An Introduction to Abstract Algebra

Alan Parks
Lawrence University
Appleton, Wisconsin

♠ This project puts text material, carefully coordinated with lectures, homework, and bibliography, into the hands of upper level students at cost. It was begun during the 1996-97 academic year, and it has been revised and expanded periodically since.

Contents

Introduction

It is easy to recognize mathematics. There is an explicit and complete list of assumptions, the definitions are formal and unambiguous, calculations and deductions follow the rules of logic unfailingly, the conclusions are unavoidable and unassailable. Now, a given argument may make *some* of its assumptions clear, may use *certain* of its terms carefully, may present conclusions which are *more or less* convincing. In this sense one argument may be *more mathematical* than another, but there is really no middle ground at all between arguments which are formal mathematics and those which are not. It is a target with only the bull's-eye and nothing else. Once the ancient Greek geometers saw how many interesting consequences could be derived rigorously from a few rather innocuous axioms, the idea spread that the constraints of mathematical method could be applied to an endless variety of problems. And they were and are.

The insistence on correctness and formality at every level of a mathematical argument might lead one to believe that the subject is cold, mechanical. Certainly the proof of some particular fact, or the solution to some particular problem, should have a certain coldness. But it is the coldness of certainty, not that of personal indifference. Proofs themselves, the finished products of mathematical investigation, come about only as a very human mind (yours!) grapples with the issues at hand. An electrical wire is cold in the sense that it conducts electricity rather effortlessly, but if the point is to light up the room then we want to waste as little energy as possible in conducting the current. A mathematician wants to waste as little doubt as possible (none!) on the certainty of mathematical results.

This text introduces abstract algebra for a course in which you will begin learning to read, write, remember, and do mathematics. To this end we will study elementary number theory and the theory of groups – subjects fundamental not just to advanced mathematics, but to virtually every discipline of quantitative science. More importantly from our point of view, they are intrinsically interesting, and we can prove results of significance starting from scratch.

Toward the end of the nineteenth century, it became clear that group theory, which arose in many different contexts from the study of symmetries and permutations, could be used to unite and organize many of the mathematical disciplines. The use of groups over the past couple of centuries has yielded fundamental insights in the study of polynomial equations, geometry, differential equations, and other disciplines in mathematics, as well as in physics and chemistry. Furthermore, some of the most exciting breakthroughs in mathematics over the past 100 years belong to group theory. Thus, in studying groups we are laying the groundwork for an understanding of mathematics as a whole, while contacting with an area of current research. Groups are simply defined, and we can construct a multitude of examples with which to make calculations or conjectures. We can exploit a small number of facts again and again in a wide variety of problems. Therefore, the subject is concrete and self-contained, which makes it ideal for providing firsthand experience with mathematics.

Firsthand experience will occur only as you diligently pursue mastery of the course content in order to gain problem solving ability and the skill of algebraic work. You will not benefit from the text unless you read it very aggressively, using your ability to reproduce the various arguments to test understanding. To repeat: you do not *know* or *understand* a subject in mathematics unless you can work out its main theorems from the ground up on your own. Thus, mathematical exposition tends toward the sparing side. It is assumed that the reader works through the arguments thoroughly and carefully.

In class we will work hard at understanding the theorems proved in the text, and we will work a variety of problems, showing how to apply the material.

At the end of each chapter, you will find select bibliography for many of the text topics. A library search over classifications QA150-272 will yield many, many texts that cover the material in this book, so you can find alternative points of view, additional problems, and other topics, if you wish.

CHAPTER 1

Logic and Sets.

Mathematics is easy to describe: you have a list of statements that you accept as true, and you construct examples and derive logical conclusions from those statements. The original statements are called *axioms* and the conclusions are called *propositions* or *theorems.* The purpose of this chapter is to introduce you to the language used to state the axioms and to derive the conclusions.

Mathematicians think in at least two ways; we might say *formally* and *intuitively.* Every mathematical argument is a formal display of precisely defined objects and strictly logical manipulations. Without precision and clarity you do not have mathematics, and to learn mathematics you need to learn to recognize when an object is well-defined, when a proof is correct and complete. But the objects and logical bindings are not interesting and not memorable unless they correspond, intuitively, with notions in the mind that are familiar and appreciated. Furthermore, you will never make much progress in producing mathematics unless you learn to think intuitively about the objects and arguments, creatively employing various metaphors or pictures. Visual or poetic images bring abstract objects to life. The skill of the mathematician consists in being able to combine these approaches: to be able to imagine a formal, abstract object pictorially; to be able to translate intuitive thought into formal language.

On the formal level, the positive integers form a set with certain definite properties (we will write down these properties momentarily). Intuitively, you have all sorts of thoughts in your mind involving the positive integers: you might remember the manipulatives you used in learning to count, you might imagine marks on a number line, you might visualize $2 \cdot 3 = 6$ as counting the entries in a table with 2 rows and 3 columns, etc. Formally speaking, understanding a proof about the positive integers is an exercise in matching clearly defined properties with logical statements about them; intuitively speaking, understanding a proof is an exercise in seeing a pattern of sensible thought. The important facts are not arbitrarily chosen, rather, they are aesthetically interesting, displaying a sense of beauty or elegance, whether we are talking about the practical beauty of the solution to an applied problem or the ethereal beauty of a symmetry in music or a painting. Aesthetic appreciation and formal understanding go hand in hand.

There are several formal ways to build mathematics from the ground up; the one we will use has been the most widely followed since the late 1800's. We want to introduce the formal vocabulary of set theory in which most mathematical statements may be constructed. First of all, we will discover what is meant by *statement* through examples. After we are familiar with some types of statements, we might have time to give a formal definition in class. We need to assume that the mathematical statements we encounter are either *true* or *false*, and not both. It is possible to formulate statements in general that are neither true nor false, either because they are meaningless or for other reasons; since we will deal only with statements that are true or false, we will not go into this any further.

Mathematical statements are put together with logical connectives that we now list. If we are given a statement **A**, then its *negation* is denoted "not **A**." The negation of **A** is false if **A** is true, and it is true if **A** is false.

If we have statements **A** and **B**, then the statement "**A** *and* **B**" is true if both **A** and **B** are true, and it is false if either **A** or **B** is false.

The statement "**A** or **B**" is true if either **A** or **B**, or both, is true, and it is false if both **A** and **B** are false. It is worth noting that this use of the word "or" is somewhat different than that of usual English. If, in everyday speech, I say, "I am going to the store, or I am going to a movie," I probably do not mean that I am both going to the store *and* that I am also going to a movie. If I did mean that both were true, I would have said, "I am going to the store and to a movie." In mathematics, however, the word "or" allows either or both its constituent statements to be true.

A statement of the form "if **A**, then **B**" is an *implication*. This statement can be written more symbolically: $\mathbf{A} \Rightarrow \mathbf{B}$. In such a compound statement, the statement **A** is the *hypothesis* and **B** is the *conclusion*. An implication is true if both its hypothesis and conclusion are true, and it is also true if the hypothesis is false, regardless whether the conclusion is true or false. Thus, the statement "if $2 + 2 = 4$, then Paris is a city" is true, as is the statement "if $1 = 0$, then pigs have wings." An implication like the second one, in which the hypothesis is false, is said to be *vacuous*. There is an important role for vacuous implications, as we will see later.

You can test your understanding of what we have done so far by showing that the statement "$\mathbf{A} \Rightarrow \mathbf{B}$" is *equivalent* to "(not **A**) or **B**." (Equivalent statements are both true or both false.)

As we will point out in class, we need to distinguish between *proving* that an implication is true and *using* an implication that is already known to be true. Look for examples as you read through the following.

We now consider the *contrapositive* of an implication. The contrapositive of the implication $\mathbf{A} \Rightarrow \mathbf{B}$ is the implication "(not **B**) $\Rightarrow$ (not **A**)." We aim to show that an implication is equivalent to its contrapositive (they are both true or both false). Let us consider the possibilities for **A** and **B**. If **A** and **B** are true, then $\mathbf{A} \Rightarrow \mathbf{B}$ is true; also, (not **B**) is false, and so (not **B**) $\Rightarrow$ (not **A**) is true. If **A** is true and **B** is false, then $\mathbf{A} \Rightarrow \mathbf{B}$ is false. And (not **B**) is true and (not **A**) is false, so that (not **B**) $\Rightarrow$ (not **A**) is false. There are two other cases. Do them![1]

The *converse* of the implication $\mathbf{A} \Rightarrow \mathbf{B}$ is the implication $\mathbf{B} \Rightarrow \mathbf{A}$. In general, an implication can be true without its converse being true, and an implication can be false without its converse being false. (Can you think of an example?)

Notice that we can express that **A** and **B** are equivalent by "$\mathbf{A} \Rightarrow \mathbf{B}$ and $\mathbf{B} \Rightarrow \mathbf{A}$." Indeed, if **A** and **B** are both true, then "$\mathbf{A} \Rightarrow \mathbf{B}$ and $\mathbf{B} \Rightarrow \mathbf{A}$" is true. If **A** and **B** are both false, then, again, "$\mathbf{A} \Rightarrow \mathbf{B}$ and $\mathbf{B} \Rightarrow \mathbf{A}$" is true. On the other hand, if **A** is true and **B** is false, then $\mathbf{A} \Rightarrow \mathbf{B}$ is false, and so "$\mathbf{A} \Rightarrow \mathbf{B}$ and $\mathbf{B} \Rightarrow \mathbf{A}$" is false. We leave the remaining case to you. We often say that **A** and **B** are equivalent by saying "**A** if and only if **B**." This is also written $\mathbf{A} \Longleftrightarrow \mathbf{B}$.

Now we are ready for sets. Intuitively, a set is a *collection* of objects, and, most of the time, the intuitive view is helpful. If we can list the objects, we enclose the list in curly brackets to indicate the set: $A = \{1, 2, 3\}$. This identifies A as a set – the collection consisting of the numbers $1, 2, 3$. We write $1 \in A$ (read 1 is an *element* of A) to indicate that 1 is in the collection called A. Similarly $2 \in A$ and $3 \in A$. We write $4 \notin A$ to indicate that 4 is *not* one of the elements in the set A. The symbol $\in$ should be distinguished from the Greek letter epsilon (ϵ).

The intuitive point of view is that a set is a collection of objects. On a formal level, the word *set* is undefined; we say it is accepted *axoimatically.* In order to work with sets, we will need to state their formal properties. Formally, every mathematical object considered in this course is a set.

[1] In class we will say over and over that you have to read mathematics actively, working out details, going back over anything that is the least obscure, always asking yourself whether you can *reproduce* what you have learned.

Wait a minute; the number 2, being a mathematical object, must be a set! It is not supposed to be obvious at this point what it means for 2 to be a "collection," in fact the answer is quite subtle so don't try to guess at it. It may well seem strange to regard numbers and functions and other familiar things as sets. You will get over this strangeness after working with sets for a while. The immediate point is that "set" is a formal term; it is often *but not always* helpful to think of a set as a collection – when it *is* helpful, it is helpful on the intuitive level. As we begin to work with sets, the intuitive idea of a collection will guide us charmingly.

Given sets x, S, the statement $x \in S$ is either true or false – it is either true of false that x belongs to the collection defined by S. If x does not belong, then $x \notin S$ is true. In other words, exactly one of these statements is true: $x \in S$, $x \notin S$. For the sets considered in mathematics, it is always the case that if $x \in S$ is true, then the statement $S \notin x$ is true. (Here is a chance to think intuitively about collections. Why does this make sense?) Notice that it follows that $S \in S$ is always false. Why?

If all the elements of a set T are elements of a set S then T is a *subset* of S, and we write $T \subseteq S$. Going back to our logical notions, the statement $T \subseteq S$ is equivalent to the statement $(x \in T) \Rightarrow (x \in S)$. For example, every set is a subset of itself. Given two sets T and S, in order to prove that $T \subseteq S$, you assume that $x \in T$ and prove that $x \in S$. This implication also introduces another type of expression. The implication $(x \in T) \Rightarrow (x \in S)$ can be expressed "$x \in S$ for all $x \in T$."

Be careful to distinguish $T \in S$ from $T \subseteq S$. The first statement says that "T is one of the S's," the second "every T is an S." Here is an intuitive example: Jumbo is an *element* of the set of Elephants. The set of Baby Elephants form a *subset* of the set of Elephants.

Given a set S, the set of all its subsets is a (usually large) set. For example, there are eight subsets of $\{1, 2, 3\}$; you should try writing them down!

Sets are equal if and only if they have the same elements. In other words, $S = T$ is equivalent to $(x \in S) \iff (x \in T)$. Another way to say this: $S = T$ if each is a subset of the other: $S \subseteq T$ and $T \subseteq S$. Intuitively, when we say that $S = T$, we are saying that "S" and "T" are different names for the same thing. Formally, if $S = T$ we can substitute T for S (or S for T) in any true statement to form another true statement.

It is trivial but mildly interesting to see that equality of sets obeys some expected laws: we have $S = S$ for all sets S. If $S = T$, then $T = S$. If $S = T$ and $T = U$, then $S = U$. Verifying each of these statements is a straightforward exercise in logic – applying the precise definition of equality.

We want to introduce the main method for constructing new sets from old ones. That method involves two auxiliary ideas. First, a statement can have a variable in it. For instance, consider the statement "x is an integer and $x > 2$." This statement is true if $x = 5$ or if $x = 7$, and it is false if $x = 1$ or $x = 3.2$ or $x = \{a, b\}$. The variable x in the statement is a *free variable* since the statement doesn't define what x is.

Our second idea involves the phrase "there is" (formally $\exists$), which posits the existence of an object with given properties. The meaning of the statement "there is x such that x is an integer and $x > 2$" is obvious. In the previous paragraph, we considered the statement "x is an integer and $x > 2$" on its own, true or false depending on x. The "there is" asserts that the statement *can be* true. The entire "there is" statement is true, since there is an integer greater than 2.

Here is a more symbolical formulation, using $\mathbb{Z}$ for the set of integers: $\exists x(x \in \mathbb{Z} \text{ and } x > 2)$. The $\exists x$ prefix entails the assumption that x is a free variable in the inner statement (surrounded by parentheses).

The principal way that new sets are constructed from old ones is by what is called the *Axiom of Specification.*[2] To give an example, suppose I have sets A, B and I want to identify the elements of A that are also elements of B. (This is the intersection of A and B; that term will be discussed momentarily.) The Axiom of Specification allows me to make the following definition:

$$C = \{x \in A \mid x \in B\}$$

This is read, "Let C be the set of elements x of A such that x is an element of B." The vertical bar in the middle is read *such that* or *for which.* The upshot is that C is a new set, and the statement $x \in C$ is same as "$x \in A$ and $x \in B$."

Here is the general formulation of the Axiom. We are given a set A and a statement S, and we define a new set C:

$$C = \{x \in A \mid S\}$$

The statement S involves x as a free variable. You might think of S as a property that a given x may or may not have, as in "$x \in B$." The Axiom tells us that the set C exists, and $x \in C$ if and only if $x \in A$ and the statement S is true. So, the Axiom is a "there is" statement. Here is what it looks like formally.

$$\exists C\big(x \in C \iff [x \in A \text{ and } S]\big)$$

An additional technicality is necessary to the construction of the last two paragraphs. The symbol C, used to name the new set, cannot already be in use to name something else. In particular, C cannot be the same symbol as A, and C should not be mentioned in the statement S.

We have given some notation and have described how to construct subsets of given sets. Up to now, we have not had the actual existence of any particular set, so it's time to assume that *there is a set*! It doesn't much matter what

[2] The Axiom of Specification has many other names: the axiom of subsets, the axiom of selection, the axiom of separation.

are the elements of this set; let's call the set A. We are assuming the existence of A axiomatically.[3] As a first use of our set A, we construct another set, the *empty set*. The Axiom of Specification constructs the set

$$\phi = \{x \in A \mid x \neq x\}$$

We can show that ϕ is a set with no elements at all! Indeed, if $x \in \phi$, then $x \in A$ and $x \neq x$. This latter statement is false, and so it must be that $x \in \phi$ is false.

The empty set can be used to form a famous vacuous implication: the empty set is a subset of every set. The statement $\phi \subseteq S$ is the implication $(x \in \phi) \Rightarrow (x \in S)$. The hypothesis $x \in \phi$ is never true, for the empty set has no elements, and therefore the implication is vacuous (and true!).

You probably remember what is meant by the *union* and *intersection* of sets. Given sets S and T, there is a set $S \cup T$ (the *union* of S and T) such that $x \in S \cup T$ if and only if $x \in S$ or $x \in T$. (Recall the meaning of "or," it is ok for x to be in both S and T.)

The intersection $S \cap T$ is such that $x \in S \cap T$ if and only if $x \in S$ and $x \in T$. We have already seen that intersections exist by the Axiom of Specification. On the other hand, the existence of set unions does not follow from this axiom, and so it must be stipulated on its own.

We say that S and T are *disjoint* if their intersection is the empty set.

Here is a fairly simple fact about unions and intersections. We use it to occasion our first proof.

PROPOSITION 1.1. *Let A, B, and C be sets. Then*

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

[3] You probably guessed that to accept something *axiomatically* is to accept it as an axiom.

PROOF. The proof will be formal, but before you read the details, draw an intuitive picture where the sets A, B, C are areas in the plane and see what the proposition says. Does it look as if the proposition is true?

The definition of set equality shows that we need to prove that each set is contained in the other. Thus, we first assume that $x \in A \cap (B \cup C)$ and prove that $x \in (A \cap B) \cup (A \cap C)$, for this establishes

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \tag{1.1}$$

Then we let $x \in (A \cap B) \cup (A \cap C)$, and prove that $x \in A \cap (B \cup C)$, concluding

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C) \tag{1.2}$$

This will complete the proof that the sets are equal.

Now let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in (B \cup C)$. This last says that $x \in B$ or $x \in C$. If $x \in B$, then since $x \in A$, we have that $x \in (A \cap B)$. If $x \in C$, then since again $x \in A$, we have $x \in (A \cap C)$. Thus $x \in (A \cap B)$ or $x \in (A \cap C)$, so that $x \in (A \cap B) \cup (A \cap C)$. This proves the containment (1.1).

Let $x \in (A \cap B) \cup (A \cap C)$. Then $x \in (A \cap B)$ or $x \in (A \cap C)$. If $x \in (A \cap B)$, then $x \in A$ and $x \in B$, so that $x \in A$ and $x \in (B \cup C)$, hence $x \in A \cap (B \cup C)$. Similarly, if $x \in (A \cap C)$, then $x \in A \cap (B \cup C)$, and this proves (1.2). □

Note our end of proof symbol: a modest open square. Some texts use the abbreviation QED to end proofs. What does QED stand for?

There is one other construction we will need in working with sets. Given sets A and B, there is a set $A \times B$, the *cartesian product* of A and B, consisting of all *ordered pairs* (a, b) where $a \in A$ and $b \in B$. The xy-plane from your calculus days is a cartesian product $\mathbb{R} \times \mathbb{R}$ where $\mathbb{R}$ is the set of real numbers (we will not use the real numbers in this course). Two ordered pairs (a_1, b_1) and (a_2, b_2) are equal if and only if $a_1 = a_2$ and $b_1 = b_2$. The existence of ordered pairs and cartesian products can be established using the axioms we have already given, but in the interest of time we will not bother to pursue this.[4]

Now we have almost everything we need to get started in mathematics. In the next section we will examine what many would call the most basic set – the set of integers.

A good introduction to doing mathematics is *How to read and do proofs : an introduction to mathematical thought process* by Daniel Solow (Wiley 1982). There are many books describing the use of set theory to build mathematics. *Naive Set Theory* by P. Halmos gives an informal introduction that leaves many details to the reader but does a good job explaining the purpose of the various axioms. The more technical *Axiomatic Set Theory* by P. Bernays (Dover, 1991) is at the advanced level, but it contains an excellent historical introduction written by A. Fraenkel in which the axioms we have used are described in more detail. This second book has an extensive bibliography. There are other ways in which mathematics may be grounded. The article *The Education of a Pure Mathematician*, by Bruce Pourciau in the American Mathematical Monthly, October 1999, uses a Socratic dialogue to introduce some of the philosophical questions involved. Beware that the issue of how to get mathematics off the ground is not easy to resolve and that there is no universally agreed upon philosophy of mathematics. Mathematicians are, in the main, more interested in doing mathematics than in arguing about its underpinnings.

[4] Except to try to intrigue you. Formally, (a, b) can be defined as $\{a, \{a, b\}\}$. Can you show that this latter set exists? Hint: you need to make free use of the fact that the set of all subsets of a set is, itself, a set.

Problems

1. Let $\mathbf{A}, \mathbf{B}, \mathbf{C}$ be statements, each of which is either true or false Prove that

$$(\mathbf{A} \Rightarrow \mathbf{B} \quad \text{and} \quad \mathbf{B} \Rightarrow \mathbf{C}) \qquad \Rightarrow \qquad (\mathbf{A} \Rightarrow \mathbf{C})$$

(Note: This is a problem of logic. Consider the possible values true or false of each statement.)

2. For statements $\mathbf{A}, \mathbf{B}$, define the statement "**A** xor **B**" to be true if **A** is true and **B** is false, and it is true if **A** is false and **B** is true. The statement **A** xor **B** is false otherwise. Show how to build this statement using *and, or, not.*

3. Let $\mathbf{A}, \mathbf{B}$ be statements. Show that

$$\Big(\mathbf{A} \Rightarrow \mathbf{B}\Big) \Longleftrightarrow \Big[\big(\text{not } \mathbf{A}\big) \ \text{ or } \ \mathbf{B}\Big]$$

4. Let $\mathbf{A}, \mathbf{B}$ be statements. Show that the negation of "**A** and **B**" is the statement "(not **A**) or (not **B**)."

5. Let **A** and **B** be statements. Use "not" and "and" to write the negation of the statement $\mathbf{A} \Rightarrow \mathbf{B}$.

6. Show that if A is a subset of B, and B is a subset of C, then A is a subset of C.

7. For sets A, B, define

$$A \setminus B = \{x \in A \bigm| x \notin B\}$$

Prove the following, for sets A, B, C.

(a) $A \setminus B = A$ if and only if $A \cap B = \phi$
(b) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
(c) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

8. Let A, B be sets. Prove that

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

9. For sets A, B, C, show that $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.

10. In mathematics *there is no universe.* In other words, there can't be a set having every set as a subset of it. Prove this. (Assume that A is a universe and derive a contradiction.)

11. Suppose that A, B are sets. Show that there is a set whose elements are A, B. (Hint: The set would be denoted $\{A, B\}$, but you need to use the axioms to define it; start with the set of all subsets of A and the set of all subsets of B.)

12. Use the notations of formal set-theory and logic to express that the set S has exactly one element. (Hint: you might start with "there is $x \in S$.")

13. Use the notation of formal set-theory to express that the set S has exactly two elements.

14. Let $A = \{1, 2\}$ and $B = \{3, 4, 5\}$ and $C = \{6, 7\}$.

(a) Write down the elements of $A \times B$.

(b) Write down the elements of $(A \times B) \times C$.

15. For sets A, B, C show that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Index