We write $2 \in E$ when we want to say that 2 is in the set E, and $-3 \notin E$ to say that -3 is not in the set E.

Some of the more important sets that we will consider are the following:

$$\begin{aligned} \mathbb{N} &= \{n : n \text{ is a natural number}\} = \{1, 2, 3, \ldots\}; \\ \mathbb{Z} &= \{n : n \text{ is an integer}\} = \{\ldots, -1, 0, 1, 2, \ldots\}; \\ \mathbb{Q} &= \{r : r \text{ is a rational number}\} = \{p/q : p, q \in \mathbb{Z} \text{ where } q \neq 0\}; \\ \mathbb{R} &= \{x : x \text{ is a real number}\}; \\ \mathbb{C} &= \{z : z \text{ is a complex number}\}. \end{aligned}$$

We can find various relations between sets as well as perform operations on sets. A set A is a ***subset*** of B, written $A \subset B$ or $B \supset A$, if every element of A is also an element of B. For example,

$$\{4, 5, 8\} \subset \{2, 3, 4, 5, 6, 7, 8, 9\}$$

and

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

Trivially, every set is a subset of itself. A set B is a ***proper subset*** of a set A if $B \subset A$ but $B \neq A$. If A is not a subset of B, we write $A \not\subset B$; for example, $\{4, 7, 9\} \not\subset \{2, 4, 5, 8, 9\}$. Two sets are ***equal***, written $A = B$, if we can show that $A \subset B$ and $B \subset A$.

It is convenient to have a set with no elements in it. This set is called the ***empty set*** and is denoted by $\emptyset$. Note that the empty set is a subset of every set.

To construct new sets out of old sets, we can perform certain operations: the ***union*** $A \cup B$ of two sets A and B is defined as

$$A \cup B = \{x : x \in A \text{ or } x \in B\};$$

the ***intersection*** of A and B is defined by

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

If $A = \{1, 3, 5\}$ and $B = \{1, 2, 3, 9\}$, then

$$A \cup B = \{1, 2, 3, 5, 9\} \quad \text{and} \quad A \cap B = \{1, 3\}.$$

We can consider the union and the intersection of more than two sets. In this case we write

$$\bigcup_{i=1}^{n} A_i = A_1 \cup \ldots \cup A_n$$

and

$$\bigcap_{i=1}^{n} A_i = A_1 \cap \ldots \cap A_n$$

for the union and intersection, respectively, of the sets $A_1, \ldots, A_n$.

When two sets have no elements in common, they are said to be ***disjoint***; for example, if E is the set of even integers and O is the set of odd integers, then E and O are disjoint. Two sets A and B are disjoint exactly when $A \cap B = \emptyset$.

Sometimes we will work within one fixed set U, called the ***universal set***. For any set $A \subset U$, we define the ***complement*** of A, denoted by A', to be the set

$$A' = \{x : x \in U \text{ and } x \notin A\}.$$

We define the ***difference*** of two sets A and B to be

$$A \setminus B = A \cap B' = \{x : x \in A \text{ and } x \notin B\}.$$

Abstract Algebra

Theory and Applications

Acknowledgements

I would like to acknowledge the following reviewers for their helpful comments and suggestions.

- David Anderson, University of Tennessee, Knoxville
- Robert Beezer, University of Puget Sound
- Myron Hood, California Polytechnic State University
- Herbert Kasube, Bradley University
- John Kurtzke, University of Portland
- Inessa Levi, University of Louisville
- Geoffrey Mason, University of California, Santa Cruz
- Bruce Mericle, Mankato State University
- Kimmo Rosenthal, Union College
- Mark Teply, University of Wisconsin

I would also like to thank Steve Quigley, Marnie Pommett, Cathie Griffin, Kelle Karshick, and the rest of the staff at PWS Publishing for their guidance throughout this project. It has been a pleasure to work with them.

Robert Beezer encouraged me to make *Abstract Algebra: Theory and Applications* available as an open source textbook, a decision that I have never regretted. With his assistance, the book has been rewritten in PreTeXt (pretextbook.org), making it possible to quickly output print, web, PDF versions and more from the same source. The open source version of this book has received support from the National Science Foundation (Awards #DUE-1020957, #DUE–1625223, and #DUE–1821329).

1

Preliminaries

A certain amount of mathematical maturity is necessary to find and study applications of abstract algebra. A basic knowledge of set theory, mathematical induction, equivalence relations, and matrices is a must. Even more important is the ability to read and understand mathematical proofs. In this chapter we will outline the background needed for a course in abstract algebra.

1.1 A Short Note on Proofs

Abstract mathematics is different from other sciences. In laboratory sciences such as chemistry and physics, scientists perform experiments to discover new principles and verify theories. Although mathematics is often motivated by physical experimentation or by computer simulations, it is made rigorous through the use of logical arguments. In studying abstract mathematics, we take what is called an axiomatic approach; that is, we take a collection of objects $\mathcal{S}$ and assume some rules about their structure. These rules are called ***axioms***. Using the axioms for $\mathcal{S}$, we wish to derive other information about $\mathcal{S}$ by using logical arguments. We require that our axioms be consistent; that is, they should not contradict one another. We also demand that there not be too many axioms. If a system of axioms is too restrictive, there will be few examples of the mathematical structure.

A ***statement*** in logic or mathematics is an assertion that is either true or false. Consider the following examples:

- $3 + 56 - 13 + 8/2$.
- All cats are black.
- $2 + 3 = 5$.
- $2x = 6$ exactly when $x = 4$.
- If $ax^2 + bx + c = 0$ and $a \neq 0$, then
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$
- $x^3 - 4x^2 + 5x - 6$.

All but the first and last examples are statements, and must be either true or false.

A ***mathematical proof*** is nothing more than a convincing argument about the accuracy of a statement. Such an argument should contain enough detail to convince the audience; for

Preface

This text is intended for a one or two-semester undergraduate course in abstract algebra. Traditionally, these courses have covered the theoretical aspects of groups, rings, and fields. However, with the development of computing in the last several decades, applications that involve abstract algebra and discrete mathematics have become increasingly important, and many science, engineering, and computer science students are now electing to minor in mathematics. Though theory still occupies a central role in the subject of abstract algebra and no student should go through such a course without a good notion of what a proof is, the importance of applications such as coding theory and cryptography has grown significantly.

Until recently most abstract algebra texts included few if any applications. However, one of the major problems in teaching an abstract algebra course is that for many students it is their first encounter with an environment that requires them to do rigorous proofs. Such students often find it hard to see the use of learning to prove theorems and propositions; applied examples help the instructor provide motivation.

This text contains more material than can possibly be covered in a single semester. Certainly there is adequate material for a two-semester course, and perhaps more; however, for a one-semester course it would be quite easy to omit selected chapters and still have a useful text. The order of presentation of topics is standard: groups, then rings, and finally fields. Emphasis can be placed either on theory or on applications. A typical one-semester course might cover groups and rings while briefly touching on field theory, using Chapters 1 through 6, 9, 10, 11, 13 (the first part), 16, 17, 18 (the first part), 20, and 21. Parts of these chapters could be deleted and applications substituted according to the interests of the students and the instructor. A two-semester course emphasizing theory might cover Chapters 1 through 6, 9, 10, 11, 13 through 18, 20, 21, 22 (the first part), and 23. On the other hand, if applications are to be emphasized, the course might cover Chapters 1 through 14, and 16 through 22. In an applied course, some of the more theoretical results could be assumed or omitted. A chapter dependency chart appears below. (A broken line indicates a partial dependency.)

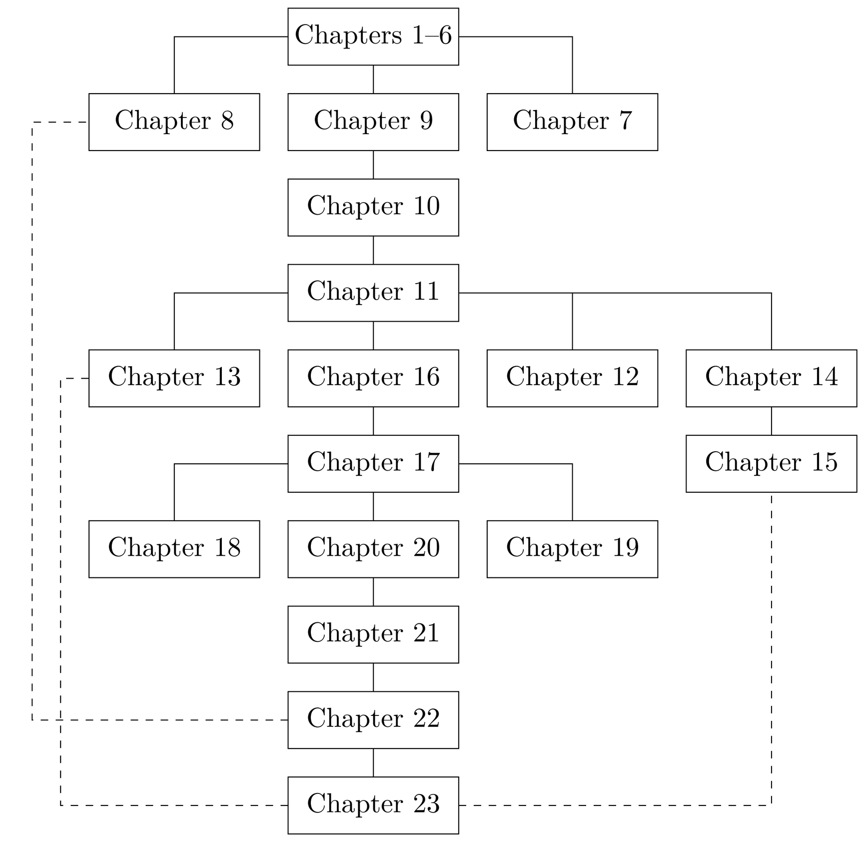
Contents

students should read the chapter before class and then answer the section's reading questions to prepare for the class.

There are additional exercises or computer projects at the ends of many of the chapters. The computer projects usually require a knowledge of programming. All of these exercises and projects are more substantial in nature and allow the exploration of new results and theory.

Sage (sagemath.org) is a free, open source, software system for advanced mathematics, which is ideal for assisting with a study of abstract algebra. Sage can be used either on your own computer, a local server, or on CoCalc (`cocalc.com`). Robert Beezer has written a comprehensive introduction to Sage and a selection of relevant exercises that appear at the end of each chapter, including live Sage cells in the web version of the book. All of the Sage code has been subject to automated tests of accuracy, using the most recent version available at this time: SageMath Version 9.3 (released 2021-05-09).

Thomas W. Judson
Nacogdoches, Texas 2021



Though there are no specific prerequisites for a course in abstract algebra, students who have had other higher-level courses in mathematics will generally be more prepared than those who have not, because they will possess a bit more mathematical sophistication. Occasionally, we shall assume some basic linear algebra; that is, we shall take for granted an elementary knowledge of matrices and determinants. This should present no great problem, since most students taking a course in abstract algebra have been introduced to matrices and determinants elsewhere in their career, if they have not already taken a sophomore or junior-level course in linear algebra.

Exercise sections are the heart of any mathematics text. An exercise set appears at the end of each chapter. The nature of the exercises ranges over several categories; computational, conceptual, and theoretical problems are included. A section presenting hints and solutions to many of the exercises appears at the end of the text. Often in the solutions a proof is only sketched, and it is up to the student to provide the details. The exercises range in difficulty from very easy to very challenging. Many of the more substantial problems require careful thought, so the student should not be discouraged if the solution is not forthcoming after a few minutes of work.

Ideally, students should read the relavent material before attending class. Reading questions have been added to each chapter before the exercises. To prepare for class,

instance, we can see that the statement "$2x = 6$ exactly when $x = 4$" is false by evaluating $2 \cdot 4$ and noting that $6 \neq 8$, an argument that would satisfy anyone. Of course, audiences may vary widely: proofs can be addressed to another student, to a professor, or to the reader of a text. If more detail than needed is presented in the proof, then the explanation will be either long-winded or poorly written. If too much detail is omitted, then the proof may not be convincing. Again it is important to keep the audience in mind. High school students require much more detail than do graduate students. A good rule of thumb for an argument in an introductory abstract algebra course is that it should be written to convince one's peers, whether those peers be other students or other readers of the text.

Let us examine different types of statements. A statement could be as simple as "$10/5 = 2$;" however, mathematicians are usually interested in more complex statements such as "If p, then q," where p and q are both statements. If certain statements are known or assumed to be true, we wish to know what we can say about other statements. Here p is called the ***hypothesis*** and q is known as the ***conclusion***. Consider the following statement: If $ax^2 + bx + c = 0$ and $a \neq 0$, then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

The hypothesis is $ax^2 + bx + c = 0$ and $a \neq 0$; the conclusion is

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Notice that the statement says nothing about whether or not the hypothesis is true. However, if this entire statement is true and we can show that $ax^2 + bx + c = 0$ with $a \neq 0$ is true, then the conclusion *must* be true. A proof of this statement might simply be a series of equations:

$$\begin{aligned} ax^2 + bx + c &= 0 \\ x^2 + \frac{b}{a}x &= -\frac{c}{a} \\ x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 &= \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \\ \left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \\ x + \frac{b}{2a} &= \frac{\pm\sqrt{b^2 - 4ac}}{2a} \\ x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \end{aligned}$$

If we can prove a statement true, then that statement is called a ***proposition***. A proposition of major importance is called a ***theorem***. Sometimes instead of proving a theorem or proposition all at once, we break the proof down into modules; that is, we prove several supporting propositions, which are called ***lemmas***, and use the results of these propositions to prove the main result. If we can prove a proposition or a theorem, we will often, with very little effort, be able to derive other related propositions called ***corollaries***.

Some Cautions and Suggestions

There are several different strategies for proving propositions. In addition to using different methods of proof, students often make some common mistakes when they are first learning

Edition: Annual Edition 2021

Website: `abstract.pugetsound.edu`

Abstract Algebra

Theory and Applications

Thomas W. Judson
Stephen F. Austin State University

Sage Exercises for Abstract Algebra
Robert A. Beezer
University of Puget Sound

Traducción al español
Antonio Behn
Universidad de Chile

August 9, 2021

how to prove theorems. To aid students who are studying abstract mathematics for the first time, we list here some of the difficulties that they may encounter and some of the strategies of proof available to them. It is a good idea to keep referring back to this list as a reminder. (Other techniques of proof will become apparent throughout this chapter and the remainder of the text.)

- A theorem cannot be proved by example; however, the standard way to show that a statement is not a theorem is to provide a counterexample.
- Quantifiers are important. Words and phrases such as *only*, *for all*, *for every*, and *for some* possess different meanings.
- Never assume any hypothesis that is not explicitly stated in the theorem. *You cannot take things for granted.*
- Suppose you wish to show that an object *exists* and is *unique*. First show that there actually is such an object. To show that it is unique, assume that there are two such objects, say r and s, and then show that $r = s$.
- Sometimes it is easier to prove the contrapositive of a statement. Proving the statement "If p, then q" is exactly the same as proving the statement "If not q, then not p."
- Although it is usually better to find a direct proof of a theorem, this task can sometimes be difficult. It may be easier to assume that the theorem that you are trying to prove is false, and to hope that in the course of your argument you are forced to make some statement that cannot possibly be true.

Remember that one of the main objectives of higher mathematics is proving theorems. Theorems are tools that make new and productive applications of mathematics possible. We use examples to give insight into existing theorems and to foster intuitions as to what new theorems might be true. Applications, examples, and proofs are tightly interconnected—much more so than they may seem at first appearance.

1.2 Sets and Equivalence Relations

Set Theory

A ***set*** is a well-defined collection of objects; that is, it is defined in such a manner that we can determine for any given object x whether or not x belongs to the set. The objects that belong to a set are called its ***elements*** or ***members***. We will denote sets by capital letters, such as A or X; if a is an element of the set A, we write $a \in A$.

A set is usually specified either by listing all of its elements inside a pair of braces or by stating the property that determines whether or not an object x belongs to the set. We might write

$$X = \{x_1, x_2, \ldots, x_n\}$$

for a set containing elements $x_1, x_2, \ldots, x_n$ or

$$X = \{x : x \text{ satisfies } \mathcal{P}\}$$

if each x in X satisfies a certain property $\mathcal{P}$. For example, if E is the set of even positive integers, we can describe E by writing either

$$E = \{2, 4, 6, \ldots\} \quad \text{or} \quad E = \{x : x \text{ is an even integer and } x > 0\}.$$

Theorem 2.9 Division Algorithm. *Let a and b be integers, with $b > 0$. Then there exist unique integers q and r such that*

$$a = bq + r$$

where $0 \leq r < b$.

PROOF. This is a perfect example of the existence-and-uniqueness type of proof. We must first prove that the numbers q and r actually exist. Then we must show that if q' and r' are two other such numbers, then $q = q'$ and $r = r'$.

Existence of q and r. Let

$$S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}.$$

If $0 \in S$, then b divides a, and we can let $q = a/b$ and $r = 0$. If $0 \notin S$, we can use the Well-Ordering Principle. We must first show that S is nonempty. If $a > 0$, then $a - b \cdot 0 \in S$. If $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. In either case $S \neq \emptyset$. By the Well-Ordering Principle, S must have a smallest member, say $r = a - bq$. Therefore, $a = bq + r$, $r \geq 0$. We now show that $r < b$. Suppose that $r > b$. Then

$$a - b(q + 1) = a - bq - b = r - b > 0.$$

In this case we would have $a - b(q + 1)$ in the set S. But then $a - b(q + 1) < a - bq$, which would contradict the fact that $r = a - bq$ is the smallest member of S. So $r \leq b$. Since $0 \notin S$, $r \neq b$ and so $r < b$.

Uniqueness of q and r. Suppose there exist integers r, r', q, and q' such that

$$a = bq + r, 0 \leq r < b \quad \text{and} \quad a = bq' + r', 0 \leq r' < b.$$

Then $bq + r = bq' + r'$. Assume that $r' \geq r$. From the last equation we have $b(q - q') = r' - r$; therefore, b must divide $r' - r$ and $0 \leq r' - r \leq r' < b$. This is possible only if $r' - r = 0$. Hence, $r = r'$ and $q = q'$. ■

Let a and b be integers. If $b = ak$ for some integer k, we write $a \mid b$. An integer d is called a ***common divisor*** of a and b if $d \mid a$ and $d \mid b$. The ***greatest common divisor*** of integers a and b is a positive integer d such that d is a common divisor of a and b and if d' is any other common divisor of a and b, then $d' \mid d$. We write $d = \gcd(a, b)$; for example, $\gcd(24, 36) = 12$ and $\gcd(120, 102) = 6$. We say that two integers a and b are ***relatively prime*** if $\gcd(a, b) = 1$.

Theorem 2.10 *Let a and b be nonzero integers. Then there exist integers r and s such that*

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

PROOF. Let

$$S = \{am + bn : m, n \in \mathbb{Z} \text{ and } am + bn > 0\}.$$

Clearly, the set S is nonempty; hence, by the Well-Ordering Principle S must have a smallest member, say $d = ar + bs$. We claim that $d = \gcd(a, b)$. Write $a = dq + r'$ where $0 \leq r' < d$. If $r' > 0$, then

$$\begin{aligned} r' &= a - dq \\ &= a - (ar + bs)q \\ &= a - arq - bsq \\ &= a(1 - rq) + b(-sq), \end{aligned}$$

Example 1.1 Let $\mathbb{R}$ be the universal set and suppose that

$$A = \{x \in \mathbb{R} : 0 < x \leq 3\} \quad \text{and} \quad B = \{x \in \mathbb{R} : 2 \leq x < 4\}.$$

Then

$$\begin{aligned} A \cap B &= \{x \in \mathbb{R} : 2 \leq x \leq 3\} \\ A \cup B &= \{x \in \mathbb{R} : 0 < x < 4\} \\ A \setminus B &= \{x \in \mathbb{R} : 0 < x < 2\} \\ A' &= \{x \in \mathbb{R} : x \leq 0 \text{ or } x > 3\}. \end{aligned}$$

□

Proposition 1.2 *Let A, B, and C be sets. Then*

1. *$A \cup A = A$, $A \cap A = A$, and $A \setminus A = \emptyset$;*
2. *$A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$;*
3. *$A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$;*
4. *$A \cup B = B \cup A$ and $A \cap B = B \cap A$;*
5. *$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;*
6. *$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*

PROOF. We will prove (1) and (3) and leave the remaining results to be proven in the exercises.

(1) Observe that

$$\begin{aligned} A \cup A &= \{x : x \in A \text{ or } x \in A\} \\ &= \{x : x \in A\} \\ &= A \end{aligned}$$

and

$$\begin{aligned} A \cap A &= \{x : x \in A \text{ and } x \in A\} \\ &= \{x : x \in A\} \\ &= A. \end{aligned}$$

Also, $A \setminus A = A \cap A' = \emptyset$.

(3) For sets A, B, and C,

$$\begin{aligned} A \cup (B \cup C) &= A \cup \{x : x \in B \text{ or } x \in C\} \\ &= \{x : x \in A \text{ or } x \in B, \text{ or } x \in C\} \\ &= \{x : x \in A \text{ or } x \in B\} \cup C \\ &= (A \cup B) \cup C. \end{aligned}$$

A similar argument proves that $A \cap (B \cap C) = (A \cap B) \cap C$. ■

Theorem 1.3 De Morgan's Laws. *Let A and B be sets. Then*

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

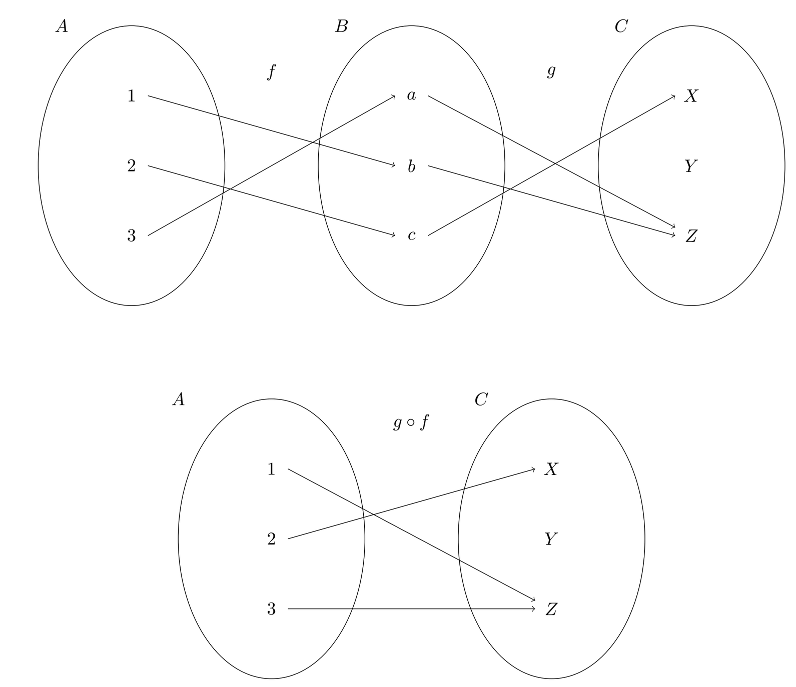


Figure 1.9 Composition of maps

Example 1.10 Consider the functions $f : A \to B$ and $g : B \to C$ that are defined in Figure 1.9 (top). The composition of these functions, $g \circ f : A \to C$, is defined in Figure 1.9 (bottom). □

Example 1.11 Let $f(x) = x^2$ and $g(x) = 2x + 5$. Then

$$(f \circ g)(x) = f(g(x)) = (2x + 5)^2 = 4x^2 + 20x + 25$$

and

$$(g \circ f)(x) = g(f(x)) = 2x^2 + 5.$$

In general, order makes a difference; that is, in most cases $f \circ g \neq g \circ f$. □

Example 1.12 Sometimes it is the case that $f \circ g = g \circ f$. Let $f(x) = x^3$ and $g(x) = \sqrt[3]{x}$. Then

$$(f \circ g)(x) = f(g(x)) = f(\sqrt[3]{x}\,) = (\sqrt[3]{x}\,)^3 = x$$

and

$$(g \circ f)(x) = g(f(x)) = g(x^3) = \sqrt[3]{x^3} = x.$$

□

Example 1.13 Given a 2×2 matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

2

The Integers

The integers are the building blocks of mathematics. In this chapter we will investigate the fundamental properties of the integers, including mathematical induction, the division algorithm, and the Fundamental Theorem of Arithmetic.

2.1 Mathematical Induction

Suppose we wish to show that

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

for any natural number n. This formula is easily verified for small numbers such as $n = 1$, 2, 3, or 4, but it is impossible to verify for all natural numbers on a case-by-case basis. To prove the formula true in general, a more generic method is required.

Suppose we have verified the equation for the first n cases. We will attempt to show that we can generate the formula for the $(n + 1)$th case from this knowledge. The formula is true for $n = 1$ since

$$1 = \frac{1(1+1)}{2}.$$

If we have verified the first n cases, then

$$\begin{aligned} 1 + 2 + \cdots + n + (n + 1) &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n^2 + 3n + 2}{2} \\ &= \frac{(n+1)[(n+1)+1]}{2}. \end{aligned}$$

This is exactly the formula for the $(n + 1)$th case.

This method of proof is known as ***mathematical induction***. Instead of attempting to verify a statement about some subset S of the positive integers $\mathbb{N}$ on a case-by-case basis, an impossible task if S is an infinite set, we give a specific proof for the smallest integer being considered, followed by a generic argument showing that if the statement holds for a given case, then it must also hold for the next case in the sequence. We summarize mathematical induction in the following axiom.

Principle 2.1 First Principle of Mathematical Induction. *Let $S(n)$ be a statement about integers for $n \in \mathbb{N}$ and suppose $S(n_0)$ is true for some integer n_0. If for all integers k with $k \geq n_0$, $S(k)$ implies that $S(k + 1)$ is true, then $S(n)$ is true for all integers n greater*

29. **Projective Real Line.** Define a relation on $\mathbb{R}^2 \setminus \{(0,0)\}$ by letting $(x_1, y_1) \sim (x_2, y_2)$ if there exists a nonzero real number λ such that $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. Prove that $\sim$ defines an equivalence relation on $\mathbb{R}^2 \setminus (0, 0)$. What are the corresponding equivalence classes? This equivalence relation defines the projective line, denoted by $\mathbb{P}(\mathbb{R})$, which is very important in geometry.

1.5 References and Suggested Readings

[1] Artin, M. *Algebra (Classic Version).* 2nd ed. Pearson, Upper Saddle River, NJ, 2018.

[2] Childs, L. *A Concrete Introduction to Higher Algebra.* 2nd ed. Springer-Verlag, New York, 1995.

[3] Dummit, D. and Foote, R. *Abstract Algebra.* 3rd ed. Wiley, New York, 2003.

[4] Ehrlich, G. *Fundamental Concepts of Algebra.* PWS-KENT, Boston, 1991.

[5] Fraleigh, J. B. *A First Course in Abstract Algebra.* 7th ed. Pearson, Upper Saddle River, NJ, 2003.

[6] Gallian, J. A. *Contemporary Abstract Algebra.* 7th ed. Brooks/Cole, Belmont, CA, 2009.

[7] Halmos, P. *Naive Set Theory.* Springer, New York, 1991. One of the best references for set theory.

[8] Herstein, I. N. *Abstract Algebra.* 3rd ed. Wiley, New York, 1996.

[9] Hungerford, T. W. *Algebra.* Springer, New York, 1974. One of the standard graduate algebra texts.

[10] Lang, S. *Algebra.* 3rd ed. Springer, New York, 2002. Another standard graduate text.

[11] Lidl, R. and Pilz, G. *Applied Abstract Algebra.* 2nd ed. Springer, New York, 1998.

[12] Mackiw, G. *Applications of Abstract Algebra.* Wiley, New York, 1985.

[13] Nickelson, W. K. *Introduction to Abstract Algebra.* 3rd ed. Wiley, New York, 2006.

[14] Solow, D. *How to Read and Do Proofs.* 5th ed. Wiley, New York, 2009.

[15] van der Waerden, B. L. *A History of Algebra.* Springer-Verlag, New York, 1985. An account of the historical development of algebra.

we can define a map $T_A : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$T_A(x, y) = (ax + by, cx + dy)$$

for (x, y) in $\mathbb{R}^2$. This is actually matrix multiplication; that is,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Maps from $\mathbb{R}^n$ to $\mathbb{R}^m$ given by matrices are called ***linear maps*** or ***linear transformations***. □

Example 1.14 Suppose that $S = \{1, 2, 3\}$. Define a map $\pi : S \to S$ by

$$\pi(1) = 2, \qquad \pi(2) = 1, \qquad \pi(3) = 3.$$

This is a bijective map. An alternative way to write π is

$$\begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

For any set S, a one-to-one and onto mapping $\pi : S \to S$ is called a ***permutation*** of S. □

Theorem 1.15 *Let $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then*

1. *The composition of mappings is associative; that is, $(h \circ g) \circ f = h \circ (g \circ f)$;*
2. *If f and g are both one-to-one, then the mapping $g \circ f$ is one-to-one;*
3. *If f and g are both onto, then the mapping $g \circ f$ is onto;*
4. *If f and g are bijective, then so is $g \circ f$.*

PROOF. We will prove (1) and (3). Part (2) is left as an exercise. Part (4) follows directly from (2) and (3).

(1) We must show that

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

For $a \in A$ we have

$$\begin{aligned} (h \circ (g \circ f))(a) &= h((g \circ f)(a)) \\ &= h(g(f(a))) \\ &= (h \circ g)(f(a)) \\ &= ((h \circ g) \circ f)(a). \end{aligned}$$

(3) Assume that f and g are both onto functions. Given $c \in C$, we must show that there exists an $a \in A$ such that $(g \circ f)(a) = g(f(a)) = c$. However, since g is onto, there is an element $b \in B$ such that $g(b) = c$. Similarly, there is an $a \in A$ such that $f(a) = b$. Accordingly,

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

■

If S is any set, we will use id_S or id to denote the ***identity mapping*** from S to itself. Define this map by $id(s) = s$ for all $s \in S$. A map $g : B \to A$ is an ***inverse mapping*** of $f : A \to B$ if $g \circ f = id_A$ and $f \circ g = id_B$; in other words, the inverse function of a function simply "undoes" the function. A map is said to be ***invertible*** if it has an inverse. We usually write f^{-1} for the inverse of f.

an invertible matrix P such that $PAP^{-1} = B$. For example, if

$$A = \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -18 & 33 \\ -11 & 20 \end{pmatrix},$$

then $A \sim B$ since $PAP^{-1} = B$ for

$$P = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}.$$

Let I be the 2×2 identity matrix; that is,

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then $IAI^{-1} = IAI = A$; therefore, the relation is reflexive. To show symmetry, suppose that $A \sim B$. Then there exists an invertible matrix P such that $PAP^{-1} = B$. So

$$A = P^{-1}BP = P^{-1}B(P^{-1})^{-1}.$$

Finally, suppose that $A \sim B$ and $B \sim C$. Then there exist invertible matrices P and Q such that $PAP^{-1} = B$ and $QBQ^{-1} = C$. Since

$$C = QBQ^{-1} = QPAP^{-1}Q^{-1} = (QP)A(QP)^{-1},$$

the relation is transitive. Two matrices that are equivalent in this manner are said to be ***similar***. □

A ***partition*** $\mathcal{P}$ of a set X is a collection of nonempty sets $X_1, X_2, \ldots$ such that $X_i \cap X_j = \emptyset$ for $i \neq j$ and $\bigcup_k X_k = X$. Let $\sim$ be an equivalence relation on a set X and let $x \in X$. Then $[x] = \{y \in X : y \sim x\}$ is called the ***equivalence class*** of x. We will see that an equivalence relation gives rise to a partition via equivalence classes. Also, whenever a partition of a set exists, there is some natural underlying equivalence relation, as the following theorem demonstrates.

Theorem 1.25 *Given an equivalence relation $\sim$ on a set X, the equivalence classes of X form a partition of X. Conversely, if $\mathcal{P} = \{X_i\}$ is a partition of a set X, then there is an equivalence relation on X with equivalence classes X_i.*

PROOF. Suppose there exists an equivalence relation $\sim$ on the set X. For any $x \in X$, the reflexive property shows that $x \in [x]$ and so $[x]$ is nonempty. Clearly $X = \bigcup_{x \in X} [x]$. Now let $x, y \in X$. We need to show that either $[x] = [y]$ or $[x] \cap [y] = \emptyset$. Suppose that the intersection of $[x]$ and $[y]$ is not empty and that $z \in [x] \cap [y]$. Then $z \sim x$ and $z \sim y$. By symmetry and transitivity $x \sim y$; hence, $[x] \subset [y]$. Similarly, $[y] \subset [x]$ and so $[x] = [y]$. Therefore, any two equivalence classes are either disjoint or exactly the same.

Conversely, suppose that $\mathcal{P} = \{X_i\}$ is a partition of a set X. Let two elements be equivalent if they are in the same partition. Clearly, the relation is reflexive. If x is in the same partition as y, then y is in the same partition as x, so $x \sim y$ implies $y \sim x$. Finally, if x is in the same partition as y and y is in the same partition as z, then x must be in the same partition as z, and transitivity holds. ■

Corollary 1.26 *Two equivalence classes of an equivalence relation are either disjoint or equal.*

Let us examine some of the partitions given by the equivalence classes in the last set of examples.

Example 1.27 In the equivalence relation in Example 1.21, two pairs of integers, (p, q) and (r, s), are in the same equivalence class when they reduce to the same fraction in its lowest terms. □

Example 1.28 In the equivalence relation in Example 1.22, two functions $f(x)$ and $g(x)$ are in the same partition when they differ by a constant. □

Example 1.29 We defined an equivalence class on $\mathbb{R}^2$ by $(x_1, y_1) \sim (x_2, y_2)$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Two pairs of real numbers are in the same partition when they lie on the same circle about the origin. □

Example 1.30 Let r and s be two integers and suppose that $n \in \mathbb{N}$. We say that r is ***congruent*** to s ***modulo*** n, or r is congruent to s mod n, if $r - s$ is evenly divisible by n; that is, $r - s = nk$ for some $k \in \mathbb{Z}$. In this case we write $r \equiv s \pmod{n}$. For example, $41 \equiv 17 \pmod{8}$ since $41 - 17 = 24$ is divisible by 8. We claim that congruence modulo n forms an equivalence relation of $\mathbb{Z}$. Certainly any integer r is equivalent to itself since $r - r = 0$ is divisible by n. We will now show that the relation is symmetric. If $r \equiv s \pmod{n}$, then $r - s = -(s - r)$ is divisible by n. So $s - r$ is divisible by n and $s \equiv r \pmod{n}$. Now suppose that $r \equiv s \pmod{n}$ and $s \equiv t \pmod{n}$. Then there exist integers k and l such that $r - s = kn$ and $s - t = ln$. To show transitivity, it is necessary to prove that $r - t$ is divisible by n. However,

$$r - t = r - s + s - t = kn + ln = (k + l)n,$$

and so $r - t$ is divisible by n.

If we consider the equivalence relation established by the integers modulo 3, then

$$\begin{aligned} [0] &= \{\ldots, -3, 0, 3, 6, \ldots\}, \\ [1] &= \{\ldots, -2, 1, 4, 7, \ldots\}, \\ [2] &= \{\ldots, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

Notice that $[0] \cup [1] \cup [2] = \mathbb{Z}$ and also that the sets are disjoint. The sets $[0]$, $[1]$, and $[2]$ form a partition of the integers.

The integers modulo n are a very important example in the study of abstract algebra and will become quite useful in our investigation of various algebraic structures such as groups and rings. In our discussion of the integers modulo n we have actually assumed a result known as the division algorithm, which will be stated and proved in Chapter 2. □

Sage. Sage is a powerful, open source, system for exact, numerical, and symbolic mathematical computations. Electronic versions of this text contain comprehensive introductions to the use of Sage to study abstract algebra, and include a set of exercises. These can be found at the book's website. Due to the format of this version of the text, at the end of each chapter we have just included brief suggestions of how Sage might be employed.

1.3 Reading Questions

1. What do relations and mappings have in common?
2. What makes relations and mappings different?
3. State carefully the three defining properties of an equivalence relation. In other words, do not just *name* the properties, give their definitions.
4. What is the big deal about equivalence relations? (Hint: Partitions.)

5. Describe a general technique for proving that two sets are equal.

1.4 Exercises

1. Suppose that

$$A = \{x : x \in \mathbb{N} \text{ and } x \text{ is even}\},$$
$$B = \{x : x \in \mathbb{N} \text{ and } x \text{ is prime}\},$$
$$C = \{x : x \in \mathbb{N} \text{ and } x \text{ is a multiple of } 5\}.$$

Describe each of the following sets.
(a) $A \cap B$
(b) $B \cap C$
(c) $A \cup B$
(d) $A \cap (B \cup C)$

2. If $A = \{a, b, c\}$, $B = \{1, 2, 3\}$, $C = \{x\}$, and $D = \emptyset$, list all of the elements in each of the following sets.
(a) $A \times B$
(b) $B \times A$
(c) $A \times B \times C$
(d) $A \times D$

3. Find an example of two nonempty sets A and B for which $A \times B = B \times A$ is true.

4. Prove $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$.

5. Prove $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

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

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

8. Prove $A \subset B$ if and only if $A \cap B = A$.

9. Prove $(A \cap B)' = A' \cup B'$.

10. Prove $A \cup B = (A \cap B) \cup (A \setminus B) \cup (B \setminus A)$.

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

12. Prove $(A \cap B) \setminus B = \emptyset$.

13. Prove $(A \cup B) \setminus B = A \setminus B$.

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

15. Prove $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

16. Prove $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

17. Which of the following relations $f : \mathbb{Q} \to \mathbb{Q}$ define a mapping? In each case, supply a reason why f is or is not a mapping.
(a) $f(p/q) = \dfrac{p+1}{p-2}$
(b) $f(p/q) = \dfrac{3p}{3q}$
(c) $f(p/q) = \dfrac{p+q}{q^2}$
(d) $f(p/q) = \dfrac{3p^2}{7q^2} - \dfrac{p}{q}$

18. Determine which of the following functions are one-to-one and which are onto. If the function is not onto, determine its range.
(a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x$
(b) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n^2 + 3$
(c) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \sin x$

on $S = \{1, 2, 3\}$, it is easy to see that the permutation defined by

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

is the inverse of π. In fact, any bijective mapping possesses an inverse, as we will see in the next theorem. □

Theorem 1.20 *A mapping is invertible if and only if it is both one-to-one and onto.*
PROOF. Suppose first that $f : A \to B$ is invertible with inverse $g : B \to A$. Then $g \circ f = id_A$ is the identity map; that is, $g(f(a)) = a$. If $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$, then $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$. Consequently, f is one-to-one. Now suppose that $b \in B$. To show that f is onto, it is necessary to find an $a \in A$ such that $f(a) = b$, but $f(g(b)) = b$ with $g(b) \in A$. Let $a = g(b)$.

Conversely, let f be bijective and let $b \in B$. Since f is onto, there exists an $a \in A$ such that $f(a) = b$. Because f is one-to-one, a must be unique. Define g by letting $g(b) = a$. We have now constructed the inverse of f. ■

Equivalence Relations and Partitions

A fundamental notion in mathematics is that of equality. We can generalize equality with equivalence relations and equivalence classes. An ***equivalence relation*** on a set X is a relation $R \subset X \times X$ such that

- $(x, x) \in R$ for all $x \in X$ (***reflexive property***);
- $(x, y) \in R$ implies $(y, x) \in R$ (***symmetric property***);
- (x, y) and $(y, z) \in R$ imply $(x, z) \in R$ (***transitive property***).

Given an equivalence relation R on a set X, we usually write $x \sim y$ instead of $(x, y) \in R$. If the equivalence relation already has an associated notation such as $=$, $\equiv$, or $\cong$, we will use that notation.

Example 1.21 Let p, q, r, and s be integers, where q and s are nonzero. Define $p/q \sim r/s$ if $ps = qr$. Clearly $\sim$ is reflexive and symmetric. To show that it is also transitive, suppose that $p/q \sim r/s$ and $r/s \sim t/u$, with q, s, and u all nonzero. Then $ps = qr$ and $ru = st$. Therefore,

$$psu = qru = qst.$$

Since $s \neq 0$, $pu = qt$. Consequently, $p/q \sim t/u$. □

Example 1.22 Suppose that f and g are differentiable functions on $\mathbb{R}$. We can define an equivalence relation on such functions by letting $f(x) \sim g(x)$ if $f'(x) = g'(x)$. It is clear that $\sim$ is both reflexive and symmetric. To demonstrate transitivity, suppose that $f(x) \sim g(x)$ and $g(x) \sim h(x)$. From calculus we know that $f(x) - g(x) = c_1$ and $g(x) - h(x) = c_2$, where c_1 and c_2 are both constants. Hence,

$$f(x) - h(x) = (f(x) - g(x)) + (g(x) - h(x)) = c_1 + c_2$$

and $f'(x) - h'(x) = 0$. Therefore, $f(x) \sim h(x)$. □

Example 1.23 For (x_1, y_1) and (x_2, y_2) in $\mathbb{R}^2$, define $(x_1, y_1) \sim (x_2, y_2)$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Then $\sim$ is an equivalence relation on $\mathbb{R}^2$. □

Example 1.24 Let A and B be 2×2 matrices with entries in the real numbers. We can define an equivalence relation on the set of 2×2 matrices, by saying $A \sim B$ if there exists

Example 1.16 The function $f(x) = x^3$ has inverse $f^{-1}(x) = \sqrt[3]{x}$ by Example 1.12. □

Example 1.17 The natural logarithm and the exponential functions, $f(x) = \ln x$ and $f^{-1}(x) = e^x$, are inverses of each other provided that we are careful about choosing domains. Observe that

$$f(f^{-1}(x)) = f(e^x) = \ln e^x = x$$

and

$$f^{-1}(f(x)) = f^{-1}(\ln x) = e^{\ln x} = x$$

whenever composition makes sense. □

Example 1.18 Suppose that

$$A = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}.$$

Then A defines a map from $\mathbb{R}^2$ to $\mathbb{R}^2$ by

$$T_A(x, y) = (3x + y, 5x + 2y).$$

We can find an inverse map of T_A by simply inverting the matrix A; that is, $T_A^{-1} = T_{A^{-1}}$. In this example,

$$A^{-1} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix};$$

hence, the inverse map is given by

$$T_A^{-1}(x, y) = (2x - y, -5x + 3y).$$

It is easy to check that

$$T_A^{-1} \circ T_A(x, y) = T_A \circ T_A^{-1}(x, y) = (x, y).$$

Not every map has an inverse. If we consider the map

$$T_B(x, y) = (3x, 0)$$

given by the matrix

$$B = \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix},$$

then an inverse map would have to be of the form

$$T_B^{-1}(x, y) = (ax + by, cx + dy)$$

and

$$(x, y) = T_B \circ T_B^{-1}(x, y) = (3ax + 3by, 0)$$

for all x and y. Clearly this is impossible because y might not be 0. □

Example 1.19 Given the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

(d) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$

19. Let $f : A \to B$ and $g : B \to C$ be invertible mappings; that is, mappings such that f^{-1} and g^{-1} exist. Show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

20.
(a) Define a function $f : \mathbb{N} \to \mathbb{N}$ that is one-to-one but not onto.
(b) Define a function $f : \mathbb{N} \to \mathbb{N}$ that is onto but not one-to-one.

21. Prove the relation defined on $\mathbb{R}^2$ by $(x_1, y_1) \sim (x_2, y_2)$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$ is an equivalence relation.

22. Let $f : A \to B$ and $g : B \to C$ be maps.
(a) If f and g are both one-to-one functions, show that $g \circ f$ is one-to-one.
(b) If $g \circ f$ is onto, show that g is onto.
(c) If $g \circ f$ is one-to-one, show that f is one-to-one.
(d) If $g \circ f$ is one-to-one and f is onto, show that g is one-to-one.
(e) If $g \circ f$ is onto and g is one-to-one, show that f is onto.

23. Define a function on the real numbers by

$$f(x) = \frac{x+1}{x-1}.$$

What are the domain and range of f? What is the inverse of f? Compute $f \circ f^{-1}$ and $f^{-1} \circ f$.

24. Let $f : X \to Y$ be a map with $A_1, A_2 \subset X$ and $B_1, B_2 \subset Y$.
(a) Prove $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
(b) Prove $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$. Give an example in which equality fails.
(c) Prove $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, where

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

(d) Prove $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.
(e) Prove $f^{-1}(Y \setminus B_1) = X \setminus f^{-1}(B_1)$.

25. Determine whether or not the following relations are equivalence relations on the given set. If the relation is an equivalence relation, describe the partition given by it. If the relation is not an equivalence relation, state why it fails to be one.
(a) $x \sim y$ in $\mathbb{R}$ if $x \geq y$
(b) $m \sim n$ in $\mathbb{Z}$ if $mn > 0$
(c) $x \sim y$ in $\mathbb{R}$ if $|x - y| \leq 4$
(d) $m \sim n$ in $\mathbb{Z}$ if $m \equiv n \pmod 6$

26. Define a relation $\sim$ on $\mathbb{R}^2$ by stating that $(a, b) \sim (c, d)$ if and only if $a^2 + b^2 \leq c^2 + d^2$. Show that $\sim$ is reflexive and transitive but not symmetric.

27. Show that an $m \times n$ matrix gives rise to a well-defined map from $\mathbb{R}^n$ to $\mathbb{R}^m$.

28. Find the error in the following argument by providing a counterexample. "The reflexive property is redundant in the axioms for an equivalence relation. If $x \sim y$, then $y \sim x$ by the symmetric property. Using the transitive property, we can deduce that $x \sim x$."

than or equal to n_0.

Example 2.2 For all integers $n \geq 3$, $2^n > n + 4$. Since

$$8 = 2^3 > 3 + 4 = 7,$$

the statement is true for $n_0 = 3$. Assume that $2^k > k + 4$ for $k \geq 3$. Then $2^{k+1} = 2 \cdot 2^k > 2(k + 4)$. But

$$2(k + 4) = 2k + 8 > k + 5 = (k + 1) + 4$$

since k is positive. Hence, by induction, the statement holds for all integers $n \geq 3$. □

Example 2.3 Every integer $10^{n+1} + 3 \cdot 10^n + 5$ is divisible by 9 for $n \in \mathbb{N}$. For $n = 1$,

$$10^{1+1} + 3 \cdot 10 + 5 = 135 = 9 \cdot 15$$

is divisible by 9. Suppose that $10^{k+1} + 3 \cdot 10^k + 5$ is divisible by 9 for $k \geq 1$. Then

$$\begin{aligned} 10^{(k+1)+1} + 3 \cdot 10^{k+1} + 5 &= 10^{k+2} + 3 \cdot 10^{k+1} + 50 - 45 \\ &= 10(10^{k+1} + 3 \cdot 10^k + 5) - 45 \end{aligned}$$

is divisible by 9. □

Example 2.4 We will prove the binomial theorem using mathematical induction; that is,

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k},$$

where a and b are real numbers, $n \in \mathbb{N}$, and

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

is the binomial coefficient. We first show that

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

This result follows from

$$\begin{aligned} \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{(n+1)!}{k!(n+1-k)!} \\ &= \binom{n+1}{k}. \end{aligned}$$

If $n = 1$, the binomial theorem is easy to verify. Now assume that the result is true for n greater than or equal to 1. Then

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n \\ &= (a + b)\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) \\ &= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \end{aligned}$$

Example 1.6 Suppose $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$. In Figure 1.7 we define relations f and g from A to B. The relation f is a mapping, but g is not because $1 \in A$ is not assigned to a unique element in B; that is, $g(1) = a$ and $g(1) = b$.

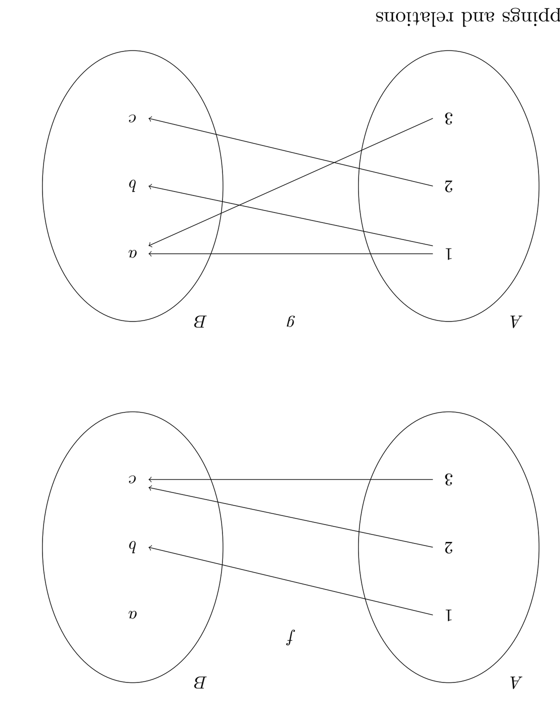


Figure 1.7 Mappings and relations

□

Given a function $f : A \to B$, it is often possible to write a list describing what the function does to each specific element in the domain. However, not all functions can be described in this manner. For example, the function $f : \mathbb{R} \to \mathbb{R}$ that sends each real number to its cube is a mapping that must be described by writing $f(x) = x^3$ or $f : x \mapsto x^3$.

Consider the relation $f : \mathbb{Q} \to \mathbb{Z}$ given by $f(p/q) = p$. We know that $1/2 = 2/4$, but is $f(1/2) = 1$ or 2? This relation cannot be a mapping because it is not well-defined. A relation is ***well-defined*** if each element in the domain is assigned to a *unique* element in the range.

If $f : A \to B$ is a map and the image of f is B, i.e., $f(A) = B$, then f is said to be ***onto*** or ***surjective***. In other words, if there exists an $a \in A$ for each $b \in B$ such that $f(a) = b$, then f is onto. A map is ***one-to-one*** or ***injective*** if $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$. Equivalently, a function is one-to-one if $f(a_1) = f(a_2)$ implies $a_1 = a_2$. A map that is both one-to-one and onto is called ***bijective***.

Example 1.8 Let $f : \mathbb{Z} \to \mathbb{Q}$ be defined by $f(n) = n/1$. Then f is one-to-one but not onto. Define $g : \mathbb{Q} \to \mathbb{Z}$ by $g(p/q) = p$ where p/q is a rational number expressed in its lowest terms with a positive denominator. The function g is onto but not one-to-one. □

Given two functions, we can construct a new function by using the range of the first function as the domain of the second function. Let $f : A \to B$ and $g : B \to C$ be mappings. Define a new map, the ***composition*** of f and g from A to C, by $(g \circ f)(x) = g(f(x))$.

PROOF. (1) If $A \cup B = \emptyset$, then the theorem follows immediately since both A and B are the empty set. Otherwise, we must show that $(A \cup B)' \subset A' \cap B'$ and $(A \cup B)' \supset A' \cap B'$. Let $x \in (A \cup B)'$. Then $x \notin A \cup B$. So x is neither in A nor in B, by the definition of the union of sets. By the definition of the complement, $x \in A'$ and $x \in B'$. Therefore, $x \in A' \cap B'$ and we have $(A \cup B)' \subset A' \cap B'$.

To show the reverse inclusion, suppose that $x \in A' \cap B'$. Then $x \in A'$ and $x \in B'$, and so $x \notin A$ and $x \notin B$. Thus $x \notin A \cup B$ and so $x \in (A \cup B)'$. Hence, $(A \cup B)' \supset A' \cap B'$ and so $(A \cup B)' = A' \cap B'$.

The proof of (2) is left as an exercise. ■

Example 1.4 Other relations between sets often hold true. For example,

$$(A \setminus B) \cap (B \setminus A) = \emptyset.$$

To see that this is true, observe that

$$\begin{aligned} (A \setminus B) \cap (B \setminus A) &= (A \cap B') \cap (B \cap A') \\ &= A \cap A' \cap B \cap B' \\ &= \emptyset. \end{aligned}$$

□

Cartesian Products and Mappings

Given sets A and B, we can define a new set $A \times B$, called the ***Cartesian product*** of A and B, as a set of ordered pairs. That is,

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

Example 1.5 If $A = \{x, y\}$, $B = \{1, 2, 3\}$, and $C = \emptyset$, then $A \times B$ is the set

$$\{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$$

and

$$A \times C = \emptyset.$$

□

We define the ***Cartesian product of*** n ***sets*** to be

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i \text{ for } i = 1, \ldots, n\}.$$

If $A = A_1 = A_2 = \cdots = A_n$, we often write A^n for $A \times \cdots \times A$ (where A would be written n times). For example, the set $\mathbb{R}^3$ consists of all of 3-tuples of real numbers.

Subsets of $A \times B$ are called ***relations***. We will define a ***mapping*** or ***function*** $f \subset A \times B$ from a set A to a set B to be the special type of relation where each element $a \in A$ has a unique element $b \in B$ such that $(a, b) \in f$. Another way of saying this is that for every element in A, f assigns a unique element in B. We usually write $f : A \to B$ or $A \xrightarrow{f} B$. Instead of writing down ordered pairs $(a, b) \in A \times B$, we write $f(a) = b$ or $f : a \mapsto b$. The set A is called the ***domain*** of f and

$$f(A) = \{f(a) : a \in A\} \subset B$$

is called the ***range*** or ***image*** of f. We can think of the elements in the function's domain as input values and the elements in the function's range as output values.

$$\begin{aligned} &= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k} + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k-1} + \binom{n}{k}\right] a^k b^{n+1-k} + b^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}. \end{aligned}$$

□

We have an equivalent statement of the Principle of Mathematical Induction that is often very useful.

Principle 2.5 Second Principle of Mathematical Induction. *Let $S(n)$ be a statement about integers for $n \in \mathbb{N}$ and suppose $S(n_0)$ is true for some integer n_0. If $S(n_0), S(n_0 + 1), \ldots, S(k)$ imply that $S(k + 1)$ for $k \geq n_0$, then the statement $S(n)$ is true for all integers $n \geq n_0$.*

A nonempty subset S of $\mathbb{Z}$ is ***well-ordered*** if S contains a least element. Notice that the set $\mathbb{Z}$ is not well-ordered since it does not contain a smallest element. However, the natural numbers are well-ordered.

Principle 2.6 Principle of Well-Ordering. *Every nonempty subset of the natural numbers is well-ordered.*

The Principle of Well-Ordering is equivalent to the Principle of Mathematical Induction.

Lemma 2.7 *The Principle of Mathematical Induction implies that 1 is the least positive natural number.*
PROOF. Let $S = \{n \in \mathbb{N} : n \geq 1\}$. Then $1 \in S$. Assume that $n \in S$. Since $0 < 1$, it must be the case that $n = n + 0 < n + 1$. Therefore, $1 \leq n < n + 1$. Consequently, if $n \in S$, then $n + 1$ must also be in S, and by the Principle of Mathematical Induction, and we have $S = \mathbb{N}$. ■

Theorem 2.8 *The Principle of Mathematical Induction implies the Principle of Well-Ordering. That is, every nonempty subset of $\mathbb{N}$ contains a least element.*
PROOF. We must show that if S is a nonempty subset of the natural numbers, then S contains a least element. If S contains 1, then the theorem is true by Lemma 2.7. Assume that if S contains an integer k such that $1 \leq k \leq n$, then S contains a least element. We will show that if a set S contains an integer less than or equal to $n + 1$, then S has a least element. If S does not contain an integer less than $n + 1$, then $n + 1$ is the smallest integer in S. Otherwise, since S is nonempty, S must contain an integer less than or equal to n. In this case, by induction, S contains a least element. ■

Induction can also be very useful in formulating definitions. For instance, there are two ways to define $n!$, the factorial of a positive integer n.

- The *explicit* definition: $n! = 1 \cdot 2 \cdot 3 \cdots (n - 1) \cdot n$.
- The *inductive* or *recursive* definition: $1! = 1$ and $n! = n(n - 1)!$ for $n > 1$.

Every good mathematician or computer scientist knows that looking at problems recursively, as opposed to explicitly, often results in better understanding of complex issues.

2.2 The Division Algorithm

An application of the Principle of Well-Ordering that we will use often is the division algorithm.