid x \in A \text{ for every } A \in \mathcal{A}\}.$$

- Given two sets  $A$  and  $B$ , the **difference** of  $A$  and  $B$  is the set

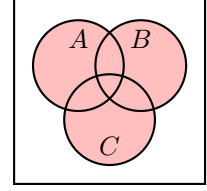
$$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}.$$

- Let  $\{A_\alpha\}_{\alpha \in J}$  be an indexed family of sets. Let  $X = \bigcup_{\alpha \in J} A_\alpha$ . We define the **cartesian product** of this indexed family, denoted by

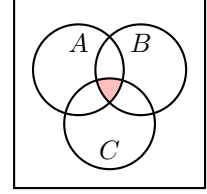
$$\prod_{\alpha \in J} A_\alpha,$$

to be the set of all  $J$ -tuples  $(x_\alpha)_{\alpha \in J}$  of elements of  $X$  such that  $x_\alpha \in A_\alpha$  for each  $\alpha \in J$ .

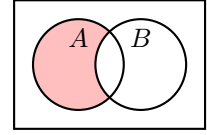
- We can also break sets down into constituent parts. The **partition** of a set  $A$  is a collection of disjoint nonempty subsets of  $A$  whose union is all of  $A$ .



(a) Here  $\mathcal{A} = A, B, C$  and the shaded region illustrates  $\bigcup_{X \in \mathcal{A}} X$  (or  $A \cup B \cup C$ ).



(b) Here  $\mathcal{A} = A, B, C$  and the shaded region illustrates  $\bigcap_{X \in \mathcal{A}} X$  (or  $A \cap B \cap C$ ).



(c) The shaded region illustrates  $A \setminus B$ .

Figure 1.3: Visualization of common set operations.

#### Theorem 1.1.1 (Laws of Combining Sets).

- *Set-Theoretic Distributive Laws:*

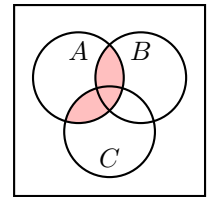
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C);$$

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

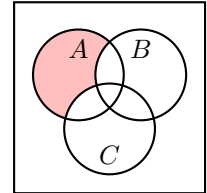
- *DeMorgan's Laws:*

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

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



(a) Visualization of the first distributive law.



(b) Visualization of the first of DeMorgan's laws.

## 1.2 Functions

### 1.2.1 Definition and Examples

#### Definition 1.2.1.

- A **rule of assignment** is a subset  $r$  of the cartesian product  $C \times D$  of two sets such that

$$[(c, d) \in r \text{ and } (c, d') \in r] \Rightarrow [d = d'].$$

The **domain** and **image set** of  $r$  are defined as

$$\begin{aligned} \text{domain } r &= \{c \mid \text{there exists } d \in D \text{ such that } (c, d) \in r\}, \\ \text{image } r &= \{d \mid \text{there exists } c \in C \text{ such that } (c, d) \in r\}. \end{aligned}$$

- A **function**  $f$  is a rule of assignment  $r$ , together with a set  $B$  that contains the image set of  $r$ . The domain  $A$  of the rule  $r$  is also called the **domain** of the function  $f$ ; the image set of  $r$  is also called the **image set** of  $f$ ; and the set  $B$  is called the **codomain** of  $f$ . We write  $f : A \rightarrow B$  and say “ $f$  is a function from  $A$  to  $B$ ”
- If  $f : A \rightarrow B$  and if  $a$  is an element of  $A$ , we denote by  $f(a)$  the unique element of  $B$  such that  $(a, f(a)) \in r$ ; it is called the **value** of  $f$  at  $a$ , or the **image** of  $a$  under  $f$ . We also write  $a \mapsto b$ .
- Let  $f : A \rightarrow B$ . If  $A_0$  is a subset of  $A$ , we denote by  $f(A_0)$  the set  $f(A_0) = \{b \mid b = f(a) \text{ for at least one } a \in A_0\}$ . This set is called the **image** of  $A_0$  under  $f$ .
- If  $B_0$  is a subset of  $B$ , we denote by  $f^{-1}(B_0)$  the set  $f^{-1}(B_0) = \{a \mid f(a) \in B_0\}$ . This set is called the **preimage** of  $B_0$  under  $f$ . The preimage of a single-element set, say  $\{b\}$ , under  $f$  is called the **fiber** of  $f$  over  $b$ .

Intuitively, a function is a mapping from one set to another. Functions are commonly visualized as arrows between the elements of sets, as in Figure 1.5.

### 1.2.2 How to Form New Functions From Given Ones

- If  $f : A \rightarrow B$  and if  $A_0$  is a subset of  $A$ , we define the **restriction** of  $f$  to  $A_0$  to be the function mapping  $A_0$  into  $B$  whose rule is  $\{(a, f(a)) \mid a \in A_0\}$ . It is denoted by  $f|A_0$ , and we say “ $f$  restricted to  $A_0$ .”

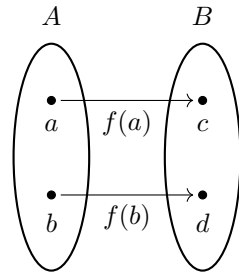


Figure 1.5: A function  $f$  between the sets  $A$  and  $B$ .



- Given functions  $f : A \rightarrow B$  and  $g : B \rightarrow C$ , we can define the **composite**  $g \circ f$  (read “ $g$  after  $f$ ”) of  $f$  and  $g$  as the function  $g \circ f : A \rightarrow C$  to be the function whose rule is

$$\{(a, c) \mid \text{For some } b \in B, f(a) = b \text{ and } g(b) = c\}.$$

- If  $f : A \rightarrow B$ , then  $f$  has a **left inverse** if there is a function  $g : B \rightarrow A$  such that  $g \circ f : A \rightarrow A$  is the identity map on  $A$ , i.e.,  $(g \circ f)(a) = a$ , for all  $a \in A$ .  $f$  has a **right inverse** if there is a function  $h : B \rightarrow A$  such that  $f \circ h : B \rightarrow B$  is the identity map on  $B$ .
- If  $f$  is bijective, there exists a function  $f^{-1}$  called the **inverse** of  $f$  defined by letting  $f^{-1}(b)$  be the unique  $a$  such that  $f(a) = b$ .

### 1.2.3 Properties a Function Can Have

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

$$[f(a) = f(a')] \Rightarrow [a = a'],$$

and **surjective** (or **onto**) if

$$[b \in B] \Rightarrow [b = f(a) \text{ for at least one } a \in A].$$

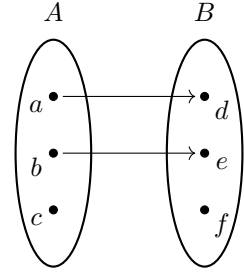
If  $f$  is both injective and surjective, it is said to be **bijective** (or is called a **one-to-one correspondence**).

The basic idea is that if we can find a bijective function between two sets, then they are the same “size” or “cardinality.” (See Section 1.1.2.) These properties are illustrated in Figure 1.6.

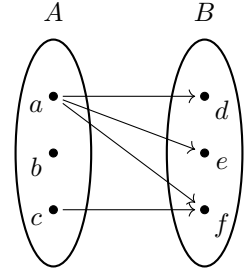
The following lemma comes in handy for showing that a given function is bijective

**Lemma 1.2.1.** *Let  $f : A \rightarrow B$ . If there are functions  $g : B \rightarrow A$  and  $h : B \rightarrow A$  such that  $g(f(a)) = a$  for every  $a$  in  $A$  and  $f(h(b)) = b$  for every  $b$  in  $B$ , then  $f$  is bijective and  $g = h = f^{-1}$ .*

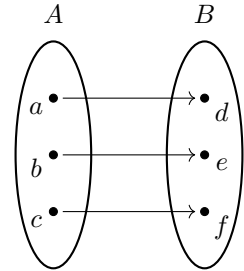
**Example 1.2.3.1.** A **permutation** of a set  $A$  is simply a bijection from  $A$  to itself.



(a) This function is injective but not surjective.



(b) This function is surjective but not injective.



(c) This function is bijective.

Figure 1.6: Visualizations of injective, surjective, and bijective functions.

## 1.3 Relations

### 1.3.1 Definition and Examples

**Definition 1.3.1** (Relation). A **binary relation** on a set  $A$  is a subset  $C$  of the cartesian product  $A \times A$ . We use the notation  $xCy$  to mean the same thing as  $(x, y) \in C$ , and we say “ $x$  is in the relation  $C$  to  $y$ .”

Remark: This is weaker than a rule of assignment in the sense that a given element is allowed to be assigned to more than one value of the second set. A function  $f : A \rightarrow A$  is a special case of a relation. Note that both sets are always the same in the case of a relation.

For a given relation  $C$  on the set  $A$ ,

- A relation is **reflexive** if  $xCx$  for every  $x$  in  $A$ .
- A relation is **symmetric** if  $xCy$  implies  $yCx$ .
- A relation is **transitive** if  $xCy$  and  $yCz$  together implies  $xCz$ .
- A relation is **comparable** if for every  $x$  and  $y$  in  $A$  for which  $x \neq y$ , either  $xCy$  or  $yCx$ .
- A relation is **nonreflexive** if for no  $x$  in  $A$  does the relation  $xCx$  hold.

### 1.3.2 Equivalence Relations

**Definition 1.3.2** (Equivalence Relation). An **equivalence relation** on a set  $A$  is a relation  $C$  on  $A$  which is reflexive, symmetric, and transitive. We often use  $\sim$  for an equivalence relation instead of  $C$ .

- Given an equivalence relation  $\sim$  on a set  $A$  and an element  $x$  of  $A$ , we define the **equivalence class** determined by  $x$  as

$$\{y \mid y \sim x\}.$$

If  $C$  is an equivalence class, any element of  $C$  is called a **representative** of the class  $C$ . Two equivalent classes are either disjoint or equal, and the collection of equivalence classes of a set  $A$  partition  $A$ .

### 1.3.3 Order Relations

**Definition 1.3.3** (Order Relation). An *order relation* on a set  $A$  is a relation  $C$  on  $A$  which is comparable, nonreflexive, and transitive. We often use  $<$  for an order relation instead of  $C$ .

Suppose that  $A$  and  $B$  are two sets with order relations. We say that  $A$  and  $B$  have the same *order type* if there is a bijective correspondence between them that preserves order.

**Example 1.3.3.1.** Suppose that  $A$  and  $B$  are two sets with order relations  $<_A$  and  $<_B$  respectively. Define an order relation  $<$  on  $A \times B$  by defining

$$a_1 \times b_1 < a_2 \times b_2$$

if  $a_1 <_A a_2$  or if  $a_1 = a_2$  and  $b_1 <_B b_2$ . This is called the *dictionary order relation*.

## 1.4 Least Upper Bound Property

### Definition 1.4.1.

- Suppose that  $A$  is a set ordered by the relation  $<$ . Let  $A_0$  be a subset of  $A$ . We say the element  $b$  is the **largest element** of  $A_0$  if  $b \in A_0$  and if  $x \leq b$  for every  $x \in A_0$ . Similarly, we say that  $a$  is the **smallest element** of  $A_0$  if  $a \in A_0$  and if  $a \leq x$  for every  $x \in A_0$ .
- We say that the subset  $A_0$  of  $A$  is **bounded above** if there is an element  $b$  of  $A$  such that  $x \leq b$  for every  $x \in A_0$ ; the element  $b$  is called an **upper bound** for  $A_0$ . If the set of all upper bounds for  $A_0$  has a smallest element, that element is called the **least upper bound**, or the **supremum**, of  $A_0$ . It is denoted by  $\sup A_0$ .
- Similarly,  $A_0$  is **bounded below** if there is an element  $a$  of  $A$  such that  $a \leq x$  for every  $x \in A_0$ ; the element  $a$  is called a **lower bound** for  $A_0$ . If the set of all lower bounds for  $A_0$  has a largest element, that element is called the **greatest lower bound**, or the **infimum**, of  $A_0$ . It is denoted by  $\inf A_0$ .
- An ordered set  $A$  is said to have the **least upper bound property** if every nonempty subset  $A_0$  of  $A$  that is bounded above has a least upper bound.

The real numbers have the least upper bound property.

## Chapter 2

# Logic

Logic provides the materials needed for a rigorous theory of how to prove theorems and build axiomatic systems such as axiomatic set theory. It contains fascinating theorems with widespread implications such as Gödel's infamous Incompleteness Theorems. The information in this chapter is based on Shoenfield's classic *Mathematical Logic* (1967).

## 2.1 Notation

- $\mathbf{u}$  and  $\mathbf{v}$  are syntactical variables which vary through all expressions.
- $\mathbf{A}$ ,  $\mathbf{B}$ ,  $\mathbf{C}$ , and  $\mathbf{D}$  are syntactical variables which vary through formulas.
- $\mathbf{x}$ ,  $\mathbf{y}$ ,  $\mathbf{z}$ , and  $\mathbf{w}$  are syntactical variables which vary through variables.
- $\mathbf{f}$  and  $\mathbf{g}$  are syntactical variables which vary through function symbols.
- $\mathbf{p}$  and  $\mathbf{q}$  are syntactical variables which vary through predicate symbols.
- $\mathbf{e}$  is a syntactical variables which varies through constants.
- $\mathbf{a}$ ,  $\mathbf{b}$ ,  $\mathbf{c}$ , and  $\mathbf{d}$  are syntactical variables which vary through terms.
- $\mathbf{b}_{\mathbf{x}_1, \dots, \mathbf{x}_n}[\mathbf{a}_1, \dots, \mathbf{a}_n]$  designates the expression obtained from  $\mathbf{b}$  by replacing all occurrences of  $\mathbf{x}_1, \dots, \mathbf{x}_n$  by  $\mathbf{a}_1, \dots, \mathbf{a}_n$  respectively.
- $\mathbf{A}_{\mathbf{x}_1, \dots, \mathbf{x}_n}[\mathbf{a}_1, \dots, \mathbf{a}_n]$  designates the expression obtained from  $\mathbf{A}$  by replacing all free occurrences of  $\mathbf{x}_1, \dots, \mathbf{x}_n$  by  $\mathbf{a}_1, \dots, \mathbf{a}_n$  respectively.
- $\mathbf{i}$  and  $\mathbf{j}$  are syntactical variables which vary through names.

## 2.2 Functions and Predicates

Main Idea: Functions assign a collection of elements from one set to a single element of another set. Predicates represent some relationship between a collection of elements from a set.

**Definition 2.2.1** (*n*-tuple). An *n-tuple* in  $A$  is a sequence of  $n$  (not necessarily distinct) objects in  $A$ .

We write  $(a_1, a_2, \dots, a_n)$  for the  $n$ -tuple consisting of the objects  $a_1, a_2, \dots, a_n$  in that order. We agree that there is exactly one 0-tuple in  $A$ , and we designate it by  $()$ .

**Definition 2.2.2** (Functions). A mapping from the set of  $n$ -tuples in  $A$  to  $B$  is called an *n-ary function from  $A$  to  $B$* .

**Example 2.2.0.1** (Truth Functions). A *truth function* is a function from the set of truth values,  $\{\mathbf{T}, \mathbf{F}\}$ , to the set of truth values. We have

- the *and* truth function:

$$\begin{aligned} H_{\wedge}(\mathbf{T}, \mathbf{T}) &= \mathbf{T}, \\ H_{\wedge}(\mathbf{T}, \mathbf{F}) &= H_{\wedge}(\mathbf{F}, \mathbf{T}) = H_{\wedge}(\mathbf{F}, \mathbf{F}) = \mathbf{F}. \end{aligned}$$

- the *or* truth function:

$$\begin{aligned} H_{\vee}(\mathbf{T}, \mathbf{T}) &= H_{\vee}(\mathbf{T}, \mathbf{F}) = H_{\vee}(\mathbf{F}, \mathbf{T}) = \mathbf{T}, \\ H_{\vee}(\mathbf{F}, \mathbf{F}) &= \mathbf{F}. \end{aligned}$$

- the *if ... then* truth function:

$$\begin{aligned} H_{\rightarrow}(\mathbf{T}, \mathbf{T}) &= H_{\rightarrow}(\mathbf{F}, \mathbf{T}) = H_{\rightarrow}(\mathbf{F}, \mathbf{F}) = \mathbf{T}, \\ H_{\rightarrow}(\mathbf{T}, \mathbf{F}) &= \mathbf{F}. \end{aligned}$$

- the *if and only if* truth function:

$$\begin{aligned} H_{\leftrightarrow}(\mathbf{T}, \mathbf{T}) &= H_{\leftrightarrow}(\mathbf{F}, \mathbf{F}) = \mathbf{T}, \\ H_{\leftrightarrow}(\mathbf{T}, \mathbf{F}) &= H_{\leftrightarrow}(\mathbf{F}, \mathbf{T}) = \mathbf{F}. \end{aligned}$$

- the *not* truth function:

$$H_{\neg}(\mathbf{T}) = \mathbf{F}, \quad H_{\neg}(\mathbf{F}) = \mathbf{T}.$$

**Definition 2.2.3** (Predicate). A subset of the set of  $n$ -tuples in  $A$  is called an  *$n$ -ary predicate in  $A$* .

If  $P$  represents such a predicate, then  $P(a_1, \dots, a_n)$  means that the  $n$ -tuple  $(a_1, \dots, a_n)$  is in  $P$ . We say ***unary*** for 1-ary and ***binary*** for 2-ary. Note that a unary function from  $A$  to  $B$  is a mapping from  $A$  to  $B$ , and that a unary predicate in  $A$  is a subset of  $A$ .



## 2.3 First-Order Languages

Main Idea: First-order languages belong to the syntactical study of axiom systems. They describe the symbols to be used.

**Definition 2.3.1** (First-order Language). A *first-order language* has as symbols the following:

a) the variables

$$x, y, z, w, x', y', z', w', x'', \dots;$$

b) for each  $n$ , the  $n$ -ary function symbols and the  $n$ -ary predicate symbols;

c) the symbols  $\neg$ ,  $\vee$ , and  $\exists$ .

Remark: The equality symbol  $=$  must be among the binary predicate symbols.

The first-order language  $L'$  is an *extension* of the first-order language  $L$  if every nonlogical symbol of  $L$  is a nonlogical symbol of  $L'$ .

**Definition 2.3.2** (Designators).

- We define the *terms* of a first-order language by the generalized inductive definition:

i) a variable is a term;

ii) if  $u_1, \dots, u_n$  are terms and  $f$  is  $n$ -ary, then  $fu_1 \dots u_n$  is a term.

- An *atomic formula* is an expression of the form  $pa_1 \dots a_n$  where  $p$  is  $n$ -ary. We define the *formulas* of a first-order language by the generalized inductive definition:

i) an atomic formula is a formula;

ii) if  $u$  is a formula, then  $\neg u$  is a formula;

iii) if  $u$  and  $v$  are formulas, then  $\vee uv$  is a formula;

iv) if  $u$  is a formula, then  $\exists xu$  is a formula.

- A *designator* is an expression which is either a term or a formula.

## 2.4 Structures

Main Idea: Structures describe the semantics, the meaning, of first-order languages; We attach meanings to the symbols. Individuals of the structure are given names. Add names to  $L$  to get  $L(\mathcal{A})$ . Assign every variable-free term of  $L(\mathcal{A})$  to an individual of the structure. Closed formulas of  $L(\mathcal{A})$  are then given truth values, specifying if they're true in the structure. Then can say  $\mathbf{A}$  is valid in  $\mathcal{A}$  if every instantiation of  $\mathbf{A}$  is true in  $\mathcal{A}$ . A model is a structure for a theory of a language in which all the nonlogical axioms of the theory are valid.

### 2.4.1 Definition

**Definition 2.4.1** (Structure). Let  $L$  be a first-order language. A **structure**  $\mathcal{A}$  for  $L$  consists of the following things:

- i) A nonempty set  $|\mathcal{A}|$ , called the **universe** of  $\mathcal{A}$ . The elements of  $|\mathcal{A}|$  are called the **individuals** of  $\mathcal{A}$ .
- ii) For each  $n$ -ary function symbol  $\mathbf{f}$  of  $L$ , an  $n$ -ary function  $\mathbf{f}_{\mathcal{A}}$  from  $|\mathcal{A}|$  to  $|\mathcal{A}|$ .
- iii) For each  $n$ -ary predicate symbol  $\mathbf{p}$  of  $L$  other than  $=$ , an  $n$ -ary predicate  $\mathbf{p}_{\mathcal{A}}$  in  $|\mathcal{A}|$ .

For each individual  $a$  of  $\mathcal{A}$ , we choose a new constant, called the **name** of  $a$ . The first-order language obtained from  $L$  by adding all the names of individuals of  $\mathcal{A}$  is designated by  $L(\mathcal{A})$ . A formula  $\mathbf{A}$  is **closed** if no variable is free in  $\mathbf{A}$ .

### 2.4.2 Individuals and Truth of Formulas in $\mathcal{A}$

For each variable-free term  $\mathbf{a}$  of  $L(\mathcal{A})$ :

- If  $\mathbf{a}$  is a name,  $\mathcal{A}(\mathbf{a})$  is the individual of which  $\mathbf{a}$  is the name.
- If  $\mathbf{a}$  is  $\mathbf{fa}_1 \cdots \mathbf{a}_n$ ,  $\mathcal{A}(\mathbf{a})$  is  $\mathbf{f}_{\mathcal{A}}(\mathcal{A}(\mathbf{a}_1), \dots, \mathcal{A}(\mathbf{a}_n))$ .

For each closed formula  $\mathbf{A}$  of  $L(\mathcal{A})$ :

- If  $\mathbf{A}$  is  $\mathbf{a} = \mathbf{b}$ ,  $\mathcal{A}(\mathbf{A}) = \mathbf{T}$  if and only if  $\mathcal{A}(\mathbf{a}) = \mathcal{A}(\mathbf{b})$ .
- If  $\mathbf{A}$  is  $\mathbf{pa}_1 \cdots \mathbf{a}_n$ , where  $\mathbf{p}$  is not  $=$ ,  $\mathcal{A}(\mathbf{A}) = \mathbf{T}$  if and only if  $\mathbf{p}_{\mathcal{A}}(\mathcal{A}(\mathbf{a}_1), \dots, \mathcal{A}(\mathbf{a}_n))$ .
- If  $\mathbf{A}$  is  $\neg \mathbf{B}$ ,  $\mathcal{A}(\mathbf{A})$  is  $H_{\neg}(\mathcal{A}(\mathbf{B}))$ .
- If  $\mathbf{A}$  is  $\forall \mathbf{B}\mathbf{C}$ ,  $\mathcal{A}(\mathbf{A})$  is  $H_{\forall}(\mathcal{A}(\mathbf{B}), \mathcal{A}(\mathbf{C}))$ .

- If  $\mathbf{A}$  is  $\exists \mathbf{x} \mathbf{B}$ ,  $\mathcal{A}(\mathbf{A}) = \mathbf{T}$  if and only if  $\mathcal{A}(\mathbf{B}_{\mathbf{x}}[\mathbf{i}]) = \mathbf{T}$  for some  $\mathbf{i}$  in  $L(\mathcal{A})$ .

If  $\mathbf{A}$  is a formula of  $L$ , an  $\mathcal{A}$ -instance of  $\mathbf{A}$  is a closed formula of the form  $\mathbf{A}[\mathbf{i}_1, \dots, \mathbf{i}_n]$  in  $L(\mathcal{A})$ . A formula  $\mathbf{A}$  is *valid* in  $\mathcal{A}$  if  $\mathcal{A}(\mathbf{A}') = \mathbf{T}$  for every  $\mathcal{A}$ -instance  $\mathbf{A}'$  of  $\mathbf{A}$ . A formula is *elementary* if it is either an atomic formula or an instantiation.

## 2.5 First-Order Theories

Main Idea: The primary object of a formal system is to provide a framework for proving theorems.

### 2.5.1 Definition

**Definition 2.5.1** (Formal System). A *formal system*  $F$  consists of a language  $L(F)$ , axioms of  $F$ , and rules of inference of  $F$  which enable us to conclude theorems from the axioms.

**Definition 2.5.2** (First-Order Theory). A *first-order theory*, or simply a *theory*, is a formal system  $T$  such that

- i) the language of  $T$  is a first-order language;
- ii) the axioms of  $T$  are the logical axioms of  $L(T)$  and certain further axioms called the *nonlogical axioms*;
- iii) the rules of  $T$  are the expansion rule, the contraction rule, the associative rule, the cut rule, and the  $\exists$ -introduction rule.

The logical axioms are the following:

- Propositional axiom:  $\neg \mathbf{A} \vee \mathbf{A}$
- Substitution axiom:  $\mathbf{A}_{\mathbf{x}}[\mathbf{a}] \rightarrow \exists \mathbf{x} \mathbf{A}$
- Identity axiom:  $\mathbf{x} = \mathbf{x}$
- Equality axiom:

$$\mathbf{x}_1 = \mathbf{y}_1 \rightarrow \cdots \rightarrow \mathbf{x}_n = \mathbf{y}_n \rightarrow \mathbf{f}\mathbf{x}_1 \dots \mathbf{x}_n = \mathbf{f}\mathbf{y}_1 \dots \mathbf{y}_n$$

or

$$\mathbf{x}_1 = \mathbf{y}_1 \rightarrow \cdots \rightarrow \mathbf{x}_n = \mathbf{y}_n \rightarrow \mathbf{p}\mathbf{x}_1 \dots \mathbf{x}_n = \mathbf{p}\mathbf{y}_1 \dots \mathbf{y}_n$$

The rules are the following:

- Expansion: Infer  $\mathbf{B} \vee \mathbf{A}$  from  $\mathbf{A}$ .
- Contraction: Infer  $\mathbf{A}$  from  $\mathbf{A} \vee \mathbf{A}$ .
- Associative: Infer  $(\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C}$  from  $\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})$ .
- Cut: Infer  $\mathbf{B} \vee \mathbf{C}$  from  $\mathbf{A} \vee \mathbf{B}$  and  $\neg \mathbf{A} \vee \mathbf{C}$ .
- $\exists$ -Introduction: If  $\mathbf{x}$  is not free in  $\mathbf{B}$ , infer  $\exists \mathbf{x} \mathbf{A} \rightarrow \mathbf{B}$  from  $\mathbf{A} \rightarrow \mathbf{B}$ .

## 2.5.2 Models of Theories

**Definition 2.5.3** (Model). A **model** of a theory  $T$  is a structure for  $L(T)$  in which all the nonlogical axioms of  $T$  are valid. A formula is **valid in  $T$**  if it is valid in every model of  $T$ ; equivalently, if it is a logical consequence of the nonlogical axioms of  $T$ .

**Example 2.5.2.1** (Elementary Theory of Groups,  $G$ ). The only nonlogical symbol of  $G$  is the binary function symbol  $\cdot$ . The nonlogical axioms of  $G$  are:

$$\text{G1. } (x \cdot y) \cdot z = x \cdot (y \cdot z).$$

$$\text{G2. } \exists x(\forall y(x \cdot y = y) \wedge \forall y \exists z(z \cdot y = x)).$$

A model of  $G$  would be the set of invertible  $2 \times 2$  matrices under matrix multiplication.

## 2.5.3 Definitions Relevant to Theories

- A theory  $T'$  is an **extension** of a theory  $T$  if  $L(T')$  is an extension of  $L(T)$  and every theorem of  $T$  is a theorem of  $T'$ . A **conservative extension** of  $T$  is an extension  $T'$  of  $T$  such that every formula of  $T$  which is a theorem of  $T'$  is also a theorem of  $T$ . The theories  $T$  and  $T'$  are **equivalent** if each is an extension of the other, i.e., they have the same language and the same theorems.
- A theory  $T$  is **inconsistent** if every formula of  $T$  is a theorem of  $T$ ; otherwise  $T$  is **consistent**.
- A formula  $\mathbf{A}$  of  $T$  is **undecidable** in  $T$  if neither  $\mathbf{A}$  nor  $\neg\mathbf{A}$  is a theorem of  $T$ ; otherwise  $\mathbf{A}$  is **decidable** in  $T$ .
- A theory is **complete** if it is consistent and if every closed formula in  $T$  is decidable in  $T$ .
- A theory is **open** if all of its nonlogical axioms are open (do not contain quantifiers).

## 2.5.4 Truth of Formulas of a Theory

**Definition 2.5.4** (Truth Valuation). A **truth valuation** for  $T$  is a mapping from the set of elementary formulas in  $T$  to the set of truth values.

We define a truth value  $V(\mathbf{A})$  for every formula  $\mathbf{A}$  by induction:

- If  $\mathbf{A}$  is elementary, then  $V(\mathbf{A})$  is already defined;
- If  $\mathbf{A}$  is  $\neg\mathbf{B}$ , then  $V(\mathbf{A}) = H_{\neg}(V(\mathbf{B}))$ ;
- If  $\mathbf{A}$  is  $\vee\mathbf{B}\mathbf{C}$ , then  $V(\mathbf{A}) = H_{\vee}(V(\mathbf{B}), V(\mathbf{C}))$ .

### 2.5.5 Theorems in First-Order Theories

**Theorem 2.5.1** (Validity Theorem). *If  $T$  is a theory, then every theorem of  $T$  is valid in  $T$ .*

## 2.6 The Characterization Problem

**Definition 2.6.1** (Characterization Problem). The *characterization problem* for a formal system  $F$  is the following: find a necessary and sufficient condition that a formula of  $F$  be a theorem of  $F$ .

Remark: We consider the characterization problem for theories.

### 2.6.1 The Reduction Theorem

Main Idea: To solve the characterization problem for all theories, it suffices to solve it for theories with no nonlogical axioms.

**Theorem 2.6.1** (Reduction Theorem). *Let  $\Gamma$  be a set of formulas in the theory  $T$ , and let  $A$  be a formula of  $T$ . Then  $A$  is a theorem of  $T[\Gamma]$  iff there is a theorem of  $T$  of the form  $B_1 \rightarrow \dots \rightarrow B_n \rightarrow A$ , where each  $B_i$  is the closure of a formula in  $\Gamma$ .*

**Theorem 2.6.2** (Reduction Theorem for Consistency). *Let  $\Gamma$  be a nonempty set of formulas in the theory  $T$ . Then  $T[\Gamma]$  is inconsistent iff there is a theorem of  $T$  which is a disjunction of negations of closures of distinct formulas in  $\Gamma$ .*

**Corollary 2.6.3.** *Let  $A'$  be the closure of  $A$ . Then  $A$  is a theorem of  $T$  iff  $T[\neg A']$  is inconsistent.*

### 2.6.2 Solutions to the Characterization Problem

A trivial solution is that a formula is a theorem if and only if it has a proof.

#### The Completeness Theorem

Main Idea: The completeness theorem, in either form, establishes an equivalence between a syntactical concept and a semantical concept. That is, it deals with concrete and abstract objects.

**Theorem 2.6.4** (Completeness Theorem, First Form (Gödel)). *A formula  $\mathbf{A}$  of a theory  $T$  is a theorem of  $T$  iff it is valid in  $T$ .*

**Theorem 2.6.5** (Completeness Theorem, Second Form). *A theory  $T$  is consistent iff it has a model.*

The second form is proved using the concept of Henkin theories and special constants. It is outlined below.

**Definition 2.6.2.** A Henkin theory is a theory such that each closed instantiation  $\exists \mathbf{x}\mathbf{A}$  of  $T$ , there is a constant  $\mathbf{e}$  such that  $\vdash_T \exists \mathbf{x}\mathbf{A} \rightarrow \mathbf{A}_{\mathbf{x}}[\mathbf{e}]$ .

One can extend any consistent theory to a Henkin theory by adding a special constant  $\mathbf{r} = c_{\exists \mathbf{x}\mathbf{A}}$  for every case where  $\exists \mathbf{x}\mathbf{A}$  is a theorem, yet there is no such  $\mathbf{e}$ . If  $\mathbf{r}$  is the special constant for  $\exists \mathbf{x}\mathbf{A}$ , then the formula  $\exists \mathbf{x}\mathbf{A} \rightarrow \mathbf{A}_{\mathbf{x}}[\mathbf{r}]$  is called the *special axiom for  $\mathbf{r}$* . One can then extend this theory to a complete Henkin theory, which one can prove has a model. After showing that a theory has a model if its extension has a model, one can conclude that the original theory has a model.

### The Consistency Theorem

Main Idea: The consistency theorem deals only with concrete objects and is therefore finitary. Say we have a model of an open theory. The completeness theorem gives a proof of the consistency of the theory. The consistency theorem then allows us to convert this into a finitary proof of the consistency of the theory.

We start with some necessary definitions.

- A theory is *open* if all of its nonlogical axioms are open (do not contain quantifiers).
- A formula is a *quasi-tautology* if it is a tautological consequence of instances of identity axioms and equality axioms.

**Theorem 2.6.6** (The Consistency Theorem (Hilbert-Ackermann)). *An open theory  $T$  is inconsistent if and only if there is a quasi-tautology which is a disjunction of negations of instances of non-logical axioms of  $T$ .*



**Herbrand's Theorem**

Main Idea: Herbrand's theorem is a finitary solution of the characterization problem for all theories.

**Theorem 2.6.7** (Herbrand's Theorem). *Let  $T$  be a theory with no nonlogical axioms, and let  $\mathbf{A}$  be a closed formula in prenex form in  $T$ . Then  $\mathbf{A}$  is a theorem of  $T$  if and only if there is a quasi-tautology which is a disjunction of instances of the matrix of  $\mathbf{A}_H$ .*

**2.7 Interpretations**

## Chapter 3

# Topology

The concept of topological space grew out of the study of the real line and euclidean space and the study of continuous functions on these spaces. The information in this chapter is based on the second edition of Munkres' *Topology* (2000).

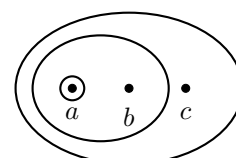
## 3.1 Topological Space

**Definition 3.1.1** (Topology/Open Set/Topological Space). A **topology** on a set  $X$  is a collection  $\mathcal{T}$  of subsets of  $X$  called **open sets** having the following properties:

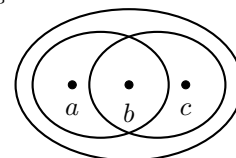
1.  $\emptyset$  and  $X$  are in  $\mathcal{T}$ .
2. The union of the elements of any subcollection of  $\mathcal{T}$  is in  $\mathcal{T}$ .
3. The intersection of the elements of any finite subcollection of  $\mathcal{T}$  is in  $\mathcal{T}$ .

A **topological space** is an ordered pair  $(X, \mathcal{T})$  consisting of a set  $X$  and a topology  $\mathcal{T}$  on  $X$ . We shorten the statement “ $U$  is an open set containing  $x$ ” to the phrase “ $U$  is a **neighborhood** of  $x$ .”

This is an extremely abstract definition, but the notion of open sets will lead to a definition of continuity: a generalization of the epsilon-delta definition from analysis. (See Section 3.7.) A given set will have more than one topology it can be equipped with.



(a) These subsets are a topology for  $X = \{a, b, c\}$ .



(b) These subsets are not a topology for  $X = \{a, b, c\}$ .

**Example 3.1.0.1.** If  $X$  is any set, the collection of all subsets of  $X$  is a topology on  $X$ ; it is called the **discrete topology**. The collection consisting of  $X$  and  $\emptyset$  only is also a topology on  $X$ ; it is called the **indiscrete topology**, or the **trivial topology**.

**Theorem 3.1.1.** Let  $X$  be a topological space. Then the following conditions hold:

- (1)  $\emptyset$  and  $X$  are closed.
- (2) Arbitrary intersections of closed sets are closed.
- (3) Finite unions of closed sets are closed.

A bijective correspondence which preserves the topological structure is called a homeomorphism. See section 3.8.

### 3.1.1 Comparing Topologies

- If  $\mathcal{T} \subseteq \mathcal{T}'$ , we say that  $\mathcal{T}'$  is **finer** than  $\mathcal{T}$ . If  $\mathcal{T} \subsetneq \mathcal{T}'$ , we say that  $\mathcal{T}'$  is **strictly finer** than  $\mathcal{T}$ . We also say that  $\mathcal{T}$

is (strictly) **coarser** than  $\mathcal{T}'$ .  $\mathcal{T}$  and  $\mathcal{T}'$  are **comparable** if  $\mathcal{T} \subseteq \mathcal{T}'$  or  $\mathcal{T}' \subseteq \mathcal{T}$ .

- The statement “ $\mathcal{T}'$  is finer than  $\mathcal{T}$ ” is equivalent to the statement “For each  $x \in X$  and each basis element  $B \in \mathcal{B}$  containing  $x$ , there is a basis element  $B' \in \mathcal{B}'$  such that  $x \in B' \subseteq B$ .”

### 3.1.2 Generating a Topology

**Definition 3.1.2** (Basis For a Topology). If  $X$  is a set, a **basis** for a topology on  $X$  is a collection  $\mathcal{B}$  of subsets of  $X$  (called **basis elements**) such that

- (1) For each  $x \in X$ , there is at least one basis element  $B$  containing  $x$ .
- (2) If  $x$  belongs to the intersection of two basis elements  $B_1$  and  $B_2$ , then there is a basis element  $B_3$  containing  $x$  such that  $B_3 \subseteq B_1 \cap B_2$ .

If  $\mathcal{B}$  satisfies these two conditions, we define the **topology  $\mathcal{T}$  generated by  $\mathcal{B}$**  as follows: A subset  $U$  of  $X$  is open in  $X$  if for each  $x \in U$ , there is a basis element  $B \in \mathcal{B}$  such that  $x \in B$  and  $B \subseteq U$ . Note that each basis element is itself an element of  $\mathcal{T}$ .

**Example 3.1.2.1.** If  $\mathcal{B}$  is the collection of all open intervals in the real line, the topology generated by  $\mathcal{B}$  is called the **standard topology** of the real line.

- Let  $X$  be a set; let  $\mathcal{B}$  be a basis for a topology  $\mathcal{T}$  on  $X$ . Then  $\mathcal{T}$  equals the collection of all unions of elements of  $\mathcal{B}$ . That is, every open set  $U$  in  $X$  can be expressed as a union of basis elements.
- We can obtain a basis for a given topology as follows: Gather a collection  $\mathcal{C}$  of open sets  $U$  of  $X$  such that for each  $x \in U$ , there is an element  $C$  of  $\mathcal{C}$  such that  $x \in C \subseteq U$ .  $\mathcal{C}$  is a basis for the topology of  $X$ .

A **subbasis**  $\mathcal{S}$  is a collection of subsets of  $X$  whose union equals  $X$ . The **topology generated by the subbasis  $\mathcal{S}$**  is defined to be the collection  $\mathcal{T}$  of all unions of finite intersections of elements of  $\mathcal{S}$ .

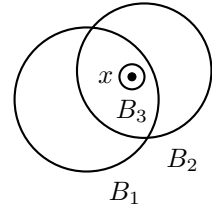


Figure 3.2: Illustration of condition (2) of Definition 3.1.2

## 3.2 Closed Sets

**Definition 3.2.1** (Closed Set). A subset  $A$  of a topological space  $X$  is said to be **closed** if the set  $X \setminus A$  is open.

A set can be both open and closed, one and not the other, or neither. There are analogous theorems/definitions for closed sets as for open sets, and these have been placed alongside the theorems/definitions for open sets.

**Definition 3.2.2** (Interior and Closure of Set). Given a subset  $A$  of a topological space, the **interior** of  $A$  is defined as the union of all open sets contained in  $A$ , and the **closure** of  $A$  is defined as the intersection of all closed sets containing  $A$ . The interior of  $A$  is denoted  $\text{Int } A$ , and the closure of  $A$  is denoted by  $\text{Cl } A$  or  $\bar{A}$ .

The main idea is that the closure of an open interval is a closed interval and the interior of a closed interval is an open interval.

- We have  $\text{Int } A \subseteq A \subseteq \bar{A}$ .
- If  $A$  is open,  $A = \text{Int } A$ ; while if  $A$  is closed,  $A = \bar{A}$ .

**Theorem 3.2.1.** Let  $A$  be a subset of the topological space  $X$ .

- Then  $x \in \bar{A}$  if and only if every neighborhood of  $x$  intersects  $A$ .
- Supposing the topology of  $X$  is given by a basis, then  $x \in \bar{A}$  if and only if every basis element  $B$  containing  $x$  intersects  $A$ .

Part (a) is illustrated in Figure 3.3.

**Definition 3.2.3** (Limit Point). If  $A$  is a subset of the topological space  $X$  and if  $x$  is a point of  $X$ , we say that  $x$  is a **limit point** of  $A$  if every neighborhood of  $x$  intersects  $A$  in some point other than  $x$  itself. Equivalently,  $x$  is a limit point of  $A$  if it belongs to the closure of  $A \setminus \{x\}$ .

The point  $x$  may lie in  $A$  or not.

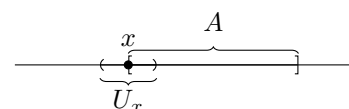


Figure 3.3: Any neighborhood of  $x$  intersects  $A$ , so  $x \in \bar{A}$ .

**Theorem 3.2.2.** *Let  $A$  be a subset of the topological space  $X$ ; let  $A'$  be the set of all limit points of  $A$ . Then*

$$\bar{A} = A \cup A'.$$

**Corollary 3.2.3.** *A subset of a topological space is closed if and only if it contains all its limit points.*

**Theorem 3.2.4.** *Let  $X$  be a space satisfying the  $T_1$  axiom; let  $A$  be a subset of  $X$ . Then the point  $x$  is a limit point of  $A$  if and only if every neighborhood of  $x$  contains infinitely many points of  $A$ .*

**Theorem 3.2.5.** *Let  $\{X_\alpha\}$  be an indexed family of spaces; let  $A_\alpha \subseteq X_\alpha$  for each  $\alpha$ . If  $\prod X_\alpha$  is given either the product or the box topology, then*

$$\prod \bar{A}_\alpha = \overline{\prod A_\alpha}.$$

## 3.3 Important Topologies

### 3.3.1 The Order Topology

**Definition 3.3.1** (Order Topology). Let  $X$  be a set with a simple order relation; assume  $X$  has more than one element. Let  $\mathcal{B}$  be the collection of all sets of the following types:

- (1) All open intervals  $(a, b)$  in  $X$ .
- (2) All intervals of the form  $[a_0, b)$ , where  $a_0$  is the smallest element (if any) of  $X$ .
- (3) All intervals of the form  $(a, b_0]$ , where  $b_0$  is the largest element (if any) of  $X$ .

The collection  $\mathcal{S}$  is a basis for a topology on  $X$  which is called the *order topology*.

**Example 3.3.1.1.** The standard topology on  $\mathbb{R}$  is just the order topology derived from the usual order on  $\mathbb{R}$ .

The collection

$$\mathcal{B} = \{(a, +\infty), (-\infty, b) \mid a, b \in X\}$$

forms a subbasis for the order topology on  $X$ .

### 3.3.2 The Box Topology

**Definition 3.3.2** (Box Topology). Let  $\{X_\alpha\}_{\alpha \in J}$  be an indexed family of topological spaces. Let us take as a basis for a topology on the product space

$$\prod_{\alpha \in J} X_\alpha$$

the collection of all sets of the form

$$\prod_{\alpha \in J} U_\alpha,$$

where  $U_\alpha$  is open in  $X_\alpha$  for each  $\alpha \in J$ . The topology generated by this basis is called the **box topology**.

Figure 3.4 illustrates that the second condition for a basis is met. We prefer the product topology over the box topology.

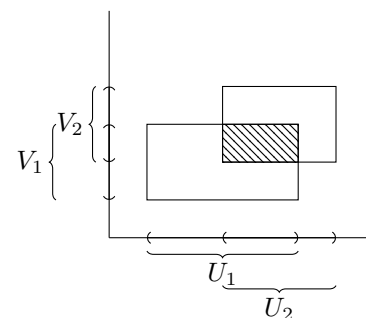


Figure 3.4: Condition 2 for a basis.

**Theorem 3.3.1.** Suppose the topology on each space  $X_\alpha$  is given by a basis  $\mathcal{B}_\alpha$ . The collection of all sets of the form  $\prod_{\alpha \in J} B_\alpha$ , where  $B_\alpha \in \mathcal{B}_\alpha$  for each  $\alpha$ , will serve as a basis for the box topology on  $\prod_{\alpha \in J} X_\alpha$ .

The box topology turns out to be less useful than the product topology, so that one will be used.



### 3.3.3 The Product Topology

**Definition 3.3.3** (Product Topology). Let  $\mathcal{S}_\beta$  denote the collection

$$\mathcal{S}_\beta = \{\pi_\beta^{-1}(U_\beta) \mid U_\beta \text{ is open in } X_\beta\},$$

and let  $\mathcal{S}$  denote the union of these collections,

$$\mathcal{S} = \bigcup_{\beta \in J} \mathcal{S}_\beta.$$

The topology generated by the subbasis  $\mathcal{S}$  is called the **product topology**. In this topology  $\prod_{\alpha \in J} X_\alpha$  is called a **product space**.

Figure 3.5 illustrates this definition.

A typical element of the basis generated by  $\mathcal{S}$  has the form

$$B = \pi_{\beta_1}^{-1}(U_{\beta_1}) \cap \pi_{\beta_2}^{-1}(U_{\beta_2}) \cap \cdots \cap \pi_{\beta_n}^{-1}(U_{\beta_n})$$

for distinct  $\beta_i$ , and therefore we have the following theorem.

**Theorem 3.3.2.** *The product topology on  $\prod X_\alpha$  has as basis all sets of the form  $\prod U_\alpha$ , where  $U_\alpha$  is open in  $X_\alpha$  for each  $\alpha$  and  $U_\alpha = X_\alpha$  except for finitely many values of  $\alpha$ .*

**Theorem 3.3.3.** *Suppose the topology on each space  $X_\alpha$  is given by a basis  $\mathcal{B}_\alpha$ . The collection of all sets of the form  $\prod_{\alpha \in J} B_\alpha$ , where  $B_\alpha \in \mathcal{B}_\alpha$  for finitely many indices  $\alpha$  and  $B_\alpha = X_\alpha$  for all the remaining indices, will serve as a basis for the product topology  $\prod_{\alpha \in J} X_\alpha$ .*

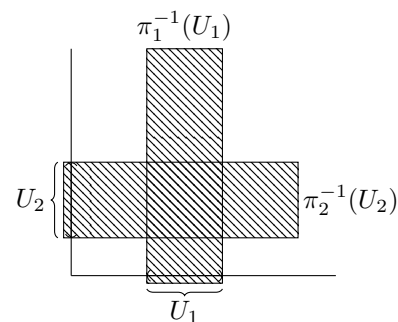


Figure 3.5: Illustration of the subbasis of the product topology for  $U_1 \times U_2$ .

### 3.3.4 The Subspace Topology

**Definition 3.3.4** (Subspace Topology). Let  $X$  be a topological space with topology  $\mathcal{T}$ . If  $Y$  is a subset of  $X$ , the collection

$$\mathcal{T}_Y = \{Y \cap U \mid U \in \mathcal{T}\}$$

is a topology on  $Y$ , called the **subspace topology**. With this topology,  $Y$  is called a **subspace** of  $X$ .

If  $\mathcal{B}$  is a basis for the topology of  $X$  then the collection

$$\mathcal{B}_Y = \{B \cap Y \mid B \in \mathcal{B}\}$$

is a basis for the subspace topology on  $Y$ .

**Theorem 3.3.4.** *Let  $Y$  be a subspace of  $X$ . Then a set  $A$  is closed in  $Y$  if and only if it equals the intersection of a closed set of  $X$  with  $Y$ .*

**Theorem 3.3.5.**

- *Let  $Y$  be a subspace of  $X$ . If  $U$  is open in  $Y$  and  $Y$  is open in  $X$ , then  $U$  is open in  $X$ .*
- *Let  $Y$  be a subspace of  $X$ . If  $A$  is closed in  $Y$  and  $Y$  is closed in  $X$ , then  $A$  is closed in  $X$ .*

**Theorem 3.3.6.** *Let  $Y$  be a subspace of  $X$ ; let  $A$  be a subset of  $Y$ ; let  $\bar{A}$  denote the closure of  $A$  in  $X$ . Then the closure of  $A$  in  $Y$  equals  $\bar{A} \cap Y$ .*

### 3.3.5 Metrics and The Metric Topology

**Main Idea:** A metric is a way to measure distance. The metric topology is the collection of open balls, a generalization of the open interval. It really belongs to the field of analysis rather than topology.

**Definition 3.3.5** (Metric). A **metric** on a set  $X$  is a function  $d : X \times X \rightarrow \mathbb{R}$  having the following properties:

1.  $d(x, y) \geq 0$  for all  $x, y \in X$ ; equality holds if and only if  $x = y$ .
2.  $d(x, y) = d(y, x)$  for all  $x, y \in X$ .
3. (Triangle Inequality)  $d(x, y) + d(y, z) \geq d(x, z)$ , for all  $x, y, z \in X$ .

**Definition 3.3.6** ( $\epsilon$ -Ball). Given a metric  $d$  on  $X$ , the number  $d(x, y)$  is often called the **distance** between  $x$  and  $y$  in the metric  $d$ . Given  $\epsilon > 0$ , consider the set

$$B_d(x, \epsilon) = \{y \mid d(x, y) < \epsilon\}$$

of all points  $y$  whose distance from  $x$  is less than  $\epsilon$ . It is called the  **$\epsilon$ -ball centered at  $x$** .

**Definition 3.3.7** (Metric Topology). If  $d$  is a metric on the set  $X$ , then the collection of all  $\epsilon$ -balls  $B_d(x, \epsilon)$ , for  $x \in X$  and  $\epsilon > 0$ , is a basis for a topology on  $X$ , called the **metric topology** induced by  $d$ .

A set  $U$  is open in the metric topology induced by  $d$  if and only if for each  $y \in U$ , there is a  $\delta > 0$  such that  $B_d(y, \delta) \subseteq U$ .

#### Relevant Definitions

- If  $X$  is a topological space,  $X$  is said to be **metrizable** if there exists a metric  $d$  on the set  $X$  which induces the topology of  $X$ . A **metric space** is a metrizable space  $X$  together with a specific metric  $d$  that gives the topology of  $X$ .
- Let  $X$  be a metric space with metric  $d$ . A subset  $A$  of  $X$  is said to be **bounded** if there is some number  $M$  such that

$$d(a_1, a_2) \leq M$$

for every pair  $a_1, a_2$  of points of  $A$ . If  $A$  is bounded and nonempty, the **diameter** of  $A$  is defined to be the number

$$\text{diam } A = \sup\{d(a_1, a_2) \mid a_1, a_2 \in A\}.$$

- Given  $\mathbf{x} = (x_1, \dots, x_n)$  in  $\mathbb{R}^n$ , we define the **norm** of  $\mathbf{x}$  by the equation

$$\|\mathbf{x}\| = (x_1^2 + \dots + x_n^2)^{1/2}.$$

Remark: Metrizability is always a highly desirable attribute for a space to possess, for the existence of a metric gives one a valuable tool for proving theorems about the space. Though Metrizability is a topological property, properties that involve a specific metric for  $X$  in general do not.

$\mathbb{R}^\omega$  equipped with the metric topology is metrizable:

**Theorem 3.3.7.** Let  $\bar{d}(a, b) = \min\{|a - b|, 1\}$  be the standard bounded metric on  $\mathbb{R}$ . If  $\mathbf{x}$  and  $\mathbf{y}$  are two points of  $\mathbb{R}^\omega$ , define

$$D(\mathbf{x}, \mathbf{y}) = \sup \left\{ \frac{\bar{d}(x_i, y_i)}{i} \right\}.$$

Then  $D$  is a metric that induces the product topology on  $\mathbb{R}^\omega$ .

### Important Metrics

- The standard metric on the real numbers  $\mathbb{R}$  is defined by the equation  $d(x, y) = |x - y|$ . It induces the order topology. Thus,  $\mathbb{R}$  with the standard topology is metrizable, and  $\mathbb{R}$  with the standard topology and the standard metric form a metric space. In fact  $\mathbb{R}^n$  and  $\mathbb{R}^\omega$  are metrizable.
- Let  $X$  be a metric space with metric  $d$ . Define  $\bar{d} : X \times X \rightarrow \mathbb{R}$  by the equation  $\bar{d}(x, y) = \min\{d(x, y), 1\}$ .  $\bar{d}$  is called the **standard bounded metric** corresponding to  $d$ , and induces the same topology as  $d$ .
- We define the **euclidean metric**  $d$  on  $\mathbb{R}^n$  by the equation

$$d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\| = [(x_1 - y_1)^2 + \dots + (x_n - y_n)^2]^{1/2}.$$

$d$  induces the product topology on  $\mathbb{R}^n$ . In  $\mathbb{R}^2$ , the basis elements under  $d$  can be pictured as circular regions.

- We define the **square metric**  $\rho$  by the equation

$$\rho(\mathbf{x}, \mathbf{y}) = \max\{|x_1 - y_1|, \dots, |x_n - y_n|\}.$$

$\rho$  induces the product topology on  $\mathbb{R}^n$ . In  $\mathbb{R}^2$ , the basis elements under  $\rho$  can be pictured as square regions.

- Given an index set  $J$ , and given points  $\mathbf{x} = (x_\alpha)_{\alpha \in J}$  and  $\mathbf{y} = (y_\alpha)_{\alpha \in J}$  of  $\mathbb{R}^J$ , let us define a metric  $\bar{\rho}$  on  $\mathbb{R}^J$  by the equation

$$\bar{\rho}(\mathbf{x}, \mathbf{y}) = \sup\{\bar{d}(x_\alpha, y_\alpha) \mid \alpha \in J\},$$

where  $\bar{d}$  is the standard bounded metric on  $\mathbb{R}$ .  $\bar{\rho}$  is called the ***uniform metric*** on  $\mathbb{R}^J$ , and the topology it induces is called the ***uniform topology***.

### 3.3.6 Relationships Between Important Topologies

The box and product topologies are equivalent when acting on a finite Cartesian product, but not on an arbitrary Cartesian product. We prefer the product topology.

**Theorem 3.3.8.** *Let  $A_\alpha$  be a subspace of  $X_\alpha$  for each  $\alpha \in J$ . Then  $\prod A_\alpha$  is a subspace of  $\prod X_\alpha$  if both products are given the box topology, or if both products are given the product topology.*

Let  $X$  be an ordered set in the order topology, and let  $Y$  be a subset of  $X$ . The order relation on  $X$ , when restricted to  $Y$ , makes  $Y$  into an ordered set. However, the resulting order topology on  $Y$  need not be the same as the topology that  $Y$  inherits as a subspace of  $X$ . The following theorem tells us when they are the same, but we need a definition first.

**Definition 3.3.8** (Convex). Given an ordered set  $X$ , let us say that a subset  $Y$  of  $X$  is **convex** in  $X$  if for each pair of points  $a < b$  of  $Y$ , the entire interval  $(a, b)$  of points of  $X$  lies in  $Y$ .

**Theorem 3.3.9.** *Let  $X$  be an ordered set in the order topology; let  $Y$  be a subset of  $X$  that is convex in  $X$ . Then the order topology on  $Y$  is the same as the topology  $Y$  inherits as a subspace of  $X$ .*

**Theorem 3.3.10.** *The uniform topology on  $\mathbb{R}^J$  is finer than the product topology and coarser than the box topology; these three topologies are all different if  $J$  is infinite.*

### 3.4 Hausdorff Spaces

Topological spaces in which one-point sets are not closed are strange and rare in other branches of mathematics. Therefore, we usually consider a class of spaces called Hausdorff spaces, which exclude such cases.

**Definition 3.4.1** (Hausdorff Space). A topological space  $X$  is called a **Hausdorff space** if for each pair  $x_1, x_2$  of distinct points of  $X$ , there exist neighborhoods  $U_1$  and  $U_2$  of  $x_1$  and  $x_2$ , respectively, that are disjoint.

Figure 3.6 illustrates the notion of a Hausdorff space using  $\mathbb{R}$  as an example. Given  $x_1$  and  $x_2$ , it is always possible to find such a  $U_1$  and  $U_2$ . Note that a different topology on  $\mathbb{R}$  (for example the finite complement topology) may not be Hausdorff.

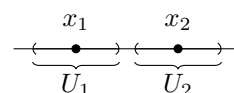


Figure 3.6: The real line equipped with the standard topology is Hausdorff.

**Theorem 3.4.1.** *Every finite point set in a Hausdorff space  $X$  is closed.*

The Hausdorff condition is stronger than the condition that finite point sets be closed, which is called the  $T_1$  axiom. See Section 3.6.

**Theorem 3.4.2.** *Every simply ordered set is a Hausdorff space in the order topology. If each space  $X_\alpha$  is a Hausdorff space, then  $\prod X_\alpha$  is a Hausdorff space in both the box and product topologies. A subspace of a Hausdorff space is a Hausdorff space.*

### 3.5 Sequences (Topology)

**Definition 3.5.1** (Convergence of a Sequence). Let  $X$  be a topological space. A sequence  $x_1, x_2, \dots$  of points in  $X$  **converges** to the point  $x$  of  $X$  provided that, corresponding to each neighborhood  $U$  of  $x$ , there is a positive integer  $N$  such that  $x_n \in U$  for all  $n \geq N$ . If the sequence  $x_n$  of points of the Hausdorff space  $X$  converges to the point  $x$  of  $X$ , we often write  $x_n \rightarrow x$ , and we say that  $x$  is the **limit** of the sequence  $x_n$ .

Note that if any neighborhood of  $x$  contains all but a finite number of points of the sequence, then there must necessarily be some  $N$  such that  $x_n$  belongs to the neighborhood for  $n \geq N$ . Figure 3.7 illustrates this view.

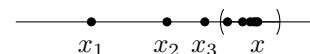


Figure 3.7: Any neighborhood of  $x$  contains all but a finite number of points of the sequence  $x_n$  and so is a limit of the sequence  $x_n$ .

**Theorem 3.5.1.** *If  $X$  is a Hausdorff space, then a sequence of points of  $X$  converges to at most one point of  $X$ .*



### 3.6 $T_i$ Axioms

**Definition 3.6.1** ( $T_i$  Axioms).

- The condition that finite point sets be closed is called the  $T_1$  *axiom*.

The  $T_1$  axiom is too weak to prove many of the interesting theorems of topology, so we rely on the Hausdorff condition.

## 3.7 Continuous Function

**Definition 3.7.1** (Continuous Function). Let  $X$  and  $Y$  be topological spaces. A function  $f : X \rightarrow Y$  is said to be **continuous** if for each open subset  $V$  of  $Y$ , the set  $f^{-1}(V)$  is an open subset of  $X$ .

In  $\mathbb{R}$ , this definition is equivalent to the epsilon-delta definition of the continuity of a function; however, the topological definition includes other spaces and situations as well.

### 3.7.1 Demonstrating a Function Is Continuous

- If the topology of the range space  $Y$  is given by a basis  $\mathcal{B}$ , then to prove continuity of  $f$  it suffices to show that the inverse image of every basis element is open.
- If the topology on  $Y$  is given by a subbasis  $\mathcal{S}$ , to prove continuity of  $f$  it suffices to show that the inverse image of each subbasis element is open.
- $f : X \rightarrow Y$  is continuous if and only if for every subset  $A$  of  $X$ , one has  $f(\bar{A}) \subseteq \overline{f(A)}$ .
- $f : X \rightarrow Y$  is continuous if and only if for every closed set  $B$  of  $Y$ , the set  $f^{-1}(B)$  is closed in  $X$ .
- $f : X \rightarrow Y$  is continuous if and only if for each  $x \in X$  and each neighborhood  $V$  of  $f(x)$ , there is a neighborhood  $U$  of  $x$  such that  $f(U) \subseteq V$ . If this condition holds for the point  $x$  of  $X$ , we say that  $f$  is **continuous at the point  $x$** .

### 3.7.2 Constructing Continuous Functions

Let  $X$ ,  $Y$ , and  $Z$  be topological spaces.

- (Constant function) If  $f : X \rightarrow Y$  maps all of  $X$  into a single point  $y_0$  of  $Y$ , then  $f$  is continuous.
- (Inclusion) If  $A$  is a subspace of  $X$ , the inclusion function  $j : A \rightarrow X$  is continuous.
- (Composites) If  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$  are continuous, then the map  $g \circ f : X \rightarrow Z$  is continuous.
- (Restricting the domain) If  $f : X \rightarrow Y$  is continuous, and if  $A$  is a subspace of  $X$ , then the restricted function  $f|_A : A \rightarrow Y$  is continuous.

- (Restricting or expanding the range) Let  $f : X \rightarrow Y$  be continuous. If  $Z$  is a subspace of  $Y$  containing the image set  $f(X)$ , then the function  $g : X \rightarrow Z$  obtained by restricting the range of  $f$  is continuous. If  $Z$  is a space having  $Y$  as a subspace, then the function  $h : X \rightarrow Z$  obtained by expanding the range of  $f$  is continuous.
- (Local formulation of continuity) The map  $f : X \rightarrow Y$  is continuous if  $X$  can be written as the union of open sets  $U_\alpha$  such that  $f|_{U_\alpha}$  is continuous for each  $\alpha$ .

**Theorem 3.7.1** (The Pasting Lemma). *Let  $X = A \cup B$ , where  $A$  and  $B$  are closed in  $X$ . Let  $f : A \rightarrow Y$  and  $g : B \rightarrow Y$  be continuous. If  $f(x) = g(x)$  for every  $x \in A \cap B$ , then  $f$  and  $g$  combine to give a continuous function  $h : X \rightarrow Y$ , defined by setting  $h(x) = f(x)$  if  $x \in A$ , and  $h(x) = g(x)$  if  $x \in B$ .*

Remark: This theorem also holds if  $A$  and  $B$  are open sets in  $X$ ; this is just a special case of the “local formulation of continuity” rule.

**Theorem 3.7.2** (Maps Into Products). *Let  $f : A \rightarrow \prod_{\alpha \in J} X_\alpha$  be given by the equation  $f(a) = (f_\alpha(a))_{\alpha \in J}$ , where  $f_\alpha : A \rightarrow X_\alpha$  for each  $\alpha$ . Let  $\prod X_\alpha$  have the product topology. Then the function  $f$  is continuous if and only if each function  $f_\alpha$  is continuous.*

Remark: The maps  $f_1$  and  $f_2$  are called the **coordinate functions** of  $f$ . Moreover, this theorem doesn’t hold if one uses the box topology, which is one reason we prefer the product topology.

### 3.8 Homeomorphisms

**Definition 3.8.1** (Homeomorphism). Let  $X$  and  $Y$  be topological spaces; let  $f : X \rightarrow Y$  be a bijection. If both the function  $f$  and the inverse function  $f^{-1} : Y \rightarrow X$  are continuous, then  $f$  is called a **homeomorphism**.

What this really means is that  $f$  is a homeomorphism if it is a bijective correspondence between the collections of open sets of  $X$  and of  $Y$ . Thus, a homeomorphism is a bijective correspondence that preserves the topological structure involved.

**Definition 3.8.2** (Topological Imbedding). Suppose  $f : X \rightarrow Y$  is an injective continuous map. Let  $Z$  be the image set  $f(X)$ , considered as a subspace of  $Y$ ; then the function  $f' : X \rightarrow Z$  obtained by restricting the range of  $f$  is bijective. If  $f'$  happens to be a homeomorphism of  $X$  with  $Z$ , we say that the map  $f : X \rightarrow Y$  is a **topological imbedding** of  $X$  in  $Y$ .

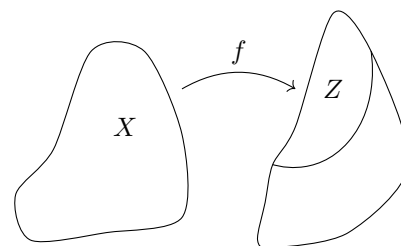


Figure 3.8: If  $f' : X \rightarrow Z$  is a homeomorphism of  $X$  with  $Z$ , then  $f'$  is a topological imbedding of  $X$  in  $Y$ .

Figure 3.8 illustrates this definition. Intuitively, the imbedding lets us treat  $X$  as a subspace of  $Y$  even though  $X$  isn't a subset of  $Y$ .

## Chapter 4

# Analysis

## Chapter 5

# Group Theory

Abstract algebra is, as its name suggests, extremely abstract. It arose as an attempt to abstract the techniques used in algebraic equations, number theory, and geometry. There are many specific examples of groups, and the power of the abstract point of view becomes apparent when results for all of these examples are obtained by providing a single result for the abstract group. The information in this chapter is based on Dummit and Foote's *Abstract Algebra* (2004).

## 5.1 Notation

- We write  $ab$  for  $a \cdot b$ .
- We denote the identity element of an abstract group  $(G, \cdot)$  by 1.
- We denote  $xx \dots x$  ( $n$  terms) by  $x^n$  and  $x^{-1}x^{-1} \dots x^{-1}$  ( $n$  terms) by  $x^{-n}$ .
- When the operation is  $+$ , the identity will be denoted by 0, and for any element  $a$ , the inverse will be written  $-a$ . Moreover,  $a + \dots + a$  ( $n > 0$  terms) will be written  $na$ ;  $-a - a \dots - a$  ( $n$  terms) will be written  $-na$  and  $0a = 0$ .
- For each  $n \in \mathbb{Z}^+$  let  $GL_n(F)$  be the set of all  $n \times n$  matrices whose entries come from  $F$  and whose determinant is nonzero.

## 5.2 Definition and Examples

**Definition 5.2.1** (Binary Operation).

1. A **binary operation**  $\cdot$  on a set  $G$  is a function  $\cdot : G \times G \rightarrow G$ . For any  $a, b \in G$  we write  $a \cdot b$ .
2. A binary operation  $\cdot$  on a set  $G$  is **associative** if for all  $a, b, c \in G$  we have  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ .
3. If  $\cdot$  is a binary operation on a set  $G$  we say elements  $a$  and  $b$  of  $G$  **commute** if  $a \cdot b = b \cdot a$ . We say  $\cdot$  (or  $G$ ) is **commutative** if for all  $a, b \in G$ ,  $a \cdot b = b \cdot a$ .
4. Suppose that  $\cdot$  is a binary operation on a set  $G$  and  $H$  is a subset of  $G$ . If the restriction of  $\cdot$  to  $H$  is a binary operation on  $H$ , i.e., for all  $a, b \in H$ ,  $a \cdot b \in H$ , then  $H$  is said to be **closed** under  $\cdot$ .

**Definition 5.2.2** (Group).

1. A **group** is an ordered pair  $(G, \cdot)$  where  $G$  is a set and  $\cdot$  is a binary operation on  $G$  satisfying the following axioms:
  - (a)  $\cdot$  is associative,
  - (b) there exists an element  $e$  in  $G$ , called an **identity** of  $G$ , such that for all  $a \in G$  we have  $a \cdot e = e \cdot a = a$ ,
  - (c) for each  $a \in G$  there is an element  $a^{-1}$  of  $G$ , called an **inverse** of  $a$ , such that  $a \cdot a^{-1} = a^{-1} \cdot a = e$ .
2. The group  $(G, \cdot)$  is called **abelian** (or **commutative**) if  $a \cdot b = b \cdot a$  for all  $a, b \in G$ .

Remark: We say  $(G, \cdot)$  is a **finite group** if in addition  $G$  is a finite set.

**Example 5.2.0.1.**

- $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$  are groups under  $+$  with  $e = 0$  and  $a^{-1} = -a$ , for all  $a$ .
- $\mathbb{Q} \setminus \{0\}$ ,  $\mathbb{R} \setminus \{0\}$ ,  $\mathbb{C} \setminus \{0\}$ ,  $\mathbb{Q}^+$ ,  $\mathbb{R}^+$  are groups under  $\times$  with  $e = 1$  and  $a^{-1} = \frac{1}{a}$ , for all  $a$ .



### 5.3 How to Form New Groups From Given Ones

- If  $(A, \cdot)$  and  $(B, *)$  are groups, we can form a new group  $(A \times B, \diamond)$ , called their **direct product**, whose elements are those in the Cartesian product  $A \times B$  and whose operation is defined componentwise:

$$(a_1, b_1)(a_2, b_2) = (a_1 \cdot a_2, b_1 * b_2).$$

**Example 5.3.0.1.** If we take  $A = B = \mathbb{R}$  (both operations addition),  $\mathbb{R} \times \mathbb{R}$  is the familiar Euclidean plane.

- Let  $G$  be a group. The subset  $H$  of  $G$  is a **subgroup** of  $G$  if  $H$  is nonempty and  $H$  is closed under products and inverses. If  $H$  is a subgroup of  $G$  we shall write  $H \leq G$ .

Remark: Subgroups of  $G$  are just subsets of  $G$  which are themselves groups with respect to the operation defined in  $G$ .

## 5.4 Basic Theorems About Groups

**Theorem 5.4.1** (Uniqueness of Identity and Inverse). *If  $(G, \cdot)$  is a group, then*

1. *the identity of  $(G, \cdot)$  is unique*
2. *for each  $a \in G$ ,  $a^{-1}$  is uniquely determined*
3.  *$(a^{-1})^{-1} = a$  for all  $a \in G$*
4.  *$(a \cdot b)^{-1} = (b^{-1}) \cdot (a^{-1})$*
5. *for any  $a_1, a_2, \dots, a_n \in G$  the value of  $a_1 \cdot a_2 \cdot \dots \cdot a_n$  is independent of how the expression is bracketed (this is called the **generalized associative law**).*

**Theorem 5.4.2** (Cancellation Laws). *Let  $(G, \cdot)$  be a group and let  $a, b \in G$ . The equations  $ax = b$  and  $ya = b$  have unique solutions for  $x, y \in G$ . In particular, the left and right cancellation laws hold in  $G$ , i.e.,*

1. *if  $au = av$ , then  $u = v$ , and*
2. *if  $ub = vb$ , then  $u = v$ .*

## 5.5 Order of An Element of A Group

**Definition 5.5.1.** For  $G$  a group and  $x \in G$ , the **order** of  $x$  is the smallest positive integer  $n$  such that  $x^n = 1$ . We denote this integer by  $|x|$ . In this case  $x$  is said to be of order  $n$ . If no positive power of  $x$  is the identity, the order of  $x$  is defined to be infinity and  $x$  is said to be of infinite order.

Remark: The order of an element in a group is the same as the cardinality of the set of all its distinct powers, which is why we use the same notation as cardinality.

**Example 5.5.0.1.**

- An element of a group has order 1 if and only if it is the identity.
- In the multiplicative groups  $\mathbb{R} \setminus \{0\}$  or  $\mathbb{Q} \setminus \{0\}$  the element  $-1$  has order 2 and all other nonidentity elements have infinite order.

## 5.6 Multiplication Table

**Definition 5.6.1** (Multiplication/Group Table). Let  $G = \{g_1, g_2, \dots, g_n\}$  be a finite group with  $g_1 = 1$ . The **multiplication table** or **group table** of  $G$  is the  $n \times n$  matrix whose  $i, j$  entry is the group element  $g_i g_j$ .

Remark: “For a finite group the multiplication table contains, in some sense, all the information about the group. Computationally, however, it is an unwieldy object (being of size the square of the group order) and visually it is not a very useful object for determining properties of the group. ... Part of our initial development of the theory of groups (finite groups in particular) is directed towards a more conceptual way of visualizing the internal structure of groups.”

## 5.7 Generators and Relations

**Definition 5.7.1** (Generators). A subset  $S$  of elements of a group  $G$  with the property that every element of  $G$  can be written as a (finite) product of elements of  $S$  and their inverses is called a set of **generators** of  $G$ . We write  $G = \langle S \rangle$  and say  $G$  is generated by  $S$  or  $S$  generates  $G$ .

**Example 5.7.0.1.**

- The integer 1 is a generator for the additive group  $\mathbb{Z}$  of integers since every integer is a sum of a finite number of  $+1$ 's and  $-1$ 's, so  $\mathbb{Z} = \langle 1 \rangle$ .
- As defined in Section 5.8.1,  $D_{2n} = \langle r, s \rangle$ .

**Definition 5.7.2.** Any equations in a general group  $G$  that the generators satisfy are called the **relations** in  $G$ .

**Example 5.7.0.2.** In  $D_{2n}$  we have the relations  $r^n = 1$ ,  $s^2 = 1$ , and  $rs = sr^{-1}$ .

If some group  $G$  is generated by a subset  $S$  and there is some collection of relations, say  $R_1, R_2, \dots, R_m$  (here each  $R_i$  is an equation in the elements from  $S \cup \{1\}$ ) such that any relation among the elements of  $S$  can be deduced from these, we shall call these generators and relations a **presentation** of  $G$  and write

$$G = \langle S \mid R_1, R_2, \dots, R_m \rangle.$$

For example,  $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$  is one presentation of the dihedral group  $D_{2n}$ . Working in terms of presentations often simplifies the situation.

## 5.8 Important Groups

### 5.8.1 Dihedral Groups

Main Idea: An important family of examples of groups is the class of groups whose elements are symmetries of geometric objects.

We rigorously define the symmetries of a regular  $n$ -gon. Label each vertex with a distinct integer  $i$  for  $1 \leq i \leq n$ . Each symmetry  $s$  can be described uniquely by the corresponding permutation  $\sigma$  of  $\{1, 2, 3, \dots, n\}$  where if the symmetry  $s$  puts vertex  $i$  in the place where vertex  $j$  was originally, then  $\sigma$  is the permutation sending  $i$  to  $j$ . There are  $n$  rotation symmetries and  $n$  reflection symmetries.

**Definition 5.8.1** (Dihedral Group). The set of symmetries  $s$  of a regular  $n$ -gon, together with the binary operation of composition form a group called the *dihedral group of order  $2n$* .

#### Notation

- Let  $r$  be the rotation clockwise about the origin through  $2\pi/n$  radian.
- Let  $s$  be the reflection about the line of symmetry through vertex 1 and the origin.

#### Theorems About Dihedral Groups

##### Theorem 5.8.1.

1.  $1, r, r^2, \dots, r^{n-1}$  are distinct and  $r^n = 1$ , so  $|r| = n$ .

2.  $|s| = 2$ .

3.  $s \neq r^i$  for any  $i$ .

4.  $sr^i \neq sr^j$ , for all  $0 \leq i, j \leq n-1$  with  $i \neq j$ , so

$$D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}.$$

5.  $rs = sr^{-1}$ . This shows in particular that  $r$  and  $s$  do not commute so that  $D_{2n}$  is non-abelian.

6.  $r^i s = sr^{-i}$ , for all  $0 \leq i \leq n$ . This indicates how to commute  $s$  with powers of  $r$ .

$r$  and  $s$  are called *generators* for the dihedral group. (See Section 5.7.)

## 5.8.2 Symmetric Groups

**Definition 5.8.2** (Symmetric Group). Let  $\Omega$  be any nonempty set and let  $S_\Omega$  be the set of all bijections from  $\Omega$  to itself (i.e., the set of all permutations of  $\Omega$ ). The set  $S_\Omega$  is a group under function composition ( $\circ$ ) called the *symmetric group on the set  $\Omega$* .

Remark: In the special case when  $\Omega = \{1, 2, 3, \dots, n\}$ , the symmetric group on  $\Omega$  is denoted  $S_n$ , the *symmetric group of degree  $n$* .

### Cycle Decomposition

**Definition 5.8.3** (Cycle). A *cycle* is a string of integers which represents the elements of  $S_n$  which cyclically permutes these integers (and fixes all other integers). The cycle  $(a_1 a_2 \dots a_m)$  is the permutation which sends  $a_i$  to  $a_{i+1}$ ,  $1 \leq i \leq m-1$  and sends  $a_m$  to  $a_1$ .

**Example 5.8.2.1.** The cycle  $(2\ 1\ 3)$  is the permutation which maps 2 to 1, 1 to 3, and 3 to 2.

Remark: Disjoint cycles commute.

For each  $\sigma \in S_n$  the numbers from 1 to  $n$  will be rearranged and grouped into  $k$  cycles of the form

$$(a_1 a_2 \dots a_{m_1})(a_{m_1+1} a_{m_1+2} \dots a_{m_2}) \dots (a_{m_{k-1}+1} a_{m_{k-1}+2} \dots a_{m_k})$$

from which the action of  $\sigma$  on any number from 1 to  $n$  can easily be read. The product of these cycles is called the *cycle decomposition* of  $\sigma$ .

### Theorems About Symmetric Groups

- The order of  $S_n$  is  $n!$ .
- $S_n$  is a non-abelian group for all  $n \geq 3$ .
- The cycle decomposition of each permutation is the unique way of expressing a permutation as a product of disjoint cycles (up to rearranging its cycles and cyclically permuting the numbers within each cycle).
- The order of a permutation is the l.c.m. of the lengths of the cycles in its cycle decomposition.

### 5.8.3 Matrix Groups

**Definition 5.8.4** (General Linear Group).  $GL_n(F)$ , that is the set of all  $n \times n$  matrices whose entries come from a field  $F$  and whose determinant is nonzero, form a group under matrix multiplication called the *general linear group of degree  $n$* .

#### Theorems About Matrix Groups

- If  $F$  is a field and  $|F| < \infty$ , then  $|F| = p^m$  for some prime  $p$  and integer  $m$ .
- If  $|F| = q < \infty$ , then  $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1})$ .



### 5.8.4 The Quaternion Group

**Definition 5.8.5** (Quaternion Group). The *quaternion group*,  $Q_8$ , is defined by

$$\{1, -1, i, -i, j, -j, k, -k\}$$

with product  $\cdot$  computed as follows:

$$\begin{aligned} 1 \cdot a &= a \cdot 1 = a, & \text{for all } a \in Q_8 \\ (-1) \cdot (-1) &= 1, & (-1) \cdot a = a \cdot (-1) = -a, & \text{for all } a \in Q_8 \\ i \cdot i &= j \cdot j = k \cdot k = -1 \\ i \cdot j &= k, & j \cdot i &= -k \\ j \cdot k &= i, & k \cdot j &= -i \\ k \cdot i &= j, & i \cdot k &= -j. \end{aligned}$$

Remark:  $Q_8$  is a non-abelian group of order 8.

#### Theorems About the Quaternion Group

## 5.9 Homomorphisms and Isomorphisms

Main Idea: A map is a homomorphism if it respects the group structures of its domain and codomain. The notion of isomorphism makes precise the idea of when two groups “look the same,” that is, have exactly the same group-theoretic structure.

**Definition 5.9.1** (Homomorphism). Let  $(G, \cdot)$  and  $(H, *)$  be groups. A map  $\varphi : G \rightarrow H$  such that

$$\varphi(x \cdot y) = \varphi(x) * \varphi(y), \quad \text{for all } x, y \in G$$

is called a *homomorphism*.

**Definition 5.9.2** (Isomorphism). The map  $\varphi : G \rightarrow H$  is called an *isomorphism* and  $G$  and  $H$  are said to be *isomorphic* or of the same *isomorphism type*, written  $G \cong H$ , if

1.  $\varphi$  is a homomorphism, and
2.  $\varphi$  is a bijection.

### Theorems About Isomorphisms

- The relation  $\cong$  is an equivalence relation, the equivalence classes of which are called *isomorphism classes*.
- If  $\varphi : G \rightarrow H$  is an isomorphism, then
  1.  $|G| = |H|$
  2.  $G$  is abelian if and only if  $H$  is abelian
  3. for all  $x \in G$ ,  $|x| = |\varphi(x)|$ .
- Let  $G$  be a finite group of order  $n$  for which we have a presentation and let  $S = \{s_1, \dots, s_m\}$  be the generators. Let  $H$  be another group and  $\{r_1, \dots, r_m\}$  be the elements of  $H$ . Suppose that any relation satisfied in  $G$  by the  $s_i$  is also satisfied in  $H$  when each  $s_i$  is replaced by  $r_i$ . Then there is a unique homomorphism  $\varphi : G \rightarrow H$  which maps  $s_i$  to  $r_i$ .

## 5.10 Group Actions

**Main Idea:** A group action is when a group acts on a set. Intuitively, a group action of  $G$  on a set  $A$  just means that every element  $g$  in  $G$  acts as a permutation on  $A$  in a manner consistent with the group operations in  $G$ .

**Definition 5.10.1** (Group Action). A **group action** of a group  $G$  on a set  $A$  is a map from  $G \times A$  to  $A$  (written as  $g \cdot a$ , for all  $g \in G$  and  $a \in A$ ) satisfying the following properties:

1.  $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ , for all  $g_1, g_2 \in G$ ,  $a \in A$ , and
2.  $1 \cdot a = a$ , for all  $a \in A$ .

For each fixed  $g \in G$  we get a map  $\sigma_g$  defined by

$$\begin{aligned}\sigma_g : A &\rightarrow A \\ \sigma_g(a) &= g \cdot a,\end{aligned}$$

where  $\sigma_g$  is a permutation of  $A$  and the map from  $G$  to  $S_A$  defined by  $g \mapsto \sigma_g$  is a homomorphism. This homomorphism is called the **permutation representation** associated to the given action.

If  $G$  acts on a set  $B$  and distinct elements of  $G$  induce distinct permutations of  $B$ , the action is said to be **faithful**.

The **kernel** of the action of  $G$  on  $B$  is defined to be  $\{g \in G \mid gb = b \text{ for all } b \in B\}$ , namely the elements of  $G$  which fix all the elements of  $B$ .

### Example 5.10.0.1.

- For any nonempty set  $A$  the symmetric group  $S_A$  acts on  $A$  by  $\sigma \cdot a = \sigma(a)$  for all  $\sigma \in S_A$ ,  $a \in A$ . The associated permutation representation is the identity map from  $S_A$  to itself.
- The axioms for a vector space  $V$  over a field  $F$  include the two axioms that the multiplicative group  $F^\times$  act on the set  $V$ .

## Chapter 6

# Ring Theory

**Definition 6.0.1** (Field). A commutative division ring is called a *field*. That is, a field is a set  $F$  together with two binary operations  $+$  and  $\cdot$  on  $F$  such that  $(F, +)$  is an abelian group (call its identity  $0$ ) and  $(F \setminus \{0\}, \cdot)$  is also an abelian group, and the following *distributive* law holds:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad \text{for all } a, b, c \in F.$$

## Chapter 7

# Combinatorics

Combinatorics is, loosely, the mathematics of counting and permutations. These notes are based on lectures given by Shiyun Wang at the University of Minnesota during the Fall 2023 semester.

## 7.1 The Pigeonhole Principle

Main idea: If we put 4 pigeons into 3 pigeonholes, at least one pigeon will have to share.

**Definition 7.1.1** (Pigeonhole Principle). Let  $n, k$  be positive integers with  $n > k$ . Suppose that we place  $n$  identical balls into  $k$  identical boxes. Then there will be at least one box in which we place at least two balls.

More generally, if we have  $n$  identical balls and  $m$  boxes with  $n > rm$ , then there will be at least one box with  $r + 1$  balls.



Figure 7.1: Too many pigeons.

**Example 7.1.0.1.** Given ten distinct positive integers less than 107, there exist two disjoint subsets with the same sum. As an illustration, consider Figure 7.2.

*Proof* The largest sum possible would be  $\sum_{i=97}^{106} i = 1015$ . We consider the possible sums of our subsets to be the boxes referred to by the Pigeonhole Principle, and so we have 1016 boxes (the subset being the empty set corresponds to the box with sum of 0). But for a set containing 10 numbers, we have  $2^{10} = 1024$  subsets. By the pigeonhole principle, at least two of these subsets have the same sum since  $1024 > 1016$ . If they are not disjoint, remove their intersection and they will still have the same sum.  $\diamond$

$\{1, 2, 3, 4, 5, 100, 101, 102, 103, 104\}$

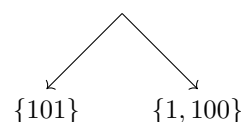


Figure 7.2: An example of a 10-digit set split into two disjoint subsets with the same sum.

**Example 7.1.0.2.** Consider  $\mathbb{R}^2$  restricted to integer coordinates. Show there is no way to assign one of six colors to each vertex such that there does not exist a rectangle whose vertices are monochromatic.

*Proof* I present a simplified version of the proof from class. Consider a vertical column of seven vertices. Since there are only 6 colors, any coloring of these seven vertices will result in a repeated color. This repeated color is red in the first vertical column of Figure 7.3. There are a finite number, let's say  $k$ , of ways to color seven vertical vertices without repeating the coloring in our first column. So if we pick  $k + 1$  neighboring columns of seven vertices, then by the pigeonhole principle at least two columns must share the same coloring. This will yield a rectangle with monochromatic vertices, drawn in red in Figure 7.3.  $\diamond$



Figure 7.3: Eventually the coloring of neighboring sets of seven vertical vertices will have to repeat, yielding a rectangle with monochromatic vertices.

## Appendix A

# Solutions to Shoenfield's *Mathematical Logic*

### A.1 The Nature of Mathematical Logic

No exercises.

### A.2 First-Order Theories

**Exercise A.2.0.1.** An  $n$ -ary truth function  $H$  is *definable in terms of* the truth functions  $H_1, \dots, H_k$  if  $H$  has a definition

$$H(a_1, \dots, a_n) = \dots,$$

where the right-hand side is built up from  $H_1, \dots, H_k, a_1, \dots, a_n$ , and commas and parentheses.

- a) Let  $H_{d,n}$  be the truth function defined by setting  $H_{d,n}(a_1, \dots, a_n) = \mathbf{T}$  if and only if  $a_i = \mathbf{T}$  for at least one  $i$ , and let  $H_{c,n}$  be the truth function defined by setting

$$H_{c,n}(a_1, \dots, a_n) = \mathbf{T} \quad \text{if and only if} \quad a_i = \mathbf{T} \text{ for all } i.$$

Show that every truth function is definable in terms of  $H_{\neg}$  and certain of the  $H_{d,n}$  and  $H_{c,n}$ .

- b) Show that every truth function is definable in terms of  $H_{\neg}$  and  $H_{\vee}$ . [Use (a).]  
c) Show that every truth function is definable in terms of  $H_{\neg}$  and  $H_{\rightarrow}$ . [Use (b).]  
d) Show that every truth function is definable in terms of  $H_{\neg}$  and  $H_{\wedge}$ . [Use (b).]

- e) Show that  $H_{\neg}$  is not definable in terms of  $H_{\vee}$ ,  $H_{\rightarrow}$ ,  $H_{\wedge}$ , and  $H_{\leftrightarrow}$ .

*Proof*

- a) We first consider the case where  $H = \mathbf{F}$  for every valuation. Then we define  $H$  as

$$H(a_1, \dots, a_n) = H_{d,n}(H_{c,2}(a_1, H_{\neg}(a_1)), \dots, H_{c,2}(a_n, H_{\neg}(a_n))) ,$$

which always evaluates to  $\mathbf{F}$ .

Now suppose  $H = \mathbf{T}$  for  $m$   $n$ -tuples  $(a_1, \dots, a_n)_i$  for  $i = 1, \dots, m$ . Then for those  $m$   $n$ -tuples define  $H_{c,n}(i)$  as replacing all  $a_j = \mathbf{F}$  in  $(a_1, \dots, a_n)_i$  with  $H_{\neg}(a_j)$ . Then we define  $H$  as

$$H(a_1, \dots, a_n) = (H_{c,n}(1), \dots, H_{c,n}(m)) ,$$

which always evaluates to  $\mathbf{T}$ .

- b) We show that  $H_{d,n}$  is definable in terms of  $H_{\vee}$ , which in turn constitutes a proof due to (a). We define  $H_{d,n}$  as

$$H_{d,n} = H_{\vee}(a_1, \dots, H_{\vee}(a_{n-2}, H_{\vee}(a_{n-1}, H_{\vee}(a_n)))) .$$

- c) We know that  $H_{\rightarrow}(a, b) = H_{\vee}(H_{\neg}(a), b)$ .

◇

**Exercise A.2.0.2.**

- a) Let  $H_d$  be the truth function defined by

$$H_d(a, b) = \mathbf{T} \text{ if and only if } a = b = \mathbf{T} .$$

Show that every truth function is definable in terms of  $H_d$ .  
[Use 1(b).]

- b) Let  $H_a$  be the truth function defined by

$$H_a(a, b) = \mathbf{F} \text{ if and only if } a = b = \mathbf{T} .$$

Show that every truth function is definable in terms of  $H_a$ .

- c) A truth function  $H$  is **singular** if there is a truth function  $H'$  and an  $i$  such that  $H(a_1, \dots, a_n) = H'(a_i)$  for all  $a_1, \dots, a_n$ . Show that if  $H$  is singular, then every truth function definable in terms of  $H$  is singular.
- d) Show that if  $H$  is a binary truth function such that every truth function is definable in terms of  $H$ , then  $H$  is  $H_d$  or  $H_a$ . [Show that  $H(\mathbf{T}, \mathbf{T}) = \mathbf{F}$  and  $H(\mathbf{F}, \mathbf{F}) = \mathbf{T}$ , and use (c).]



*Proof* asdf

◇

**Exercise A.2.0.3.** Show that if  $uv$  and  $vv'$  are designators, then either  $v$  or  $v'$  is the empty expression.

*Proof* Suppose  $uv$  and  $vv'$  are designators. We use induction on the length of  $uv$ . If  $uv$  is a variable, then either  $u$  or  $v$  are empty (since variables have length 1). If  $v$  is empty, we are done, so suppose  $u$  is empty and  $v$  is a variable. But then  $vv'$  can only be a designator if  $v'$  is empty because the only way to obtain a new designator from a variable is to add either a function symbol or predicate symbol to the left of the variable.

If  $uv$  is an arbitrary term or formula, it is still the case that ◇

**Exercise A.2.0.4.** Show that the result of replacing  $a$  by  $x$  in a term is a term, and that the result of replacing  $a$  by  $x$  in a formula is a formula.

*Proof* asdf

◇

**Exercise A.2.0.5.** Let  $T$  be the theory with no nonlogical symbols and no nonlogical axioms.

## Appendix B

# Solutions to D&F's *Abstract Algebra*

### Preliminaries

#### B.0.1 Basics

In Exercises 1 to 4 let  $\mathcal{A}$  be the set of  $2 \times 2$  matrices with real number entries. Recall that matrix multiplication is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix}.$$

Let

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and let

$$\mathcal{B} = \{X \in \mathcal{A} \mid MX = XM\}.$$

**Exercise B.0.1.1.** Determine which of the following elements of  $\mathcal{A}$  lie in  $\mathcal{B}$ :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

*Solution* We have

$$\begin{aligned}
 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \text{ so } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathcal{B}; \\
 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} &= \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \\
 &\text{so } \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin \mathcal{B}; \\
 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \text{ so } \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{B}; \\
 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \\
 &\text{so } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \notin \mathcal{B}; \\
 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \text{ so } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{B}; \\
 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \\
 &\text{so } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \notin \mathcal{B};
 \end{aligned}$$

◇

**Exercise B.0.1.2.** Prove that if  $P, Q \in \mathcal{B}$ , then  $P + Q \in \mathcal{B}$  (where  $+$  denotes the usual sum of two matrices).

*Proof* We have

$$M(P + Q) = MP + MQ = PM + QM = (P + Q)M.$$

◇

**Exercise B.0.1.3.** Prove that if  $P, Q \in \mathcal{B}$ , then  $P \cdot Q \in \mathcal{B}$  (where  $\cdot$  denotes the usual product of two matrices).

*Proof* We have

$$M(PQ) = (MP)Q = (PM)Q = P(MQ) = P(QM) = (PQ)M.$$

◇

**Exercise B.0.1.4.** Find conditions on  $p, q, r, s$  which determine precisely when  $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{B}$ .

*Solution* We have

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix},$$

and

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix}.$$

Setting these resultant matrices equal to each other yields the required condition:  $r = 0$  and  $p = s$ .  $\diamond$

**Exercise B.0.1.5.** Determine whether the following functions  $f$  are well defined:

- (a)  $f : \mathbb{Q} \rightarrow \mathbb{Z}$  defined by  $f(a/b) = a$ .
- (b)  $f : \mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $f(a/b) = a^2/b^2$ .

*Solution*

- (a) This function  $f$  is not well defined for the following two reasons:  $f(1/2) \neq f(2/4)$  and  $f(-1/2) \neq f(1/-2)$ .
- (b) This function  $f$  is well defined, since any negatives will be squared away and equivalent ways of writing a fraction give the same result:  $f(na/nb) = n^2a^2/n^2b^2 = a^2/b^2 = f(a/b)$ .

$\diamond$

**Exercise B.0.1.6.** Determine whether the function  $f : \mathbb{R}^+ \rightarrow \mathbb{Z}$  defined by mapping a real number  $r$  to the first digit to the right of the decimal point in a decimal expansion of  $r$  is well defined.

*Solution* This function  $f$  is not well defined since  $f(.9) = 9$  and  $f(1) = 0$  even though  $.9 = 1$ .  $\diamond$

**Exercise B.0.1.7.** Let  $f : A \rightarrow B$  be a surjective map of sets. Prove that the relation

$$a \sim b \text{ if and only if } f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of  $f$ .

*Proof* We first prove  $\sim$  is reflexive. Since  $f$  is well defined,  $f(a) = f(a)$ . Next we prove  $\sim$  is symmetric. If  $f(a) = f(b)$ , then  $f(b) = f(a)$ . Finally, we show  $\sim$  is transitive. If  $f(a) = f(b)$  and  $f(b) = f(c)$ , then  $f(a) = f(c)$ .

We now need to show that the equivalence classes of  $\sim$  are the fibers of  $f$ .  $a \sim b$  means  $f(a) = f(b)$ . This means that  $a$  and  $b$  map to the same element of  $B$ ; that is, they belong to the same fiber of  $f$ .  $\diamond$

## B.0.2 Properties of the Integers

**Exercise B.0.2.1.** For each of the following pairs of integers  $a$  and  $b$ , determine their greatest common divisor, their least common multiple, and write their greatest common divisor in the form  $ax + by$  for some integers  $x$  and  $y$ .

(a)  $a = 20, b = 13$ .

(b)  $a = 69, b = 372$ .

(c)  $a = 792, b = 275$ .

(d)  $a = 11391, b = 5673$ .

(e)  $a = 1761, b = 1567$ .

(f)  $a = 507885, b = 60808$ .

*Solution*

(a) We first find the g.c.d.:

$$20 = (1)(13) + 7$$

$$13 = (1)(7) + 6$$

$$7 = (1)(6) + 1$$

$$6 = (6)(1) .$$

So  $\gcd(20, 13) = 1$ .

We now find the l.c.m. We have  $\gcd(a, b) \operatorname{lcm}(a, b) = ab$ , and so

$$\operatorname{lcm}(20, 13) = \frac{20(13)}{\gcd(20, 13)} = 260.$$

We now write the g.c.d. in the form  $ax + by$ :

$$\begin{aligned} 1 &= 7 - (1)(6) \\ &= 7 - (1)[13 - (1)(7)] \\ &= (2)7 - (13)1 \\ &= (2)[20 - (1)13] - 13(1) \\ &= (2)20 - (3)13 \end{aligned}$$

(b) We first find the g.c.d.:

$$\begin{aligned} 69 &= (0)(372) + 69 \\ 372 &= (5)(69) + 27 \\ 69 &= (2)(27) + 15 \\ 27 &= (1)(15) + 12 \\ 15 &= (1)(12) + 3 \\ 12 &= (4)(3). \end{aligned}$$

So  $\gcd(69, 372) = 3$ .

We now find the l.c.m.:

$$\operatorname{lcm}(69, 372) = \frac{69(372)}{3} = 8556.$$

We now write the g.c.d. in the form  $ax + by$ :

$$\begin{aligned} 3 &= 15 - (1)(12) \\ &= 15 - [27 - 15] \\ &= (2)15 - 27 \\ &= (2)[69 - 2(27)] - 27 \\ &= (2)69 - 5(27) \\ &= (2)69 - 5[372 - (5)69] \\ &= (27)69 - (5)372. \end{aligned}$$

(c) We first find the g.c.d.:

$$\begin{aligned} 792 &= 2(275) + 242 \\ 275 &= 1(242) + 33 \\ 242 &= 7(33) + 11 \\ 33 &= 3(11). \end{aligned}$$

So  $\gcd(792, 275) = 11$ .

We now find the l.c.m.:

$$\text{lcm}(792, 275) = \frac{792(275)}{11} = 19800.$$

We now write the g.c.d. in the form  $ax + by$ :

$$\begin{aligned} 11 &= 242 - 7(33) \\ &= 242 - 7[275 - 242] \\ &= (8)242 - (7)275 \\ &= 8[792 - (2)275] - (7)275 \\ &= (8)792 - (23)275. \end{aligned}$$

(d) We first find the g.c.d.:

$$\begin{aligned} 11391 &= 2(5673) + 45 \\ 5673 &= 126(45) + 3 \\ 45 &= 15(3). \end{aligned}$$

So  $\text{gcd}(11391, 5673) = 3$ .

We now find the l.c.m.:

$$\text{lcm}(11391, 5673) = \frac{11391(5673)}{3} = 21540381.$$

We now write the g.c.d. in the form  $ax + by$ :

$$\begin{aligned} 3 &= 5673 - 126(45) \\ &= 5673 - 126[11391 - 2(5673)] \\ &= (253)5673 - (126)11391. \end{aligned}$$

(e) We first find the g.c.d.:

$$\begin{aligned} 1761 &= (1)1567 + 194 \\ 1567 &= (8)194 + 15 \\ 194 &= (12)15 + 14 \\ 15 &= (1)14 + 1 \\ 14 &= (14)1. \end{aligned}$$

So  $\text{gcd}(1761, 1567) = 1$ .

We now find the l.c.m.:

$$\text{lcm}(1761, 1567) = \frac{1761(1567)}{1} = 2759487.$$

We now write the g.c.d. in the form  $ax + by$ :

$$\begin{aligned}
 1 &= 15 - 14 \\
 &= 15 - [194 - (12)15] \\
 &= (13)15 - 194 \\
 &= (13)[1567 - (8)194] - 194 \\
 &= (13)1567 - (105)194 \\
 &= (13)1567 - (105)[1761 - 1567] \\
 &= (118)1567 - (105)1761.
 \end{aligned}$$

(f) We first find the g.c.d.:

$$\begin{aligned}
 507885 &= (8)60808 + 21421 \\
 60808 &= (2)21421 + 17966 \\
 21421 &= (1)17966 + 3455 \\
 17966 &= (5)3455 + 691 \\
 3455 &= (5)691.
 \end{aligned}$$

So  $\gcd(507885, 60808) = 691$ .

We now find the l.c.m.:

$$\text{lcm}(507885, 60808) = \frac{507885(60808)}{691} = 44693880.$$

We now write the g.c.d. in the form  $ax + by$ :

$$\begin{aligned}
 691 &= 17966 - (5)3455 \\
 &= 17966 - (5)[21421 - 17966] \\
 &= (6)17966 - (5)21421 \\
 &= (6)[60808 - (2)21421] - (5)21421 \\
 &= (6)60808 - (17)21421 \\
 &= (6)60808 - (17)[507885 - (8)60808] \\
 &= (142)60808 - (17)507885.
 \end{aligned}$$

◇

**Exercise B.0.2.2.** Prove that if the integer  $k$  divides the integers  $a$  and  $b$  then  $k$  divides  $as + bt$  for every pair of integers  $s$  and  $t$ .

*Proof* Suppose  $k \mid a$  and  $k \mid b$ . Then  $a = km$  and  $b = nk$  for some integers  $m$  and  $n$ . So  $as + bt = mks + nkt = k(ms + nt)$ , and therefore  $k \mid (as + bt)$ . ◇



**Exercise B.0.2.3.** Prove that if  $n$  is composite then there are integers  $a$  and  $b$  such that  $n$  divides  $ab$  but  $n$  does not divide either  $a$  or  $b$ .

*Proof* Suppose  $n$  is composite. Then  $n = ab$  for some  $a$  and  $b$  with  $|a| < n$  and  $|b| < n$ . Since  $n = ab$ ,  $n \mid ab$ , but  $n \nmid a$  and  $n \nmid b$  since  $|a| < n$  and  $|b| < n$ .  $\diamond$

**Exercise B.0.2.4.** Let  $a, b$  and  $N$  be fixed integers with  $a$  and  $b$  nonzero and let  $d = \gcd(a, b)$  be the greatest common divisor of  $a$  and  $b$ . Suppose  $x_0$  and  $y_0$  are particular solutions to  $ax + by = N$  (i.e.,  $ax_0 + by_0 = N$ ). Prove for any integer  $t$  that the integers

$$x = x_0 + \frac{b}{d}t \quad \text{and} \quad y = y_0 - \frac{a}{d}t$$

are also solutions to  $ax + by = N$  (this is in fact the general solution).

*Proof* Suppose  $ax + by = N$  has the particular solutions  $x_0$  and  $y_0$ ; that is, suppose  $ax_0 + by_0 = N$ . Let  $t$  be arbitrary. Then

$$a \left( x_0 + \frac{b}{d}t \right) + b \left( y_0 - \frac{a}{d}t \right) = ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t = N.$$

$\diamond$

**Exercise B.0.2.5.** Determine the value  $\varphi(n)$  for each integer  $n \leq 30$  where  $\varphi$  denotes the Euler  $\varphi$ -function.

*Solution* We have  $\varphi(1) = 1$ ,  $\varphi(2) = 1$ ,  $\varphi(3) = 2$ ,  $\varphi(4) = 2$ ,  $\varphi(5) = 4$ ,  $\varphi(6) = 2$ ,  $\varphi(7) = 6$ ,  $\varphi(8) = \varphi(2^3) = 2^{3-1}(2-1) = 4$ ,  $\varphi(9) = \varphi(3^2) = 3(3-1) = 6$ ,  $\varphi(10) = \varphi(2)\varphi(5) = 4$ ,  $\varphi(11) = 10$ ,  $\varphi(12) = \varphi(3)\varphi(4) = 2(2) = 4$ ,  $\varphi(13) = 12$ ,  $\varphi(14) = \varphi(2)\varphi(7) = 6$ ,  $\varphi(15) = \varphi(3)\varphi(5) = 2(4) = 8$ ,  $\varphi(16) = \varphi(2^4) = 2^3(2-1) = 8$ ,  $\varphi(17) = 16$ ,  $\varphi(18) = \varphi(2)\varphi(9) = 6$ ,  $\varphi(19) = 18$ ,  $\varphi(20) = \varphi(4)\varphi(5) = 8$ ,  $\varphi(21) = \varphi(3)\varphi(7) = 12$ ,  $\varphi(22) = \varphi(2)\varphi(11) = 10$ ,  $\varphi(23) = 22$ ,  $\varphi(24) = \varphi(3)\varphi(8) = 8$ ,  $\varphi(25) = \varphi(5^2) = 5(4) = 20$ ,  $\varphi(26) = \varphi(2)\varphi(13) = 12$ ,  $\varphi(27) = \varphi(3^3) = 3^2(2) = 18$ ,  $\varphi(28) = \varphi(4)\varphi(7) = 12$ ,  $\varphi(29) = 28$ ,  $\varphi(30) = \varphi(3)\varphi(10) = 8$ .  $\diamond$

**Exercise B.0.2.6.** Prove the Well Ordering Property of  $\mathbb{Z}$  by induction and prove the minimal element is unique.

*Proof* Let  $A$  be an arbitrary nonempty subset of  $\mathbb{Z}^+$ .

Base Case:  $A$  has a single element. Then this element is the minimal element of  $A$ , for  $m \leq m$ . Moreover, being the only element, it is unique.

Inductive Step: Now suppose  $A$  has  $n$  elements, and the theorem holds for any set of  $n$  or fewer elements. We show the theorem holds for a set of  $n + 1$  elements. If new element is smaller than existing minimal element, it is the minimal element. Otherwise, the existing minimal element remains the minimal element.  $\diamond$

**Exercise B.0.2.7.** If  $p$  is a prime prove that there do not exist nonzero integers  $a$  and  $b$  such that  $a^2 = pb^2$  (i.e.,  $\sqrt{p}$  is not a rational number).

*Proof* By way of contradiction, suppose  $p$  is prime and there exists  $a, b$  such that  $a^2 = pb^2$ ; that is,  $\sqrt{p} = \frac{a}{b}$ . Assume  $\gcd(a, b) = 1$ ; that is, suppose  $\sqrt{p}$  is written in its most reduced form. Then  $p \mid a^2$ , and so  $p \mid a$ . That is,  $a = pc$  for some integer  $c$ . Then  $a^2 = p^2c^2 = pb^2$ . And so,  $pc^2 = b^2$ , and we see that  $p \mid b^2$  and so  $p \mid b$ . Since  $p \mid a$  and  $p \mid b$ , then  $p \mid ab$ , contradicting the fact that  $\gcd(a, b) = 1$ .  $\diamond$

**Exercise B.0.2.8.** Let  $p$  be a prime,  $n \in \mathbb{Z}^+$ . Find a formula for the largest power of  $p$  which divides  $n! = n(n-1)(n-2) \cdots 2 \cdot 1$  (it involves the greatest integer function).

*Solution* There are  $\left\lfloor \frac{n}{p^k} \right\rfloor$  multiples of  $p^k$  in the list  $1, 2, \dots, n$ ; that is,  $p^k$  divides  $\left\lfloor \frac{n}{p^k} \right\rfloor$  numbers less than or equal to  $n$ . Thus,  $\sum_k \left\lfloor \frac{n}{p^k} \right\rfloor$  accounts for the highest order of  $p$  which divides  $n!$ .  $\diamond$

**Exercise B.0.2.9.** Write a computer program to determine the greatest common divisor  $\gcd(a, b)$  of two integers  $a$  and  $b$  and to express  $\gcd(a, b)$  in the form  $ax + by$  for some integers  $x$  and  $y$ .

*Solution*

```
def lineargcd(a, b):
    alist = [a]
    coeff = []
    counter = 0
    while b:
```

```

    a, b = b, a%b
    alist.append(a)
    coeff.append( (alist[counter] - b) // a)
    counter = counter + 1
x, y = 1, 0
for i in range(len(coeff) - 1):
    x, y = x, y + x*coeff[-i-2]
    x, y = y, x
if len(coeff) % 2 == 0:
    x, y = y, x
return alist[-1], x, y, len(coeff) % 2

x, y = input("Enter the two numbers you'd like to find the \
            "g.c.d. of: ").split()
x = int(x)
y = int(y)

if lineargcd(x,y)[3] == 0:
    print(f"The g.c.d. of {x} and {y} is {lineargcd(x,y)[0]}.")
    print(f"You can write this g.c.d. as: \
          "{x}*{lineargcd(x,y)[1]} - {y}*{lineargcd(x,y)[2]}".")


if lineargcd(x,y)[3] == 1:
    print(f"The g.c.d. of {x} and {y} is {lineargcd(x,y)[0]}.")
    print(f"You can write this g.c.d. as: \
          "{y}*{lineargcd(x,y)[1]} - {x}*{lineargcd(x,y)[2]}".")

```



**Exercise B.0.2.10.** Prove for any given positive integer  $N$  there exist only finitely many integers  $n$  with  $\varphi(n) = N$  where  $\varphi$  denotes Euler's  $\varphi$ -function. Conclude in particular that  $\varphi(n)$  tends to infinity as  $n$  tends to infinity.

*Proof* Let  $N \in \mathbb{Z}^+$  be arbitrary. For any  $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$  such that  $\varphi(n) = p_1^{\alpha_1-1}(p_1-1) \cdots p_s^{\alpha_s-1}(p_s-1) = N$ , it is clear from this formula that for any prime factor  $p_i$  of  $n$ , we have  $\varphi(p_i) = p_i - 1 \mid N$ . Thus  $p_i - 1 \leq N$ , or  $p_i \leq N + 1$ .

Therefore, let  $p_1, \dots, p_t$  be the primes which are less than or equal to  $N + 1$ . All  $n$  such that  $\varphi(n) = N$  thus have prime factorizations of the form  $p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ . Moreover, for  $1 \leq i \leq t$ , we have  $p_i^{\alpha_i-1} \mid N$ . Let  $k_i$  be the largest integer such that  $p_i^{k_i} \mid N$ . Obviously,  $\alpha_i \leq k_i + 1$ , and so there are at most  $\prod_i (k_i + 1)$  integers  $n$  such that  $\varphi(n) = N$ . 

**Exercise B.0.2.11.** Prove that if  $d$  divides  $n$  then  $\varphi(d)$  divides  $\varphi(n)$  where  $\varphi$  denotes Euler's  $\varphi$ -function.

*Proof* Suppose  $d \mid n$ , and let the prime factorizations of  $n$  and  $d$  be  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$  and  $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s} p_{s+1}^{\beta_{s+1}} \cdots p_t^{\beta_t}$ , where  $\beta_i \geq \alpha_i$  for  $1 \leq i \leq s$ .

We have

$$\varphi(n) = p_1^{\alpha_1-1}(p_1-1) \cdots p_s^{\alpha_s-1}(p_s-1),$$

and therefore

$$\begin{aligned} \varphi(d) &= p_1^{\beta_1-1}(p_1-1) \cdots p_s^{\beta_s-1}(p_s-1) p_{s+1}^{\beta_{s+1}-1}(p_{s+1}-1) \cdots p_t^{\beta_t-1}(p_t-1) \\ &= p_1^{\alpha_1-1} p_1^{\gamma_1}(p_1-1) \cdots p_s^{\alpha_s-1} p_s^{\gamma_s}(p_s-1) p_{s+1}^{\beta_{s+1}-1}(p_{s+1}-1) \cdots p_t^{\beta_t-1}(p_t-1) \\ &= \varphi(n) p_1^{\gamma_1} \cdots p_s^{\gamma_s} p_{s+1}^{\beta_{s+1}-1}(p_{s+1}-1) \cdots p_t^{\beta_t-1}(p_t-1). \end{aligned}$$

And so we have that  $\varphi(n) \mid \varphi(d)$ . ◇

### B.0.3 $\mathbb{Z}/n\mathbb{Z}$ : The Integers Modulo $n$

**Exercise B.0.3.1.** Write down explicitly all the elements in the residue classes of  $\mathbb{Z}/18\mathbb{Z}$ .

**Exercise B.0.3.2.** Prove that the distinct equivalence classes in  $\mathbb{Z}/n\mathbb{Z}$  are precisely  $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$  (use the Division Algorithm).

**Exercise B.0.3.3.** Prove that if  $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$  is any positive integer then  $a \equiv_9 a_n + a_{n-1} + \cdots + a_1 + a_0$  (note that this is the usual arithmetic rule that the remainder after division by 9 is the same as the sum of the decimal digits mod 9—in particular an integer is divisible by 9 if and only if the sum of its digits is divisible by 9) [note that  $10 \equiv_9 1$ ].

**Exercise B.0.3.4.** Compute the remainder when  $37^{100}$  is divided by 29.

**Exercise B.0.3.5.** Compute the last two digits of  $9^{1500}$ .

**Exercise B.0.3.6.** Prove that the squares of the elements in  $\mathbb{Z}/4\mathbb{Z}$  are just  $\bar{0}$  and  $\bar{1}$ .

**Exercise B.0.3.7.** Prove for any integers  $a$  and  $b$  that  $a^2 + b^2$  never leaves a remainder of 3 when divided by 4 (use the previous exercise).

**Exercise B.0.3.8.** Prove that the equation  $a^2 + b^2 = 3c^2$  has no solutions in nonzero integers  $a$ ,  $b$ , and  $c$ . [Consider the equation mod 4 as in the previous two exercises and show that  $a$ ,  $b$ , and  $c$  would all have to be divisible by 2. Then each of  $a^2$ ,  $b^2$ , and  $c^2$  has a factor of 4 and by dividing through by 4 show that there would be a smaller set of solutions to the original equation. Iterate to reach a contradiction.]

**Exercise B.0.3.9.** Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.

**Exercise B.0.3.10.** Prove that the number of elements of  $(\mathbb{Z}/n\mathbb{Z})^\times$  is  $\varphi(n)$  where  $\varphi$  denotes the Euler  $\varphi$ -function.

**Exercise B.0.3.11.** Prove that if  $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ , then  $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ .

**Exercise B.0.3.12.** Let  $n \in \mathbb{Z}$ ,  $n > 1$ , and let  $a \in \mathbb{Z}$  with  $1 \leq a \leq n$ . Prove if  $a$  and  $n$  are not relatively prime, there exists an integer

$b$  with  $1 \leq b < n$  such that  $ab \equiv_n 0$  and deduce that there cannot be an integer  $c$  such that  $ac \equiv_n 1$ .

**Exercise B.0.3.13.** Let  $n \in \mathbb{Z}$ ,  $n > 1$ , and let  $a \in \mathbb{Z}$  with  $1 \leq a \leq n$ . Prove that if  $a$  and  $n$  are relatively prime then there is an integer  $c$  such that  $ac \equiv_n 1$  [use the fact that the g.c.d. of two integers is a  $\mathbb{Z}$ -linear combination of the integers].

**Exercise B.0.3.14.** Conclude from the previous two exercises that  $(\mathbb{Z}/n\mathbb{Z})^\times$  is the set of elements  $\bar{a}$  of  $\mathbb{Z}/n\mathbb{Z}$  with  $\gcd(a, n) = 1$  and hence prove Proposition 4. Verify this directly in the case  $n = 12$ .

**Exercise B.0.3.15.** For each of the following pairs of integers  $a$  and  $n$ , show that  $a$  is relatively prime to  $n$  and determine the multiplicative inverse of  $\bar{a}$  in  $\mathbb{Z}/n\mathbb{Z}$ .

- (a)  $a = 13$ ,  $n = 20$ .
- (b)  $a = 69$ ,  $n = 89$ .
- (c)  $a = 1891$ ,  $n = 3797$ .
- (d)  $a = 6003722857$ ,  $n = 77695236973$ . [The Euclidean Algorithm requires on 3 steps for these integers.]

**Exercise B.0.3.16.** Write a computer program to add and multiply mod  $n$ , for any  $n$  given as input. The output of these operations should be the least residues of the sums and products of two integers. Also include the feature that if  $\gcd(a, n) = 1$ , an integer between 1 and  $n - 1$  such that  $\bar{a} \cdot \bar{c} = \bar{1}$  may be printed on request. (Your program should not, of course, simply quote "mod" functions already built into many systems.)

## B.1 Introduction to Groups

### B.1.1 Basic Axioms and Examples

Let  $G$  be a group.

**Exercise B.1.1.1.** Determine which of the following binary operations are associative:

- (a) the operation  $\cdot$  on  $\mathbb{Z}$  defined by  $a \cdot b = a - b$
- (b) the operation  $\cdot$  on  $\mathbb{R}$  defined by  $a \cdot b = a + b + ab$
- (c) the operation  $\cdot$  on  $\mathbb{Q}$  defined by  $a \cdot b = \frac{a+b}{5}$
- (d) the operation  $\cdot$  on  $\mathbb{Z} \times \mathbb{Z}$  defined by  $(a, b) \cdot (c, d) = (ad + bc, bd)$
- (e) the operation  $\cdot$  on  $\mathbb{Q} \setminus \{0\}$  defined by  $a \cdot b = \frac{a}{b}$ .

**Exercise B.1.1.2.** Decide which of the binary operations in the preceding exercise are commutative.

**Exercise B.1.1.3.** Prove that addition of residue classes in  $\mathbb{Z}/n\mathbb{Z}$  is associative (you may assume it is well defined).

**Exercise B.1.1.4.** Prove that multiplication of residue classes in  $\mathbb{Z}/n\mathbb{Z}$  is associative (you may assume it is well defined).

**Exercise B.1.1.5.** Prove for all  $n > 1$  that  $\mathbb{Z}/n\mathbb{Z}$  is not a group under multiplication of residue classes.

**Exercise B.1.1.6.** Determine which of the following sets are groups under addition:

- (a) the set of rational numbers (including  $0 = 0/1$ ) in lowest terms whose denominators are odd
- (b) the set of rational numbers (including  $0 = 0/1$ ) in lowest terms whose denominators are even
- (c) the set of rational numbers of absolute value  $< 1$

- (d) the set of rational numbers of absolute value  $\geq 1$  together with 0
- (e) the set of rational numbers with denominators equal to 1 or 2
- (f) the set of rational numbers with denominators equal to 1, 2, or 3.

**Exercise B.1.1.7.** Let  $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$  and for  $x, y \in G$  let  $x \cdot y$  be the fractional part of  $x + y$  (i.e.,  $x \cdot y = x + y - \lfloor x + y \rfloor$  where  $\lfloor a \rfloor$  is the greatest integer less than or equal to  $a$ ). Prove that  $\cdot$  is a well defined binary operation on  $G$  and that  $G$  is an abelian group under  $\cdot$  (called the *real numbers mod 1*).

**Exercise B.1.1.8.** Let  $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$ .

- (a) Prove that  $G$  is a group under multiplication (called the group of *roots of unity* in  $\mathbb{C}$ ).
- (b) Prove that  $G$  is not a group under addition.

**Exercise B.1.1.9.** Let  $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$ .

- (a) Prove that  $G$  is a group under addition.
- (b) Prove that the nonzero elements of  $G$  are a group under multiplication. [“Rationalize the denominators” to find multiplicative inverses.]

**Exercise B.1.1.10.** Prove that a finite group is abelian if and only if its group table is a symmetric matrix.

**Exercise B.1.1.11.** Find the orders of each element of the additive group  $\mathbb{Z}/12\mathbb{Z}$ .



**Exercise B.1.1.12.** Find the orders of the following elements of the multiplicative group  $(\mathbb{Z}/12\mathbb{Z})^\times$ :  $\overline{1}$ ,  $\overline{-1}$ ,  $\overline{5}$ ,  $\overline{7}$ ,  $\overline{-7}$ ,  $\overline{13}$

## Appendix C

# Solutions to Munkres' *Topology*

### C.1 Set Theory and Logic

#### C.1.1 Fundamental Concepts

**Exercise C.1.1.1.** Check the distributive laws for  $\cup$  and  $\cap$  and DeMorgan's laws.

*Proof* We first show that  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ . Let  $x$  be an arbitrary element of  $A \cap (B \cup C)$ . Then  $x \in A$  and  $x \in (B \cup C)$ . In the case that  $x \in B$ , we have  $x \in A \cap B$ , and therefore  $x \in (A \cap B) \cup (A \cap C)$ . In the case that  $x \in C$ , we have  $x \in A \cap C$ , and therefore  $x \in (A \cap B) \cup (A \cap C)$ . Thus,  $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ . Now let  $x$  be an arbitrary element of  $(A \cap B) \cup (A \cap C)$ . Then  $x \in A \cap B$  or  $x \in A \cap C$ . In the case that  $x \in A \cap B$ , we have  $x \in A$  and  $x \in B$ . But then  $x \in B \cup C$ , and so  $x \in A \cap (B \cup C)$ . In the case that  $x \in A \cap C$ , we have  $x \in A$  and  $x \in C$ . But then  $x \in B \cup C$ , and so  $x \in A \cap (B \cup C)$ . Thus,  $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$  and we are done.

The proof of the second distributive law is similar.

We now show that  $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ . Let  $x$  be an arbitrary element of  $A \setminus (B \cup C)$ . Then  $x \in A$  and  $x \notin B \cup C$ . But then  $x \notin B$  and  $x \notin C$ , and thus  $x \in (A \setminus B) \cap (A \setminus C)$ . Thus,  $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$ . Now let  $x$  be an arbitrary element of  $(A \setminus B) \cap (A \setminus C)$ . Then  $x \in A \setminus B$  (and so  $x \in A$  and  $x \notin B$ ) and  $x \in A \setminus C$  (and so  $x \in A$  and  $x \notin C$ ). But then  $x \notin B \cup C$ , and so  $x \in A \setminus (B \cup C)$ . Thus,  $(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C)$ , and we are done.

The proof of DeMorgan's second law is similar. ◇

**Exercise C.1.1.2.** Determine which of the following statements are true for all sets  $A$ ,  $B$ ,  $C$ , and  $D$ .

**Exercise C.1.1.3.**

- (a) Write the contrapositive and converse of the following statement: "If  $x < 0$ , then  $x^2 - x > 0$ ," and determine which (if any) of the three statements are true.
- (b) Do the same for the statement "If  $x > 0$ , then  $x^2 - x > 0$ ."

**Exercise C.1.1.4.** Let  $A$  and  $B$  be sets of real numbers. Write the negation of each of the following statements:

- (a) For every  $a \in A$ , it is true that  $a^2 \in B$ .
- (b) For at least one  $a \in A$ , it is true that  $a^2 \in B$ .
- (c) For every  $a \in A$ , it is true that  $a^2 \notin B$ .
- (d) For at least one  $a \notin A$ , it is true that  $a^2 \in B$ .

**Exercise C.1.1.5.** Let  $\mathcal{A}$  be a nonempty collection of sets. Determine the truth of each of the following statements and of their converses:

- (a)  $x \in \bigcup_{A \in \mathcal{A}} A \Rightarrow x \in A$  for at least one  $A \in \mathcal{A}$ .
- (b)  $x \in \bigcup_{A \in \mathcal{A}} A \Rightarrow x \in A$  for every  $A \in \mathcal{A}$ .
- (c)  $x \in \bigcap_{A \in \mathcal{A}} A \Rightarrow x \in A$  for at least one  $A \in \mathcal{A}$ .
- (d)  $x \in \bigcap_{A \in \mathcal{A}} A \Rightarrow x \in A$  for every  $A \in \mathcal{A}$ .

**Exercise C.1.1.6.** Write the contrapositive of each of the statements of Exercise 5.

**Exercise C.1.1.7.** Given sets  $A$ ,  $B$ , and  $C$ , express each of the following sets in terms of  $A$ ,  $B$ , and  $C$ , using the symbols  $\cup$ ,  $\cap$ , and  $\setminus$ .

$$D = \{x \mid x \in A \text{ and } (x \in B \text{ or } x \in C)\},$$

$$E = \{(x \mid x \in A \text{ and } (x \in B \text{ or } x \in C)\},$$

$$F = \{x \mid x \in A \text{ and } (x \in B \Rightarrow x \in C)\}.$$

**Exercise C.1.1.8.** Given a set  $A$  has two elements, show that  $\mathcal{P}(A)$  has four elements. How many elements does  $\mathcal{P}(A)$  if  $A$  has one element? Three elements? No elements? Why is  $\mathcal{P}(A)$  called the power set of  $A$ ?

**Exercise C.1.1.9.** Formulate and prove DeMorgan's laws for arbitrary unions and intersections.

**Exercise C.1.1.10.** Let  $\mathbb{R}$  denote the set of real numbers. For each of the following subsets of  $\mathbb{R} \times \mathbb{R}$ , determine whether it is equal to the cartesian product of two subsets of  $\mathbb{R}$ .

(a)  $\{(x, y) \mid x \text{ is an integer}\}.$

(b)  $\{(x, y) \mid 0 < y \leq 1\}.$

(c)  $\{(x, y) \mid y > x\}.$

(d)  $\{(x, y) \mid x \text{ is not an integer and } y \text{ is an integer}\}.$

(e)  $\{(x, y) \mid x^2 + y^2 < 1\}.$

# Index

- binary relation, 9
  - comparable, 9
  - dictionary order
    - relation, 10
  - equivalence class, 9
  - equivalence relation, 9
  - nonreflexive, 9
  - order relation, 10
  - order type, 10
  - reflexive, 9
  - representative of an
    - equivalence class, 9
  - symmetric, 9
  - transitive, 9
- function, 7
  - bijective, 8
  - codomain, 7
  - composite, 8
  - domain, 7
  - fiber, 7
  - image of element, 7
  - image of subset, 7
  - image set, 7
  - injective, 8
  - inverse, 8
  - left inverse, 8
  - one-to-one, 8
  - one-to-one
    - correspondence, 8
  - onto, 8
  - permutation, 8
  - preimage, 7
  - restriction of, 7
  - rule of assignment, 7
  - surjective, 8
  - value of element, 7
- group theory
  - abelian, 47
  - associative, 47
  - binary operation, 47
  - closed under operation,
    - 47
  - commutative, 47
  - commutative group, 47
  - cycle, 54
  - cycle decomposition, 54
  - dihedral group, 53
  - direct product, 48
  - faithful group action, 58
  - finite group, 47
  - general linear group, 55
  - generators, 52
  - group, 47
  - group action, 58
  - homomorphism, 57
  - identity element, 47
  - inverse of element, 47
  - isomorphism, 57
  - kernel of group action,
    - 58
  - multiplication/group
    - table, 51
  - order of element, 50
  - permutation
    - representation of
      - group action, 58
  - presentation, 52
  - quaternion group, 56
  - relations, 52
  - subgroup, 48
  - symmetric group, 54
- logic

- $n$ -tuple, 14
  - atomic formula, 16
  - characterization
    - problem, 22
  - closed formula, 17
  - complete, 20
  - completeness theorem, 22
  - consistent, 20
  - decidable, 20
  - designator, 16
  - elementary formula, 18
  - equivalent theories, 20
  - extension of language, 16
  - extension of theory, 20
  - first-order language, 16
  - first-order theory, 19
  - formulas, 16
  - function, 14
  - Henkin theory, 23
  - inconsistent, 20
  - logical axioms, 19
  - model, 20
  - name, 17
  - open theory, 20, 23
  - predicate, 15
  - quasi-tautology, 23
  - special axiom, 23
  - special constant, 23
  - structure, 17
  - terms, 16
  - truth function, 14
  - truth valuation for a
    - theory, 20
  - undecidable, 20
  - valid formula, 18
- pigeonhole principle, 61
- ring theory
  - field, 59
- set, 4
  - bounded above, 11
  - bounded below, 11
  - cardinality, 5
  - cartesian product, 6
  - countable, 5
  - difference of, 6
  - disjoint sets, 5
  - element of a, 4
  - empty set, 4
  - finite, 5
  - greatest lower bound, 11
  - infimum, 11
  - intersection of, 6
  - largest element of, 11
  - least upper bound, 11
  - least upper bound
    - property, 11
  - lower bound, 11
  - partition of, 6
  - power set, 4
  - smallest element of, 11
  - subset, 5
  - supremum, 11
  - union of, 6
  - upper bound, 11
- topology, 26
  - $T_1$  axiom, 40
  - $\epsilon$ -ball, 34
  - basis for a, 27
  - box topology, 31
  - closed set, 28
  - closure, 28
  - coarser, 27
  - comparable, 27
  - continuous function, 41
  - converging sequence, 39
  - convex, 37
  - coordinate function, 42
  - discrete topology, 26
  - finer, 26
  - Hausdorff, 38
  - homeomorphism, 43
  - imbedding, 43
  - indiscrete topology, 26
  - interior, 28
  - limit of sequence, 39
  - limit point, 28
  - metric, 34
  - metric space, 34
  - metric topology, 34
  - metrizable, 34
  - neighborhood, 26
  - open set, 26
  - order topology, 30

- pasting lemma, 42
- product space, 32
- product topology, 32
- standard topology of the
  - real line, 27
- subbasis, 27
- subspace, 33
- subspace topology, 33
- topological space, 26
- trivial topology, 26