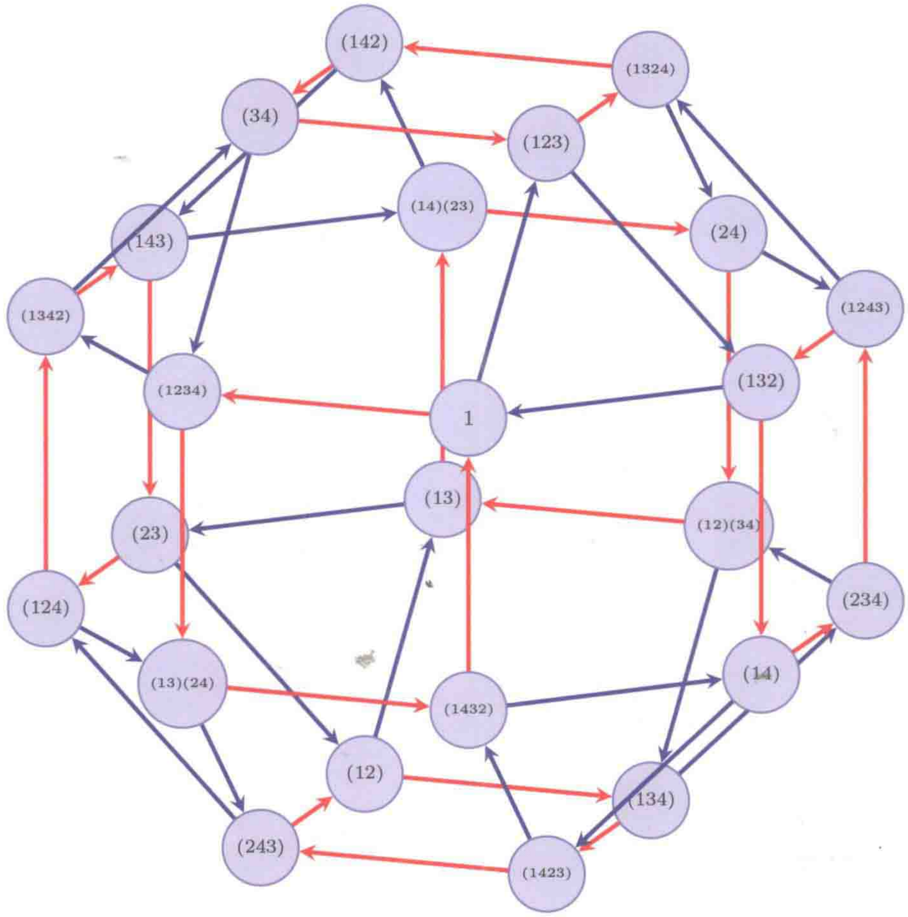
ABSTRACT ALGEBRA

STRUCTURES AND APPLICATIONS



STEPHEN LOVETT

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

ABSTRACT ALGEBRA

STRUCTURES AND APPLICATIONS

STEPHEN LOVETT
Wheaton College
Wheaton, Illinois, USA

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20150227

International Standard Book Number-13: 978-1-4822-4890-6 (Hardback)

Library of Congress Cataloging-in-Publication Data

Lovett, Stephen (Stephen T.)
Abstract algebra : structures and applications / Stephen Lovett, Wheaton College.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4822-4890-6 (alk. paper)
1. Algebra, Abstract--Textbooks. I. Title.

QA162.L68 2015
512'.02--dc23 2015006269

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY

ABSTRACT ALGEBRA

STRUCTURES AND APPLICATIONS

Preface

What Is Abstract Algebra?

When a student of mathematics studies abstract algebra, he or she inevitably faces questions in the vein of, "What makes the algebra abstract?" or "What is it good for?" or, more teasingly, "I finished algebra in high school; why are you still studying it as a math student?" Since undergraduate mathematics curriculum designers nearly always include an algebra requirement, then these questions illustrate the general lack of awareness by the general public about advanced mathematics. Consequently, we try to answer this question up front: "What is abstract algebra?"

Abstract algebra in its broadest sense describes a way of thinking about classes of mathematical objects. In contrast to high school algebra in which one studies properties of the operations (+, −, ×, and ÷) on real numbers, abstract algebra studies consequences of properties of operations without specifying what types of number or object we work with. Hence, any theorem established in the abstract context holds not only for real numbers but for every possible algebraic structure that has operations with the stated properties. Furthermore, some profound theorems in algebra, called *classification theorems*, enumerate all possible objects of a structure with a given property. Such theorems often lead to profound results when algebra is applied to other areas of mathematics.

Classical (high school) algebra, including vectors and algorithms to solve equations or systems of equations, finds applications in every area of natural and social sciences. Algebra has many applications in number theory, topology, geometry, analysis, and nearly every branch of mathematics. For nearly a hundred years, scientists have noted applications of abstract algebra to advanced physics, inorganic chemistry, and certain types of art. More recent applications include Boolean algebras in digital electronics, the mathematics of information security, and coding theory in telecommunications.

The general modern mindset of studying an algebraic structure has found applications in many areas: linguistics, machines, social networks, etc. Even in music, there exist some natural connections to algebra. A connection between music theory, both classical and atonal, and group theory has been studied recently. (See [34], [18], [13], or [24].) Recent attempts to codify atonal music borrowed from group theory more generally. Though there is not necessarily a direct connection between modern programming languages and abstract algebra, defining a class in object-oriented programming is reminiscent of how an algebraist defines an algebraic structure, and instantiating an object is not unlike an algebraist considering a specific object with that structure.

The fundamental importance of the notion of a structure in algebra has not escaped philosophers of mathematics. Structuralism, a recent position in the philosophy of mathematics, holds to a modified Platonist position that mathematical objects exist independent of human activity but that they always exist in reference to a structure. (See [58].)

Organizing Principles

Algebraic Structure. Many abstract algebra textbooks focus on three specific algebraic structures: groups, rings, and fields. These particular structures have indeed played important roles throughout mathematics and arguably deserve considerable attention. However, this book emphasizes the general concept of an algebraic structure as a unifying principle. Therefore, we present the core topics of structures following a consistent order and deliberately introduce the reader to other algebraic structures besides these standard three.

When studying a given algebraic structure, we follow this outline of topics:

- Definition of Structure—What are the axioms?
- Motivation—What value is there in minding this structure?

- Examples—What are some examples that demonstrate the scope and restrictions of a structure's definition?
- General Properties—What can we prove about all objects with a given structure?
- Important Objects—Are there some objects in this structure that are singularly important?
- Description—How do we conveniently describe an object with the given structure or elements in this structure?
- Subobjects—What can be said generally about the internal structure of a given object?
- Morphisms—What are the properties of functions that preserve the structure?
- Subclasses—What are some interesting subclasses of the structure that we can obtain by imposing additional conditions?
- Quotient Objects—Under what conditions do equivalence classes behave nicely with respect to the structure?
- Action Structures—Can we create some interesting/useful structures by considering how one structure might act on another?
- Applications—What are some other places this structure is used effectively?

For convenience in the rest of the text, we will often refer to this list simply as "the Outline." With a given structure, some of these topics may be brief and others lead to considerable investigation. Consequently, we do not give equal relative weight to these topics when studying various algebraic structures.

Algebraists may dislike the expression "algebraic structure" as it is not a well-defined mathematical term. Nonetheless, we use this term loosely until, in Chapter 13, we finally make the idea of algebraic structure rigorous by introducing categories.

Applications. The second guiding principle of this book is application of algebra. Examples, exercises, investigative projects, and whole sections, illustrate how abstract algebra is applied to other branches of mathematics or to areas of science. In addition, this textbook offers a few sections whose titles begin with "A Brief Introduction to..." These sections are just the trailhead for a whole branch of algebra and are intended to whet the student's appetite for further investigations and study.

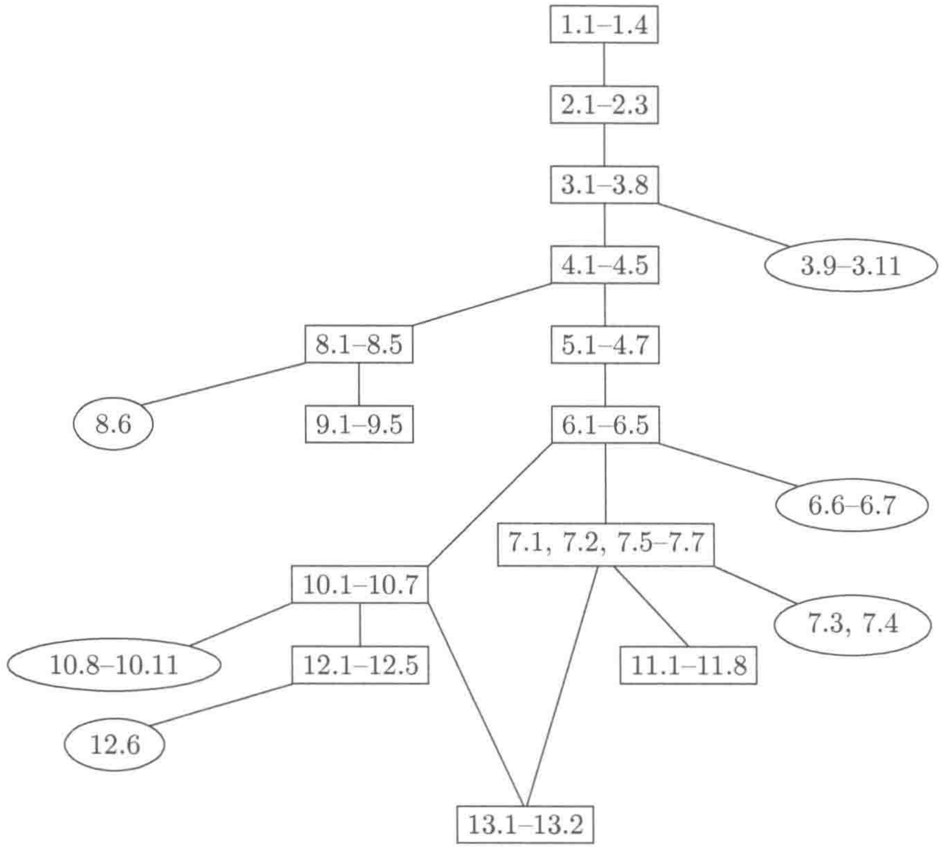
A Note to Instructors

Though covering groups, rings, and fields in detail, this textbook emphasizes the more general concept of an algebraic structure while simultaneously keeping an eye on applications. The style deliberately acknowledges the process of discovery, making this book suited for self-study.

This book is designed so that full coverage of all the sections will fill a two-semester sequence, with the semester split occurring between Chapters 7 and 8. However, it can be used for a one-semester introductory course in abstract algebra with many possible variations.

There are a variety of pathways to work through this textbook. Some colleges require a robust discrete mathematics background or transition course before abstract algebra. In this case, Chapters 1 and 2, which cover some basic set theory and a few motivating number theory concepts, might serve as a review or could be skipped entirely. Some application sections or topic sections are not essential for the development of later theory.

Each section was written with the intent to fill a one-hour lecture. Occasionally, some subsections carry the label (Optional). These optional subsections are not needed for further theory outside that section but offer additional perspective. In the dependency chart below, sections in rectangles represent core theory and build on each other within the boxes. Sections in ellipses are application or "brief introduction" sections and can generally be done in any order within the ellipse.



A Note to Students

From a student's perspective, one of the biggest challenges to modern algebra is its abstraction. A student taking a first course in modern algebra quickly discovers that most of the exercises are proofs. Calculus, linear algebra, and differential equations can be taught from many perspectives but often a preponderance of exercises simply require the student to carefully follow a certain prescribed algorithm. In algebra, a student does not typically learn many algorithms to solve a specific range of problems. Instead, he or she is expected to prove new results using the theorems presented in the text. By doing exercises, the student becomes an active participant in the development of the field. This common aspect of algebraic textbooks is very valuable because it trains the student in the methods of mathematical investigation. In this textbook, however, for many exercises (though not all) the student will find a similar example in the section that will illustrate a useful strategy.

The text includes many properties of the objects we study. However, this does not mean that everything that is interesting or even useful for some further result is proved or even mentioned in the text. If every interesting fact were proved in the text, this book would swell to unwieldy proportions and regularly digress from a coherent presentation. Consequently, to get a full experience of the material, the reader is encouraged to peruse the exercises in order to absorb many consequences of the theory.

Computer Algebra Systems (CAS)

There exist a number of general computer algebra systems (CAS) (e.g., *Maple* and *Mathematica*) that provide packages that offer commands that implement certain calculations that are useful in algebra. There also exist a number of free CAS that are specifically designed for computations in algebra (e.g., *Magma* and *Macaulay2*). It is impossible in such a textbook to offer a tutorial on each one or give a complete description of the full functionality of the commands. However, occasionally a section ends with a subsection that lists a few commands or libraries of commands that are relevant to that section. Unless otherwise indicated, it is generally expected that the computations in the exercises be done by hand and would not require the use of a computer algebra system. Whether a specific command is listed or whether a library of commands is given, the reader should visit the CAS's help page for specific examples on how to use that given command or to see what functions are in the library.

Investigative Projects

Another feature of this book are the investigative projects. In addition to regular exercises, at the end of most chapters, there is a list of ideas for investigative projects. The idea of assigning projects stems from a pedagogical experiment to challenge all students to write investigative or expository mathematical papers in undergraduate classes. As a paper, the projects should be (1) Clear: Use proper prose, follow the structure of a paper and provide proper references; (2) Correct: Proofs and calculations must be accurate; (3) Complete: Address all the questions or questions one should naturally address associated to the investigation; (4) Creative: Evidence creative problem-solving or question-asking skills.

These project ideas stand as guidelines. A reader who tackles one is encouraged to add his or her own investigations. While some questions associated to a project idea are precise and lead to well-defined answers, other questions are left vague on purpose, might not have clear cut solutions, or lead to open-ended problems. Some questions require proofs while others may benefit from technology: calculator work, a computer program, or a computer algebra system.

The ideas in some projects are known and have been developed in articles, books, or online resources. Consequently, if the investigative project is an assignment, then the student should generally not consult online resources besides the ones allowed by the project description. Otherwise, the project ideas may offer topics for further reading.

Habits of Notation

This book uses without explanation the logic quantifiers $\forall$, to be read as "for all," $\exists$, to be read as "there exists," and $\exists!$, to be read as "there exists a unique." We also regularly use $\Longrightarrow$ for logical implication and $\Longleftrightarrow$ logical equivalence. More precisely, if $P(x, y, \ldots)$ is a predicate with some variables and $Q(x, y, \ldots)$ is another predicate using the same variables, then

$$P(x,y,\ldots) \Longrightarrow Q(x,y,\ldots) \quad \text{means} \quad \forall x \forall y \ldots \big[P(x,y,\ldots) \longrightarrow Q(x,y,\ldots)\big]$$

and

$$P(x,y,\ldots) \Longleftrightarrow Q(x,y,\ldots) \quad \text{means} \quad \forall x \forall y \ldots \big[P(x,y,\ldots) \longleftrightarrow Q(x,y,\ldots)\big].$$

As another habit of language, this textbook is careful to always and only use the expression "Assume [hypothesis]" as the beginning of a proof by contradiction. Like so, the reader can know ahead of time that whenever she sees this expression, the hypothesis will eventually lead to a contradiction.

Acknowledgments

I must first thank the mathematics majors at Wheaton College (IL) who served for many years as the test environment for many topics, exercises, and projects. I am indebted to Wheaton College (IL) for the funding provided through the Aldeen Grant that contributed to portions of this textbook. I especially thank the students who offered specific feedback on the draft versions of this book, in particular Kelly McBride, Roland Hesse, and David Garringer. Joel Stapleton, Caleb DeMoss, Daniel Bradley, and Jeffrey Burge deserve special gratitude for working on the solutions manual to the textbook. I also must thank Justin Brown for test running the book and offering valuable feedback. I also thank Africa Nazarene University for hosting my sabbatical, during which I wrote a major portion of this textbook. Finally, I must absolutely thank the publishing and editing team at Taylor & Francis for their work in making this project become a reality.

Contents

1. Set Theory

Set theory sits at the foundation of all of modern mathematics.

Just as Boolean logic provides a rigorous framework to how we think, set theory provides a similarly precise framework for how we mentally gather instances of objects into classes. Notions from set theory such as relations, equivalences, operations, functions, etc. give a logically rigorous way to ascribe properties to objects or to think of how classes of objects are in relation to one another or to consider how two objects might be combined to make another object. Consequently, the terminology and notation of set theory provides a concise way to say many different things, mathematical or otherwise, with exacting precision.

Nearly every algebraic structure begins with a set as its first piece of data. Hence, familiarity with the fundamentals of set theory is essential for modern algebra. More importantly for the perspective of this textbook, set theory also provides us a basic example of an algebraic structure. The properties and concepts we choose to highlight in set theory focus on topics needed later, but also serve as a template for our study of other algebraic structures.

Since set theory serves as a preliminary topic to algebra, this chapter only offers a quick introduction to sets. For many readers this will be a review. Section 1.1 presents the notion of sets, subsets, operations on subsets, and functions between sets. Section 1.2 begins by introducing the Cartesian product of two sets and proceeds to discuss standard concepts related to sets that become available with the notion of the Cartesian product: binary operations on sets and relations. Section 1.3 discusses equivalence relations, equivalence classes, partitions, and quotient sets. This chapter concludes with an introduction to partial orders in Section 1.4, where we present posets as a first example of a nontrivial algebraic structure.

1.1 Sets and Functions

In mathematics, the concept of a set makes precise the notion of a collection of things. As broad as this concept appears, it is foundational for modern mathematics.

1.1.1 – Sets

Definition 1.1.1

(1) A *set* is a collection of objects for which there is a clear rule to determine whether an object is included or excluded.

(2) An object in a set is called an *element* of that set. We write $x \in A$ to mean "the element x is an element of the set A." We write $x \notin A$ if x is not an element of A.

Alternate expressions for $x \in A$ include "x is in A" or "A contains x."

Some examples of sets include the registered voters in Illinois, or the man-made structures above 800 feet tall. Both of these examples have clear rules that allow someone with enough information to clearly determine whether a given object is included in the collection or not. In natural languages, we regularly use terms or expressions that we treat as sets but in fact do not have a clear rule. For example, I cannot legitimately talk about the set of "my friends." There are some people, for whom, at a given point in time, I am hard pressed to say whether I consider them a friend or not.

In contrast, the people listed as "Friends" or "Contacts" on someone's preferred social networking site does form a set. As another nonexample of a set, consider the collection of all chairs. Whether this is a set is debatable. Indeed, by some artistic or functional failure, a piece of furniture may not be comfortable enough to sit on. Furthermore, should we consider a rock beside a hiking trail as a chair if we happen to sit on it?

Some discussion in logic is appropriate here. Set theory based on this idea of a "clear rule" is called *naive set theory* [33]. The idea of a clear rule in set theory is as precise as Boolean logic, which calls a *proposition* any statement for which there a clear rule to decide whether it is true or false. However, like Russell's Paradox in logic (e.g., consider the truth value of the statement "This sentence is false."), naive set theory ultimately can lead to contradictions. For example, if S is the set of all sets that do not contain themselves, does S contain itself? The Zermelo-Fraenkel axioms of set theory, denoted **ZF**, offer more technical foundations and avoid these contradictions. (See [47] for a presentation of set theory with **ZF**. See [25] for a philosophical discussion of **ZF** axioms.)

The most widely utilized form of set theory adds one axiom to the standard **ZF**, the so-called Axiom of Choice, and the resulting set of axioms is denoted by **ZFC**. Occasionally, certain theorems emphasize when their proofs directly utilize the Axiom of Choice. The reason for this is primarily historical. In the context of **ZF**, the Axiom of Choice implies many statements that seem downright obvious and others that feel counterintuitive. Consequently, there is a habit in mathematical literature to make clear when a certain result (and all results that use it as a hypothesis) rely on the Axiom of Choice.

A thorough treatment of axiomatic set theory would detract from an introduction to abstract algebra. Naive set theory will suffice for our purposes. Whenever we need a technical aspect of set theory, we provide appropriate references. The interested reader is encouraged to consult [21, 39, 62] for a deeper treatment of set theory.

Some sets occur so frequently in mathematics that they have their own standard notation. Here are a few:

- Standard sets of numbers:
  - $\mathbb{N}$ is the set of natural numbers (includes 0).
  - $\mathbb{Z}$ is the set of integers.
  - $\mathbb{Q}$ is the set of rational numbers.
  - $\mathbb{R}$ is the set of real numbers.
  - $\mathbb{C}$ is the set of complex numbers.
- Sometimes we use modifiers to the above sets. For example, $\mathbb{R}^+$ denotes the set of nonnegative reals and $\mathbb{R}^{<0}$ denotes the set negative (strictly) reals.
- A modifier we use consistently in this book is $\mathbb{N}^*$, $\mathbb{Z}^*$, etc. to stand for the given number set excluding 0. In particular, $\mathbb{N}^*$ denotes the set of positive integers.
- $\emptyset$, called the *empty set*, is the set that contains no elements.
- Intervals of real numbers:
  - $[a, b]$ denotes the closed interval of real numbers between a and b inclusive.
  - $[a, b)$ is the interval or reals between a and b, including a but not b.
  - $[a, \infty)$ is the interval of all real numbers greater than or equal to a.
  - Other self-explanatory combinations are possible such as (a, b); $(a, b]$; (a, ∞); $(-\infty, b]$; and $(-\infty, b)$.

There are two common notations for defining sets. Both of them explicitly provide the clear rule as to whether an object is in or out. However, in either case, the parentheses { marks the beginning of the defining rule and } marks the end.

(1) List the elements. For example, writing $S = \{1, 3, 7\}$ means that the set S is comprised of the three integers 1, 3, and 7. It is important to note that in this notation, order does not matter and we do not list numbers more than once. We only care about whether a certain object is in or not; we don't care about order or repetitions. (It is important to note that what we write in the list is merely a signifier that points to the actual object. Hence, the symbol 1 is pointing to the mathematical object of "one." Similarly, I may write $F = \{AL, CL, SL\}$ as a set of three elements that describes my family where the symbols AL, CL, and SL are pointers to the actual objects in the set, namely my daughter, my wife, and myself.)

(2) Explicitly state a defining property. For example,

$$\{x \mid x \text{ is a rational number with } x^2 < 2\}$$

means the set of all x such that x is a rational number such that $x^2 < 2$. Since we already have a set label for the rational numbers, we will usually rewrite this more concisely as

$$\{x \in \mathbb{Q} \mid x^2 < 2\}$$

and read it as, "the set of rational numbers x such that $x^2 < 2$." An alternate notation for this construction is $\{x \in \mathbb{Q} : x^2 < 2\}$.

Two sets A and B are considered equal when $x \in A \iff x \in B$, or in other words, they have exactly the same elements. We write $A = B$ to denote set equality.

1.1.2 – Subsets and Operations

When working with sets, it is common to work within a context set and consider sets within this context. For example, if a given problem or discussion only involves the set of living people, then we will only be interested in considering sets that exist within this context set.

Definition 1.1.2

A set A is called a *subset* of a set S if $x \in A \implies x \in S$. In other words, every element of A is an element of S. We write $A \subseteq S$.

The symbol $\subseteq$ should remind the reader of the symbol $\leq$ on the real numbers. This similarity of notation might inspire us to assume that $A \subset B$ would, like the strict inequality symbol $<$, mean $A \subseteq B$ and $A \neq B$. Unfortunately, by a fluke of historical inconsistency in notation, some authors do use the $\subset$ symbol to mean a strict subset, while others use it synonymously with $\subseteq$. To remove confusion, we use the symbol $A \subsetneq B$ to mean $A \subset B$ and $A \neq B$. The symbol $A \not\subseteq B$ means that A is not a subset of B.

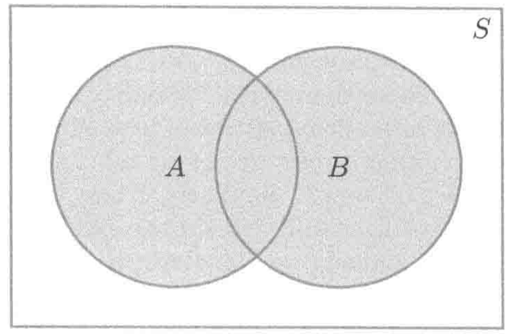
Example 1.1.3. Let $C^0([2,5])$ denote the set of continuous real-valued functions on the interval $[2,5]$ and let $C^1([2,5])$ denote the set of differentiable functions whose derivative is continuous on the interval $[2,5]$. The statement that

$$C^1([2,5]) \subseteq C^0([2,5])$$

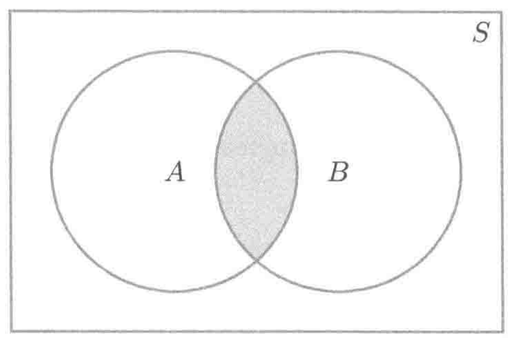
follows from the nontrivial result in analysis that if a function is differentiable over a closed interval, it is continuous over that interval. △

There are a few basic operations on subsets of a given set S. In the following list, we define operations on subsets A and B of S and provide corresponding Venn diagrams, in which the shaded portion illustrates the result of the operation.

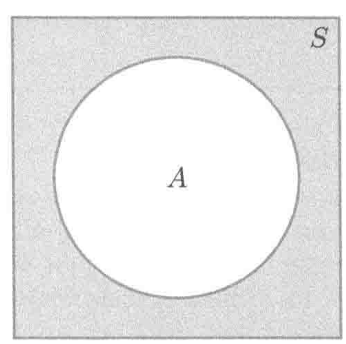
- The *union* of A and B is $A \cup B = \{x \in S \mid x \in A \text{ or } x \in B\}$.



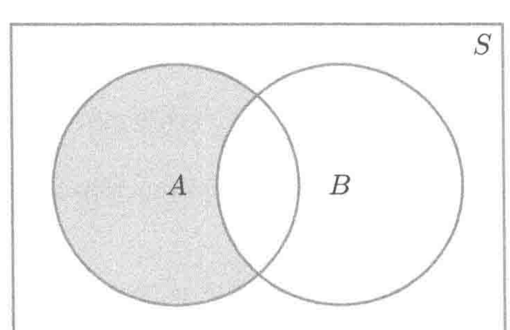
- The *intersection* of A and B is $A \cap B = \{x \in S \,|\, x \in A \text{ and } x \in B\}$.



- The *complement* of A is $\overline{A} = \{x \in S \,|\, x \notin A\}$.



- The *set difference* of B from A is $A - B = \{x \in S \,|\, x \in A \text{ and } x \notin B\}$.



- The *symmetric difference* of A and B is $A \triangle B = \{x \in S \,|\, x \in A \text{ or } x \in B \text{ but } x \notin A \cap B\}$.