Sections 14 and 15, Sections 26-28, Section 17, or Sections 30 and 31. One semester I attempted to cover enough field extension material in order to cover Section 41. This required me to carefully select material in Sections 27, 28, 39, and 40 in order to prepare the students for Section 41.

For the second semester, I usually have as goals proving the impossibility of bisecting an angle using compass and straightedge and the insolvability of quintic polynomials. Assuming that students have seen the basic material in the first semester as described above, these goals require covering material from Sections 16, 18, 27, 28, 30, 31, 33, 34, and 39-49. This turns out to be an ambitious undertaking, but the purpose of rewriting Part IX was to make the material more accessible to students, and therefore make the goal of covering Galois Theory in a second-semester class more feasible.

Acknowledgments

I am very grateful to those who have reviewed the text or who have sent suggestions and corrections. Below is a list of faculty who contributed their thoughts on improving the text.

- Deb Bergstrand, Swarthmore College
- Anthony E. Clement, Brooklyn College
- Richard M. Green, University of Colorado
- Cheryl Grood, Swarthmore College
- Gary Gordon, Lafayette College
- John Harding, New Mexico State University
- Timothy Kohl, Boston University
- Cristian Lenart, University at Albany, SUNY
- Mariana Montiel, Georgia Southern University
- Anne Shiu, Texas A&M University
- Mark Stankus, California Polytechnic State University
- Janet Vassilev, University of New Mexico
- Cassie L. Williams, James Madison University
- T. E. Williamson, Montclair State University
- Michael Zuker, Massachusetts Institute of Technology

I also wish to express appreciation to Jeff Weidenaar, Tara Corpuz, and Jon Krebs at Pearson for their help with this project.

Neal Brand
University of North Texas

Student's Preface

This course may well require a different approach than those you used in previous mathematics courses. You may have become accustomed to working a homework problem by turning back in the text to find a similar problem, and then just changing some numbers. That may work with a few problems in this text, but it will not work for most of them. This is a subject in which understanding is all-important, and where problems should not be tackled without first studying the text.

Let us make some suggestions on studying the text. Notice that the text bristles with definitions, theorems, corollaries, and examples. The definitions are crucial. We must agree on terminology to make any progress. Sometimes a definition is followed by an example that illustrates the concept. Examples are probably the most important aids in studying the text. *Pay attention to the examples.*

Before reading a section, it may be helpful to watch the video associated with the section. I have two general pieces of advice for watching a video or reading the text. First, minimize your distractions. It takes a good deal of concentration for most of us to learn new technical information. Second, have paper and pen (or the electronic equivalent) at hand to take notes and to occasionally work out computations on your own.

I suggest you skip the proofs of the theorems on your first reading of a section, unless you are really “gung-ho” on proofs. You should read the statement of the theorem and try to understand just what it means. Often, a theorem is followed or preceded by an example that illustrates it, which is a great aid in really understanding what the theorem says. Pay particular attention to the summary at the end of each video to get an overview of the topics covered.

In summary, on your first viewing and reading of a section, I suggest you concentrate on what information the section gives and on gaining a real understanding of it. If you do not understand what the statement of a theorem means, it will probably be meaningless for you to read the proof.

Proofs are basic to mathematics. After you feel you understand the information given in a section, you should read and try to understand at least some of the proofs. In the videos you will find a few proofs. Watching the videos a second time after you have a better understanding of the definitions and the statements of the theorems will help to clarify these proofs. Proofs of corollaries are usually the easiest ones, for they often follow directly from the theorem. Many of the exercises under the ”Theory” heading ask for a proof. Try not to be discouraged at the outset. It takes a bit of practice and experience. Proofs in algebra can be more difficult than proofs in geometry and calculus, for there are usually no suggestive pictures that you can draw. Often, a proof falls out easily if you happen to look at just the right expression. Of course, it is hopeless to devise a proof if you do not really understand what it is that you are trying to prove. For example, if an exercise asks you to show that a given thing is a member of a certain set, you must *know* the defining criterion for a thing to be a member of that set, and then show that your given thing satisfies that criterion.

There are several aids for your study at the back of the text. Of course, you will discover the answers to odd-numbered problems that do not involve a proof. If you run into a notation such as Z_n that you do not understand, look in the list of notations that appears after the bibliography. If you run into terminology like *inner automorphism* that you do not understand, look in the index for the first page where the term occurs.

In summary, although an understanding of the subject is important in every mathematics course, it is crucial to your performance in this course. May you find it a rewarding experience.

SECTION 0 Sets and Relations

On Definitions, and the Notion of a Set

Many students do not realize the great importance of definitions to mathematics. This importance stems from the need for mathematicians to communicate with each other. If two people are trying to communicate about some subject, they must have the same understanding of its technical terms. However, there is an important structural weakness.

It is impossible to define every concept.

Suppose, for example, we define the term *set* as "A **set** is a well-defined collection of objects." One naturally asks what is meant by a *collection.* We could define it as "A collection is an aggregate of things." What, then, is an *aggregate?* Now our language is finite, so after some time we will run out of new words to use and have to repeat some words already examined. The definition is then circular and obviously worthless. Mathematicians realize that there must be some undefined or primitive concept with which to start. At the moment, they have agreed that *set* shall be such a primitive concept. We shall not define *set,* but shall just hope that when such expressions as "the set of all real numbers" or "the set of all members of the United States Senate" are used, people's various ideas of what is meant are sufficiently similar to make communication feasible.

We summarize briefly some of the things we shall simply assume about sets.

1. A set S is made up of **elements,** and if a is one of these elements, we shall denote this fact by $a \in S$.
2. There is exactly one set with no elements. It is the **empty set** and is denoted by $\varnothing$.
3. We may describe a set either by giving a characterizing property of the elements, such as "the set of all members of the United States Senate," or by listing the elements. The standard way to describe a set by listing elements is to enclose the designations of the elements, separated by commas, in braces, for example, $\{1, 2, 15\}$. If a set is described by a characterizing property $P(x)$ of its elements x, the brace notation $\{x \mid P(x)\}$ is also often used, and is read "the set of all x such that the statement $P(x)$ about x is true." Thus

$$\begin{aligned}\{2,4,6,8\} &= \{x \mid x \text{ is an even whole positive number} \leq 8\}\\ &= \{2x \mid x = 1,2,3,4\}.\end{aligned}$$

   The notation $\{x \mid P(x)\}$ is often called "set-builder notation."

4. A set is **well defined,** meaning that if S is a set and a is some object, then either a is definitely in S, denoted by $a \in S$, or a is definitely not in S, denoted by $a \notin S$. Thus, we should never say, "Consider the set S of some positive numbers," for it is not definite whether $2 \in S$ or $2 \notin S$. On the other hand, we can consider the set T of all prime positive integers. Every positive integer is definitely either prime or not prime. Thus $5 \in T$ and $14 \notin T$. It may be hard to actually determine whether an object is in a set. For example, as this book goes to press it is probably unknown whether $2^{(2^{65})} + 1$ is in T. However, $2^{(2^{65})} + 1$ is certainly either prime or not prime.

It is not feasible for this text to push the definition of everything we use all the way back to the concept of a set. For example, we will never define the number π in terms of a set.

Every definition is an *if and only if* type of statement.

With this understanding, definitions are often stated with the *only if* suppressed, but it is always to be understood as part of the definition. Thus we may define an isosceles triangle as follows: "A triangle is **isosceles** if it has two congruent sides" when we really mean that a triangle is isosceles *if and only if* it has two congruent sides.

In our text, we have to define many terms. We use specifically labeled and numbered definitions for the main algebraic concepts with which we are concerned. To avoid an overwhelming quantity of such labels and numberings, we define many terms within the body of the text and exercises using boldface type.

Boldface Convention

A term printed **in boldface** in a sentence is being defined by that sentence.

Do not feel that you have to memorize a definition word for word. The important thing is to *understand* the concept, so that you can define precisely the same concept in your own words. Thus the definition "An **isosceles** triangle is one having two sides of equal length" is perfectly correct. Of course, we had to delay stating our boldface convention until we had finished using boldface in the preceding discussion of sets, because we do not define a set!

In this section, we do define some familiar concepts as sets, both for illustration and for review of the concepts. First we give a few definitions and some notation.

0.1 Definition A set B is a **subset of a set** A, denoted by $B \subseteq A$ or $A \supseteq B$, if every element of B is in A. The notations $B \subset A$ or $A \supset B$ will be used for $B \subseteq A$ but $B \neq A$. ■

Note that according to this definition, for any set A, A itself and $\varnothing$ are both subsets of A.

0.2 Definition If A is any set, then A is the **improper subset of** A. Any other subset of A is a **proper subset of** A. ■

0.3 Example Let $S = \{1, 2, 3\}$. This set S has a total of eight subsets, namely $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, and $\{1, 2, 3\}$. ▲

0.4 Definition Let A and B be sets. The set $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$ is the **Cartesian product** of A and B. ■

0.5 Example If $A = \{1, 2, 3\}$ and $B = \{3, 4\}$, then we have

$$A \times B = \{(1,3), (1,4), (2,3), (2,4), (3,3), (3,4)\}. \qquad ▲$$

Throughout this text, much work will be done involving familiar sets of numbers. Let us take care of notation for these sets once and for all.

$\mathbb{Z}$ is the set of all integers (that is, whole numbers: positive, negative, and zero).

$\mathbb{Q}$ is the set of all rational numbers (that is, numbers that can be expressed as quotients m/n of integers, where $n \neq 0$).

$\mathbb{R}$ is the set of all real numbers.

$\mathbb{Z}^+$, $\mathbb{Q}^+$, and $\mathbb{R}^+$ are the sets of positive members of $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, respectively.

$\mathbb{C}$ is the set of all complex numbers.

$\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$ are the sets of nonzero members of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, respectively.

0.6 Example The set $\mathbb{R} \times \mathbb{R}$ is the familiar Euclidean plane that we use in first-semester calculus to draw graphs of functions. ▲

Relations Between Sets

We introduce the notion of an element a of set A being *related* to an element b of set B, which we might denote by $a\,\mathscr{R}\,b$. The notation $a\,\mathscr{R}\,b$ exhibits the elements a and b in left-to-right order, just as the notation (a, b) for an element in $A \times B$. This leads us to the following definition of a relation $\mathscr{R}$ as a *set*.

0.7 Definition A **relation** between sets A and B is a subset $\mathscr{R}$ of $A \times B$. We read $(a, b) \in \mathscr{R}$ as "a is related to b" and write $a\,\mathscr{R}\,b$. ■

0.8 Example Let S be any set. We can define an **Equality Relation** $=$ between S and itself as the subset $\{(x, x) \mid x \in S\}$. Of course, this is nothing new. It is simply the usual idea of what it means for two "things" to be equal. So if $x, y \in S$ are different elements, then they are not related by the equality relation and we write $x \neq y$, but if x and y are the same then we write $x = y$. ▲

We will refer to any relation between a set S and itself, as in the preceding example, as a **relation on** S.

0.9 Example The graph of the function f where $f(x) = x^3$ for all $x \in \mathbb{R}$, is the subset $\{(x, x^3) \mid x \in \mathbb{R}\}$ of $\mathbb{R} \times \mathbb{R}$. Thus it is a relation on $\mathbb{R}$. The function is completely determined by its graph. ▲

The preceding example suggests that rather than define a "function" $y = f(x)$ to be a "rule" that assigns to each $x \in \mathbb{R}$ exactly one $y \in \mathbb{R}$, we can easily describe it as a certain type of subset of $\mathbb{R} \times \mathbb{R}$, that is, as a type of relation. We free ourselves from $\mathbb{R}$ and deal with any sets X and Y.

0.10 Definition A **function** ϕ mapping X into Y is a relation between X and Y with the property that each $x \in X$ appears as the first member of exactly one ordered pair (x, y) in ϕ. Such a function is also called a **map** or **mapping** of X into Y. We write $\phi : X \to Y$ and express $(x, y) \in \phi$ by $\phi(x) = y$. The **domain** of ϕ is the set X and the set Y is the **codomain** of ϕ. The **range** of ϕ is $\phi[X] = \{\phi(x) \mid x \in X\}$. ■

0.11 Example We can view the addition of real numbers as a function $+ : (\mathbb{R} \times \mathbb{R}) \to \mathbb{R}$, that is, as a mapping of $\mathbb{R} \times \mathbb{R}$ into $\mathbb{R}$. For example, the action of $+$ on $(2, 3) \in \mathbb{R} \times \mathbb{R}$ is given in function notation by $+((2, 3)) = 5$. In set notation we write $((2, 3), 5) \in +$. Of course, our familiar notation is $2 + 3 = 5$. ▲

Cardinality

The number of elements in a set X is the **cardinality** of X and is often denoted by $|X|$. For example, we have $|\{2, 5, 7\}| = 3$. It will be important for us to know whether two sets have the same cardinality. If both sets are finite, there is no problem; we can simply count the elements in each set. But do $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ have the same cardinality?