Math 101 Textnotes [1]

Daniel Goroff with Michael Hutchings

Contents

Chapter 0

Suggestions on Using this Book

It is probably not a good idea to try to read a math book as if it were a novel. What if you tried to read a novel as if it were a math book? Here are some of the questions you might ask yourself.

"This new character, Jane, is neat. Why don't I flip through to see what she does later in the story."

"The scene where John and Mary talk in the park looks like tough going. Why don't I skip over it for now and see if I need it later."

"I hate the way the restaurant scene is written! How could I explain it better?"

"Does it really matter that Sally's vacation was in France? What if we make it China instead? How would that affect the story?"

"John's daily routine is really strange. Can I find some more examples of this type of behavior?"

"I'm confused about the plot. Why don't I take some notes, make an outline."

"The point of this chapter seems to be that the police chase the suspect and catch him. I don't think I need to worry about the details right now, although I might be curious about them later."

"What's Ed's purpose in this story? Is he really necessary?"

"This party scene is too sketchy. I think I should pause and work out some of the details."

At the same time, there are some ways in which reading a novel is very much like reading a math book. In both cases, you need to make mental models of what's going on. You can't just memorize a list of facts; you need to create a framework in which to place them. This is much easier with a novel, because a novel usually talks about objects with which you are familiar. It is not hard to imagine a house, but it might be harder to imagine a closure operator if you have never seen one before. I personally like to draw lots of pictures, although

other people may think differently. These pictures are gradually refined as I see more examples.

In short, try to read as actively as possible. A pencil and paper can make it easier to concentrate. Try writing down questions, comments, summaries, examples, pictures, explanations, details, notes. You might even want to collect these in a "journal". At the same time, don't always concentrate so hard; feel free to skip around through the text, and look over whatever seems interesting or fun.

About the notation: words typically appear in **bold** where they are first defined. Usually a word in "quotes" either has not yet been defined, or has no precise meaning. The notation

$$x \stackrel{\text{def}}{=} y$$

means that x is defined to be equal to y. Exercise 9.1.3 is Exercise 3 of section 1 of Chapter 9. Sections marked with a '*' appear only in the "director's cut", and may not be essential to the story.

Part I

Topology

Introduction to Part I

Suppose you have a pad of notepaper on your desk. Suppose you tear off a piece of paper, crumple it up without tearing it, and toss it back on top of the pad. Then at least one point on the crumpled sheet will lie exactly above the point where it was before. This surprising and beautiful fact is stated by the *Brouwer Fixed Point Theorem.* Our goal in Part I of this book is to prove this theorem.

The most immediate problem we need to address in Part I is this: how are we to describe mathematically the physical situation described in the first paragraph above? How can we describe the piece of paper in mathematical terms? How can we find an unambiguous way of saying "crumple up the piece of paper without tearing it"? What do we mean when we say that one point lies above another? Perhaps there is no single correct answer to any of these questions, but in the first few chapters we will *choose* answers, built out of the language of set theory (which is reviewed in Appendix B). It will eventually become clear that our precise statement of the theorem models the physical situation very well. And even if it does not, trying to prove (or disprove) such a statement is an interesting problem.

A wonderful result on its own, the Brouwer theorem also has many powerful applications to other areas of mathematics. We will examine some of these in Part II. Along the way to proving the fixed-point theorem, we will introduce a number of mathematical concepts which will be extremely useful, both in proving the theorem and in solving other mathematical problems like those in Part II. Most important, our treatment is meant to help you learn by example how to write mathematical proofs. A brief introduction to the mechanics of proofs is given in Appendix A.

While reading Part I, be sure to keep in mind our final destination, the proof of the Brouwer Fixed Point Theorem. Try not to lose sight of this goal amid all the technical language and intermediary steps. Test your powers of foresight, just as you would in reading a novel, by figuring out where the plot is going before it has already gone.

Chapter 1

Topological Spaces

Before proving the Brouwer Fixed Point Theorem, we must figure out how to state it precisely. In particular, we need a mathematically precise definition of "crumple up a piece of paper without tearing it". Roughly speaking, we want to transform our "piece of paper" in such a way that points which are close together stay close after the piece of paper is transformed. A first step towards stating the Brouwer theorem will be to decide what we mean by "close".

Before saying what we mean by "close" on a disk (our piece of paper), we are first going to answer a more abstract question: *What, in general, should a notion of "closeness" entail?* After choosing an answer to this question, we will see that there are a number of possible "notions of closeness" on a disk; we will choose a natural one in a later chapter.

There are many other notions of closeness, on different spaces, that we will need to consider in our investigations. By studying the idea of closeness in the abstract, we can study all these different spaces simultaneously. As we will see, this strategy saves us work, and makes our arguments simpler and more conceptual.

We will make use of some of the basic notions and notations of set theory; these are reviewed in Appendix B. The most important thing we mean when we say that X is a set is that, given any object whatsoever, it is either true or false that it belongs to X. We will introduce more set theory as we go along.

1.1 Sets and Their Closures

The way we will capture a notion of closeness is by specifying what should be considered nearby each set A. All points that, intuitively speaking, want to stick to A will be called the closure of A and denoted $\mathbf{K}(A)$ or just $\mathbf{K}A$ for short. Given an operator $\mathbf{K}$ that associates a set $\mathbf{K}(A)$ to each set A, what properties should $\mathbf{K}$ satisfy in order to be considered a closure operator? That is the question we take up in this chapter.

We will see that there are many different admissible closure operators. One stands out, however, as providing strong intuition about what we are trying to accomplish. This is the Euclidean closure operator $\mathbf{K}_e$. While the tools for constructing the Euclidean closure operator will take a few chapters to develop, the idea to keep in mind and test against what we are doing can be readily visualized. On the real line $\mathbb{R}$, for example, we would like the Euclidean closure $\mathbf{K}_e(A)$ of an interval without endpoints, say $A = (a, b)$ consisting of the set of numbers x satisfying $a < x < b$ for some $a < b$, to come out to be the interval $[a, b]$ with its endpoints included. Also, the Euclidean closure of a punctured interval of the form $[a, b) \cup (b, c]$ should be the interval $[a, b]$. Similarly, we want the Euclidean closure of an area in the plane $\mathbb{R}^2$ enclosed by a loop to come out so that it includes that bounding loop, and the closure of a disk punctured by removing a point inside should have that point within it.

Helpful as these pictures are for motivation, we will not restrict ourselves to situations with geometric significance. It is useful to develop the idea of closure operators so that our definitions apply to all kinds of sets. For example, we could specify a set A as a list of objects surrounded by braces such as $A =$\{bear, pig, heffalump\} or $B =$\{China, Brazil, The United States, Oxford Street\}, for instance. We tend to refer to elements of a set as points in it even if there is no natural geometric interpretation that suggests this usage.

Can any kind of collection count as a set? After all, if we are going to be taking closures of sets to get new sets, it would be good to know just what we mean by the word "set." For reasons we will suggest later, saying precisely everything there is to say about sets and set operations is harder and more controversial than it might seem. Rather than go into the formalities in detail, we will assume (as nearly all working mathematicians do) what is known in the trade as "naive set theory" and just mention some common set theoretic axioms and definitions along the way.

As a practical matter, calling X a set simply means that membership in X is well-defined. In other words, given any object a whatsoever and a set X, it should either be true that a belongs to X (in which case we write $a \in X$), or not (in which case we write $a \notin X$), but not both. For example, we cannot specify a set by saying it consists of all the large countries in the world. Without further information, there would be no way of asserting or denying whether certain European countries belong.

In fact, it is worth noting that sets have no other distinguishing characteristics besides their membership. In other words, to say that sets X and Y are equal means that, for all objects a, we have $a \in X$ if and only if $a \in Y$. So, supposing $X = \{a, b, c\}$ and Y has as its only members the first three lower case letters of the English alphabet, then we can and must write that $X = Y$ as sets. This understanding of set equality is known as the "Axiom of Extensionality" in set theory. It seems obvious, but does prevent you from saying that two sets

with the exact same members could be considered unequal because you think one of the sets is pink. Set theory is all about and only about belonging. The axiom limits other possible interpretations of the symbol string $x \in A$. As Halmos points out, "Suppose, for instance, that we consider human beings instead of sets, and that, if x and A are human beings, we write $x \in A$ whenever x is an ancestor of A. The analogue of the axiom of extension would say here that if two human beings are equal, then they have the same ancestors (this is the 'only if' part, and it is true), and also that if two human beings have the same ancestors, then they are equal (this is the 'if' part, and it is false)."

Listing all the members of a set is not always possible or practical. Instead, we can also define sets by imposing membership qualifications that can, at least in principle, be checked. A bit more formally, given a set X, we will call P a predicate on X if, for each $x \in X$, $P(x)$ is a statement that is either true or false, but not both. The "Axiom of Separation" says that if X is a set and P is a predicate on X, then the collection of all x in X such that $P(x)$ is true is also a set, denoted $\{x \in X | P(x)\}$. The definition we gave of Y in the example above is of this form where $P(x)$ asserts that x is one of the first three lower case letters of the English alphabet.

One thing to notice about this Axiom of Separation is that, while it does allow you to construct new sets, you must start with and operate inside something you already know to be a set. In other words, you should notice not only that $\{x \in X | P(x)\}$ is a set, but that it is a subset of the set X. In general, the assertion that a set A is a subset of a set B is denoted $A \subset B$ and means that, no matter what x is, $x \in A$ implies $x \in B$. Why not avoid having to mention X by assuming there exists some universal set that consisting of all sets? Russell's Paradox shows that there is no such set. If there were, then you can check that the assertion "$x \notin x$" would be a predicate P(x) on this universe to which the Axiom of Separation would not apply. So if you believe in that Axiom, then the universe of all sets, no matter what it is, cannot be considered a set.

A bit more on this Russell business for those interested. It is only a paradox if you believe there should be no restrictions on what you consider a set. Certainly, there exist sets that are not members of themselves. The set of all students is not a student, for example. Philosophers would warn that, in trying to consider the collection of all sets which are not members of themselves, we are attempting to make an impredicative definition. In other words, we should take caution whenever a collection X is allowed to contain members whose definition presupposes or involves X itself, since there is serious danger of circularity. If there were a set X consisting of all sets that are not members of themselves, then we would have to be able to say whether or not X belongs to itself. Either possibility leads to a contradiction.

On the other hand, given a set X, the assertion "$x \neq x$" is a predicate on X that just happens to be always false. In general a predicate $P(x)$ on X that

is either false for all x in X or true for all x in X is called a proposition on (or about) X and can simply be denoted P. Because $x \neq x$ is a false proposition, the Axiom of Separation implies that $\{x \in X | x \neq x\}$ is a set. It has no members, and so is called the empty set and denoted $\emptyset$. Check your logic by convincing yourself that, because $x \in \emptyset$ is always false, the assertion $\emptyset \subset A$ is true for any set A. What set do you think the closure of the empty set should be?

How else can we make sets? The Axiom of Separation shows that you get new sets by taking the union and the intersection of two sets A and B that are both subsets of another set X. Then both $P(x) =$ "$x \in A$ or $x \in B$" and $Q(x) =$ "$x \in A$ and $x \in B$" are predicates on X, and so defining the union and intersection respectively of $A, B \subset X$ as

$$A \cup B = \{x \in X |\ x \in A \textit{ or } x \in B\}$$
$$A \cap B = \{x \in X |\ x \in A \textit{ and } x \in B\}$$

does determine these as sets. The union of sets not known in advance to all belong to some encompassing X does form a set, too, according to the Union Axiom. In contrast to the Separation Axiom, this allows us to manufacture new sets that are bigger than the ones we start off knowing are sets.

Another set theoretic axiom worth mentioning before stating the definition of a closure operator also produces bigger sets. We will want a closure operator $\mathbf{K}$ to define $\mathbf{K}(A)$ for all subsets of a given set X. In order to check that this or other properties hold for all $A \subset X$, it better be the case that we can tell whether or not something is a subset of X. In other words, the set of all subsets of a set better be a set. That this is always the case is called the Power Set Axiom since the set of all subsets of subsets of a given set X is called the power set of X and denoted either $\wp(X)$ or 2^X. For a hint of where the latter notation comes from, consider how many elements there are in the power set of $X = \{a_1, a_2, \ldots, a_n\}$.

As an aside for those obsessed with set theory, we can formally interpret Axiom C1 below from this point of view in terms of power sets and predicates. Given a set X and an operator $\mathbf{K}$ that associates a set $\mathbf{K}(A) \subset X$ to each $A \subset X$, we can imagaine the predicate P on the power set 2^X determined by declaring $P(A)$ to be true if and only if $A \subset \mathbf{K}A$. If this predicate P constructed out of $\mathbf{K}$ is a true proposition on 2^X, then we say $\mathbf{K}$ satisfies Axiom C1. Similarly, Axiom C3 can be viewed in terms of the predicate Q on 2^X such that $Q(A)$ is true if and only if $\mathbf{KK}A = A$. To think of the third Axiom this way requires a predicate R defined on pairs of subsets of X so that $R(A, B)$ holds if and only if $\mathbf{K}(A \cup B) = \mathbf{K}A \cup \mathbf{K}B$. The Pairing Axiom of set theory assures us, in case there was any doubt, that given sets Z and W, there does exist a set, called the Cartesian Product of Z and W and denoted $Z \times W$, consisting of all the ordered pairs (z, w) with $z \in Z$ and $w \in W$. This justifies for anyone worried about it that the predicate R is well-defined on the set $2^X \times 2^X$.

1.2 The Closure Axioms

Assuming enough "naive set theory" to say when two sets are equal, when one is a subset of another, and how to work with the empty set, with unions, and with intersections, we are ready to plunk down four conditions that a closure operator should satisfy.

Definition 1.1 *A* **closure operator** $\mathbf{K}$ *on a set* X *is a rule that associates to each subset* A *of* X *a subset of* X *denoted* $\mathbf{K}(A)$ *or simply* $\mathbf{K}A$*, in such a way that for all* $A, B \subset X$*, the following statements are true:*

Axiom C1. $A \subset \mathbf{K}A$

Axiom C2. $\mathbf{K}(A \cup B) = \mathbf{K}A \cup \mathbf{K}B$

Axiom C3. $\mathbf{K}\mathbf{K}A = \mathbf{K}A$

Axiom C4. $\mathbf{K}\emptyset = \emptyset$

Let's translate these statements into English and see what they say about the notion of closeness. The first axiom simply holds that any point in a set is very close to that set. The second axiom says that a point is very close to the union of two sets if and only if it is very close to at least one of the two sets. Applying Axiom C1 to the set $\mathbf{K}A$, we find that $\mathbf{K}A \subset \mathbf{K}\mathbf{K}A$; Axiom C3 tells us that in addition, $\mathbf{K}\mathbf{K}A \subset \mathbf{K}A$. This means that if a point is really close to the set of points really close to A, then it is really close to A. Axiom C4 says that nothing is really close to the empty set.

These particular axioms were formulated by Kuratowski in the middle of the 20th century, and have a certain intuitive appeal. Indeed, one might feel that if a notion of "really close" failed to satisfy the basic requirements listed above, then we should use some term other than "really close" to describe it! We could define a closure operator any way we like, of course. Mathematics is less about truth than it is about what is true if other things are true. To be considered a good set of axioms to begin with, however, mathematicians would insist that at least three criteria are met. Without being too formal, a good set of axioms should be consistent, independent, and sufficient. To see roughly what we mean by these terms, consider three statements about closure operators that did not make it onto our list of axioms:

$$\mathbf{K}X = X?$$
$$A \subset B \Longrightarrow \mathbf{K}A \subset \mathbf{K}B?$$
$$\mathbf{K}(A \cap B) = \mathbf{K}A \cap \mathbf{K}B?$$

Figure 1.1: Point x is close to A and close to B but far away from $A \cap B$.

where the symbol $\Longrightarrow$ means "implies." The first two statements seem like very reasonable properties for any notion of closeness to possess. However, it would be redundant to add them to the list of axioms, because as we will see in the next section, they are logical consequences of the axioms we have already given. And we want our definition of closure operator to be as simple as possible, to make it easier to verify when a particular operator satisfies the axioms. In other words, it is desirable for axioms to be independent of one another.

The third statement makes less sense. Figure 1.1 shows an example where, intuitively, a point is close to both A and B yet far away from $A \cap B$. In the next chapter, we will see that there exists a Euclidean closure operator which satisfies axioms C1 to C4, but which is a **counterexample** to (i.e. fails to satisfy) the assertion that $\mathbf{K}(A \cap B) = \mathbf{K}A \cap \mathbf{K}B$ for all $A, B \subset X$. Of course, we could adopt the statement $\mathbf{K}(A \cap B) = \mathbf{K}A \cap \mathbf{K}B$ as an axiom anyway and see what happens, but, by ruling out the Euclidean closure, our axioms would not be sufficient to the task we set out with of capturing our intuition about closeness.

To see if the kinds of $\mathbf{K}$ satisfying these axioms are worth studying for our purposes, one step is to construct and verify interesting examples. This will also establish that our axioms are consistent, meaning that it would be impossible to derive a contradiction from them (unless that contradiction is already derivable from the naive set theory we are using under the working hypothesis that it is consistent). For example, a silly axiom such as the requirement the $A \subset \mathbf{K}(A \cap B)$ for all $A, B \subset X$ would be inconsistent with the other axioms unless $X = \emptyset$, so it would be impossible to find a nontrivial example or model simultaneously satisfying this and the other axioms.

Results we prove using only the Kuratowski Axioms above will apply to all examples of closure operators. The nature and usefulness of these results are the ultimate justification of our axioms. Starting here, we will eventually be able to prove results like the "fundamental theorem of algebra," not to mention the Brouwer Fixed Point Theorem.

1.3 Examples of closure operators

In our first examples of proofs, we will verify that several different ways of specifying a $\mathbf{K}$ really do result in closure operators. By Definition 1.1, a $\mathbf{K}$ associating subsets of X to subsets of X is a closure operator if it follows four specific requirements, so all we need to do here is verify that the rule in question does indeed satisfy these conditions.

Example 1.2 Let X be a set, and define $\mathbf{K}A = A$ for every subset A of X. Then $\mathbf{K}$ is a closure operator on X.

Proof.
Axiom C1 holds because

$$\mathbf{K}A = A \supset A.$$

Axiom C2 holds because

$$\mathbf{K}(A \cup B) = A \cup B = \mathbf{K}A \cup \mathbf{K}B.$$

Axiom C3 holds because $\mathbf{K}\mathbf{K}A = \mathbf{K}A$, by definition of $\mathbf{K}$. Axiom C4 is also immediate from the definition of $\mathbf{K}$.

□

(The symbol '□' indicates the end of a proof.)

This $\mathbf{K}$ is called the **discrete** closure operator on X. The reason is that if $p \in X$, then $\mathbf{K}(X - \{p\}) = X - \{p\} \not\ni p$. Intuitively, this means that any point p in X is not close to the rest of X; hence the term "discrete", which means "separate". For example, the discrete closure operator might seem like a reasonable choice when X is the set of integers, $\mathbb{Z}$. Our intuition suggests that an integer on a line should not be close to other integers (only to itself), for there is always a gap of length one in between them.

In our next example, to verify each of the first three axioms we need to use "proof by cases" as described in Appendix A.

Example 1.3 Let X be a set. For each $A \subset X$, define

$$\mathbf{K}A = \begin{cases} \emptyset & \text{if } A = \emptyset, \\ X & \text{if } A \neq \emptyset. \end{cases}$$

Then $\mathbf{K}$ is a closure operator on X.

Proof.

To prove Axiom C1, let $A \subset X$ be given. If $A = \emptyset$, then $\mathbf{K}A = \emptyset \supset A$; and if $A \neq \emptyset$ then $\mathbf{K}A = X \supset A$.

To prove Axiom C2, let $A, B \subset X$ be given. If A and B are both empty, then

$$\mathbf{K}(A \cup B) = \mathbf{K}\emptyset = \emptyset = \emptyset \cup \emptyset = \mathbf{K}A \cup \mathbf{K}B.$$

If A is nonempty, then $A \cup B$ is also nonempty, so

$$\mathbf{K}(A \cup B) = X = X \cup \mathbf{K}B = \mathbf{K}A \cup \mathbf{K}B.$$

(Note that $X = X \cup \mathbf{K}B$ because $\mathbf{K}B \subset X$.) The case where B is nonempty is handled similarly. This takes care of all cases.

Now for Axiom C3. If $A = \emptyset$, then

$$\mathbf{K}\mathbf{K}A = \mathbf{K}\emptyset = \mathbf{K}A.$$

If $A \neq \emptyset$, then

$$\mathbf{K}\mathbf{K}A = \mathbf{K}X = X = \mathbf{K}A.$$

Axiom C4 is immediate from the definition of $\mathbf{K}$.

□

This $\mathbf{K}$ is called the **trivial** closure operator. It is the opposite of the discrete closure operator; every point is really close to every nonempty set. The trivial closure operator is not used very often.

Note that in the proof of Axiom C2 above, the two cases $A \neq \emptyset$ and $B \neq \emptyset$ behave identically. There is a convention which saves ink in situations like this. After the case where $A = B = \emptyset$, we change the rest of the proof to read:

> Otherwise, *without loss of generality*, A is nonempty. Then $A \cup B$ is also nonempty, so
>
> $$\mathbf{K}(A \cup B) = X = X \cup \mathbf{K}B = \mathbf{K}A \cup \mathbf{K}B.$$
>
> (Note that $X = X \cup \mathbf{K}B$ because $\mathbf{K}B \subset X$.)

What "without loss of generality" says is that the difference between A and B is purely semantic, and that they behave entirely identically in the context of the proof and thus it is redundant to consider them as separate cases. In other words, if it were B instead of A that were nonempty, we could always just relabel them. Here is another example which illustrates the use of the phrase "without loss of generality".

Example 1.4 Consider the set $A = \{\text{bear, pig, heffalump}\}$ mentioned above. Given that there are heffalumps about, the bear and the pig stick together and are always found close to each other. We can then define the closure of this set. We know that it must be a function which relates all the subsets of A to their closures, so we say:

$$\begin{aligned}
\mathbf{K}\{b,p,h\} &= \{b,p,h\} \\
\mathbf{K}\{\emptyset\} &= \{\emptyset\} \\
\mathbf{K}\{b,h\} &= \{b,p,h\} \\
\mathbf{K}\{p,h\} &= \{b,p,h\} \\
\mathbf{K}\{p\} &= \{b,p\} \\
\mathbf{K}\{b\} &= \{b,p\} \\
\mathbf{K}\{h\} &= \{h\} \\
\mathbf{K}\{b,p\} &= \{b,p\}
\end{aligned}$$

where the letters "b, p, h" stand for "bear, pig, heffalump" respectively. It is easy to see that this set of relations satisfies all of the axioms given above, so it is a closure operator.

Example 1.5 Let X be a set, and let p be an element of X. For each $A \subset X$, define

$$\mathbf{K}A = \begin{cases} \emptyset & \text{if } A = \emptyset, \\ A \cup \{p\} & \text{if } A \neq \emptyset. \end{cases}$$

Then $\mathbf{K}$ is a closure operator on X.

Proof. To prove Axiom C1, let A be a subset of X. If A is the empty set, then

$$A \subset \emptyset = \mathbf{K}A.$$

If A is nonempty, then

$$A \subset A \cup \{p\} = \mathbf{K}A.$$

To prove Axiom C2, let A and B be subsets of X.

Case 1: Suppose A and B are both nonempty. Since $A \cup B$ is also nonempty, we have

$$\mathbf{K}(A \cup B) = (A \cup B) \cup \{p\} = (A \cup \{p\}) \cup (B \cup \{p\}) = \mathbf{K}A \cup \mathbf{K}B.$$

Case 2: Otherwise, without loss of generality, A is empty. Then

$$\mathbf{K}A \cup \mathbf{K}B = \mathbf{K}\emptyset \cup \mathbf{K}B = \emptyset \cup \mathbf{K}B = \mathbf{K}B = \mathbf{K}(\emptyset \cup B) = \mathbf{K}(A \cup B).$$

To prove Axiom C3, let A be a subset of X. If A is empty, then

$$\mathbf{KK}A = \mathbf{K}\emptyset = \mathbf{K}A.$$

If A is nonempty, then $A \cup \{p\}$ is also nonempty, so

$$\mathbf{KK}A = \mathbf{K}(A \cup \{p\}) = (A \cup \{p\}) \cup \{p\} = A \cup \{p\} = \mathbf{K}A.$$

Axiom C4 is immediate from the definition.

□

Exercises

1. The following are four different candidates for closure operators on the integers $\mathbb{Z}$. Two of them are actually closure operators, while the other two are not. Which is which, and why? (The symbol '$\exists$' means 'there exists'; see Appendix A.)

   (a) $\mathbf{K}A = \{x \in \mathbb{Z} \mid (\exists a \in A)\ a < x\}$

   (b) $\mathbf{K}A = \{x \in \mathbb{Z} \mid (\exists a \in A)\ a \leq x\}$

   (c) $\mathbf{K}A = \{x \in \mathbb{Z} \mid (\exists a \in A)\ (\exists k \in \mathbb{Z})\ x = ka\}$

   (d) $\mathbf{K}A = \{x \in \mathbb{Z} \mid (\exists a_1 \in A)\ (\exists a_2 \in A)\ a_1 \leq x \leq a_2\}$

2. Recall that a set is **finite** if it has exactly n elements, where n is some integer. A set is **infinite** if it is not finite.

   Let $L = \mathbb{Z}^+ \cup \{\infty\}$. In other words, L is the set of positive integers with an additional point added, which we call '∞'. For $A \subset L$, define

   $$\mathbf{K}A = \begin{cases} A & \text{if } A \text{ is finite,} \\ A \cup \{\infty\} & \text{if } A \text{ is infinite.} \end{cases}$$

   Show that $(L, \mathbf{K})$ is a topological space.

3. Suppose X and Y are disjoint sets (i.e. $X \cap Y = \emptyset$). Suppose $\mathbf{K}_X$ is a closure operator on X and $\mathbf{K}_Y$ is a closure operator on Y. (The subscripts are used to distinguish the two closure operators.) Define an operator $\mathbf{K}$ on $X \cup Y$ by setting

   $$\mathbf{K}A = \mathbf{K}_X(A \cap X) \cup \mathbf{K}_Y(A \cap Y)$$

   for each $A \subset X \cup Y$. Prove that $\mathbf{K}$ is a closure operator. (You will probably need to use the associative, commutative, and distributive properties of union

and intersection; see §B.2.) The topological space $(X \cup Y, \mathbf{K})$ is called the **disjoint union** of $(X, \mathbf{K}_X)$ and $(Y, \mathbf{K}_Y)$.

If X and Y are not disjoint, must $\mathbf{K}$ still be a closure operator?

1.4 Some fundamental facts

We will now prove some basic facts about closure operators that we will use almost as frequently as the axioms. In the following, assume that $(X, \mathbf{K})$ is a topological space and that A and B are subsets of X.

Proposition 1.6 *If* $\mathbf{K}A \subset A$*, then* $\mathbf{K}A = A$*.*

Proof. We know that two sets A and B are equal if and only if $A \subset B$ and $B \subset A$. Suppose $\mathbf{K}A \subset A$. By Axiom C1, $A \subset \mathbf{K}A$. Hence $\mathbf{K}A = A$.

□

Corollary 1.7 $\mathbf{K}X = X$.

Proof. Since $\mathbf{K}$ takes subsets of X to subsets of X, $\mathbf{K}X \subset X$. By Proposition 1.6, $\mathbf{K}X = X$.

□

Our next goal is to prove that if $A \subset B$ then $\mathbf{K}A \subset \mathbf{K}B$, as we promised in §1.1. This may appear difficult, since our axioms do not tell us anything about subsets. However, we do have an axiom about unions. The trick is to relate the statement '$A \subset B$' to a statement about unions.

It turns out that the statement $A \subset B$ is equivalent to the statement $A \cup B = B$. Recall that two statements P and Q are **equivalent** (and we write $P \iff Q$) whenever each statement implies the other. Many textbooks will use the statement "if and only if" or "iff" to denote the same thing. To prove $P \iff Q$, we first prove $P \implies Q$ and we then prove $P \impliedby Q$. (For more details, see Appendix A.)

Lemma 1.8 $A \subset B \iff A \cup B = B$*.*

(A **lemma** is something that you prove for the purpose of proving something else, and which is not so interesting by itself.)

Proof. ($\implies$) Suppose $A \subset B$. We need to show that $A \cup B = B$. Clearly $B \subset A \cup B$. On the other hand, since $A \subset B$ and $B \subset B$, $A \cup B \subset B$. So $A \cup B = B$.

($\impliedby$) Suppose $A \cup B = B$. Then $A \cup B \subset B$. This means that $A \subset B$ and $B \subset B$. In particular, $A \subset B$.

□

We are now ready to show that $A \subset B \Longrightarrow \mathbf{K}A \subset \mathbf{K}B$. Suppose $A \subset B$. Then, by our lemma, $A \cup B = B$. We can now apply Axiom C2 to deduce that $\mathbf{K}A \cup \mathbf{K}B = \mathbf{K}B$. Applying our lemma again (this time "in reverse"), we find that $\mathbf{K}A \subset \mathbf{K}B$, which is what we wanted.

We should point out that the above proof is a lot more detailed than proofs in most mathematics books. Mathematical writers like to be concise. A short proof can better highlight essential ideas; also, a short proof invites the reader to work out some of the details on his or her own, so as to understand it better. In a typical mathematics book, the above proof might look like this:

Theorem 1.9 $A \subset B \Longrightarrow \mathbf{K}A \subset \mathbf{K}B$.

Proof. Suppose $A \subset B$. Then $A \cup B = B$, so by Axiom C2, $\mathbf{K}A \cup \mathbf{K}B = \mathbf{K}B$. Thus $\mathbf{K}A \subset \mathbf{K}B$.

□

As we asserted in §1.1, it is not always the case that $\mathbf{K}(A \cap B) = \mathbf{K}A \cap \mathbf{K}B$. However, the following is still true:

Theorem 1.10 $\mathbf{K}(A \cap B) \subset \mathbf{K}A \cap \mathbf{K}B$.

Proof. Since $A \cap B \subset A$, it follows by Theorem 1.9 that $\mathbf{K}(A \cap B) \subset \mathbf{K}A$. Likewise, $\mathbf{K}(A \cap B) \subset \mathbf{K}B$. Therefore $\mathbf{K}(A \cap B) \subset \mathbf{K}A \cap \mathbf{K}B$.

□

Exercises

1. Let $(X, \mathbf{K})$ be a topological space, and let A_1, A_2, A_3, and A_4 be subsets of X.

   (a) Prove that $\mathbf{K}(A_1 \cup A_2 \cup A_3) = \mathbf{K}A_1 \cup \mathbf{K}A_2 \cup \mathbf{K}A_3$.

   (b) Prove that $\mathbf{K}(A_1 \cup A_2 \cup A_3 \cup A_4) = \mathbf{K}A_1 \cup \mathbf{K}A_2 \cup \mathbf{K}A_3 \cup \mathbf{K}A_4$.

   (c) Can you make a general conjecture? How do you think one might go about proving it?

   What happens if we use intersections instead of unions?

2. Let $(X, \mathbf{K})$ be a topological space, and suppose $A, B \subset X$. One of the following is always true, while the other is only sometimes true.

   (a) $\mathbf{K}(A - B) \subset \mathbf{K}A - \mathbf{K}B$

   (b) $\mathbf{K}A - \mathbf{K}B \subset \mathbf{K}(A - B)$

   Prove the one that is always true, and give a counterexample for the other. *Hint:* $C - D \subset E \Longleftrightarrow C \subset D \cup E$. (Proof?)

3. Let $(X, \mathbf{K})$ be a topological space, and let $A \subset X$. The **exterior** of A, which we denote by Ext A, is defined by

$$\text{Ext } A \stackrel{\text{def}}{=} X - \mathbf{K}A.$$

Intuitively, this is the set of all points that are not close to A. The **interior** of A, which we denote by Int A, is defined to be

$$\text{Int } A \stackrel{\text{def}}{=} \text{Ext}(X - A) = X - \mathbf{K}(X - A).$$

Intuitively, this is the set of all points that are not close to the complement of A. The **boundary** of A, which we denote by ∂A, is defined to be

$$\partial A \stackrel{\text{def}}{=} \mathbf{K}A \cap \mathbf{K}(X - A).$$

Intuitively, this is the set of all points that are close to both A and its complement. Notice that under our definition, the boundary of A is not necessarily contained in A.

(a) Let $(X, \mathbf{K})$ be a topological space and let $A \subset X$. Show that each point of X is contained in exactly one of the sets Int $A, \partial A,$ Ext A.

(b) Show that $\mathbf{K}A = A \cup \partial A$.

(c) Show that Int $A = A - \partial A$.

4. Using the definition of Int given in Exercise 3, prove the following:

(a) Int $A \subset A$

(b) $\text{Int}(A \cap B) = \text{Int } A \cap \text{Int } B$

(c) Int Int $A =$ Int A

(d) Int $X = X$

(You will probably need to use De Morgan's laws; see §B.3.)

A function Int with these four properties is called an **interior operator.** Notice the similarity between interior operators and closure operators. See if you can state and prove three fundamental propositions for interior operators, by analogy with closure operators.

1.5 Topology and Axiom Systems

A set X with a closure operator $\mathbf{K}$ on it is sometimes called a Kuratowski space. There is a totally different looking definition of what is usually called a topological space that turns out to be equivalent in the sense that every Kuratowski space naturally corresponds to a topological space and vice-versa. For details, see Exercise 2.3.3. We will therefore call what we have been studying topological spaces even though ours is not the standard definition. Certain facts can be built into axioms or definitions in one development of a theory that appear instead as lemmas or theorems in another treatment. This is a matter of taste. As we will see throughout some of the chapters that follow, taking a nonstandard route also provides many opportunities for proving that the unusual definitions are equivalent to the usual ones. We have chosen Kuratowski's approach because it is a more immediate and, in many ways, more intuitive way of arriving at what we will still call a topological space.

Definition 1.11 *A* **topological space** *is a pair* $(X, \mathbf{K})$*, where* X *is a set and* $\mathbf{K}$ *is a closure operator on* X*.*

In other words, a topological space is just a set on which a notion of closeness has been defined. Topological spaces are the basic objects of study in topology. For example, the disk, the sphere, the surface of a doughnut, and the Klein bottle are popular examples of topological spaces, not to mention the line and the plane. All these are just sets to begin with, of course, but on each of them can be equiped with a standard closure operator. There are also stranger topological spaces which are hard to visualize. Topologists are concerned with devising ways to tell topological spaces apart and determining how they may and may not be transformed into one another.

You could say that topology is the set of all logical consequences of the Kuratowski Axioms. To be a bit more formal, we should specify an axiom system consisting of 4 components: first, a collection of undefined terms and primitive symbols such as $\mathbf{K}$, $\cap$, and so forth; second, a collection of syntactical rules for determining which strings of these symbols count as grammatical sentences; third, a collection of properly formed sentences called axioms; and finally, rules of inference. Like nearly all working mathematicians, we have been rather informal about the set theory and logic we accept, relegating what details seem necessary to Appendices. If we imagine specifying everything in our axiom system more precisely, however, we could formulate tantalizing metamathematical questions about what we are doing. For example, given any grammatical sentence concerning topological spaces, for example, must there be a proof that it is either true or false? Gödel showed that all but the most uninteresting axiom systems are necessarily incomplete in the sense that there must exist "undecidable" sentences that they cannot be proven true or false within the given system.

Moreover, among these undeciable sentences is one that asserts the consistency of the given system. The upshot is that you cannot prove everything, and you cannot even prove within your system that you will never find a contradiction. Whether a given set of axioms are good or not is therefore mainly a matter of judgment about how well the proofs and examples they generate can illustrate, explain, and amplify your intuition. In our case, that means we must turn towards studying the Euclidean closure operator.

1.6 Appendix: Logic, Sets, and Notation

Without formalizing rules of inference or syntax for our axiom system much further, we can nevertheless present a few helpful observations about notation, particularly concerning the relationship between predicate logic and the algebra of sets.

As mentioned above, a **predicate** P on a set X is a statement that is either true or false, but not both, for each given $x \in X$. For example, if X denotes the integers, then letting $P(x)$ stand for "x is even" defines a predicate on X. We can write the condition that P is a predicate as saying that, for all $x \in X$, either $P(x) = T$ or $P(x) = F$ but not both.

According to the Axiom of Separation, the collection of all $x \in X$ such that $P(x)$ holds really is a set. It is called the **truth set** of P on X and is denoted $\{x \in X |\ P(x) = T\}$. If we think of P as a function or rule on X that associates to each $x \in X$ a member of the two-element set $\{T, F\}$, then we will see later that it is also both natural and convenient to denote the truth set of P as $P^{-1}(T)$ and its complement, the set where P is false, as $P^{-1}(F)$. For P as in the example above, $P^{-1}(T)$ would be the set of all positive even integers and $P^{-1}(F)$ would be all the odds.

Given predicates P and Q on X, new predicates on X can be formed using logical operations as follows:

1. The **negation** of P, denoted $R = \neg P$ and pronounced "not P", is defined by setting $R^{-1}(T) = P^{-1}(F)$, so that $R(x)$ is true if and only if $P(x)$ is not.

2. The **conjunction** of P and Q, denoted $R = P \wedge Q$ and pronounced "P and Q", is defined by setting $R^{-1}(T) = P^{-1}(T) \cap Q^{-1}(T)$, so $R(x)$ is true if and only if both $P(x)$ and $Q(x)$ are true.

3. The **disjunction** of P and Q, denoted $R = P \vee Q$ and pronounced "P and Q", is defined by setting $R^{-1}(T) = P^{-1}(T) \cup Q^{-1}(T)$, so that $R(x)$ is true if and only if either $P(x)$ or $Q(x)$ is true.

4. The **conditional** "if P then Q", denoted $R = P \Longrightarrow Q$ and pronounced "P implies Q", is defined by setting $R^{-1}(T) = P^{-1}(F) \cup Q^{-1}(T)$, so that $R(x)$ is true whenever either $Q(x) = T$ or $P(x) = F$.

5. The **biconditional** "P if and only if Q", denoted $R = P \iff Q$ and pronounced "P is equivalent to Q", is defined by setting $R^{-1}(T) = [P^{-1}(F) \cup Q^{-1}(T)] \cap [P^{-1}(T) \cup Q^{-1}(T)]$, so $R(x)$ is true if and only if $P(x)$ and $Q(x)$ are either both true or both false.

A predicate P on $X$is called a **proposition** if $P^{-1}(T)$ is either X or $\emptyset$. In other words, the truth value of a proposition does not depend on any particular x; it is either always true or always false. For example, on $\mathbb{Z}^+$ the proposition $P(x) =$ "$x + 3 = x$" is a false proposition and $Q(x) =$ "$x + 3 = x + 3$" is a true proposition.

Given a predicate, we can construct propositions from them by prefixing the universal quantifier "for all" or the existential quantifier "there exists." Thus, if P is a predicate on X, and A is a subset of X, we have:

1. The proposition $(\forall x \in A)P(x)$, which we read as "for all x in A, $P(x)$", is true if and only if $A \subset P^{-1}(T)$.

2. The proposition $(\exists x \in A)P(x)$, which we read as "there exists and x in A such that $P(x)$", is true if and only if $A \cup P^{-1}(T) \neq \emptyset$.

An important case in mathematics is when the domain X of a predicate P is a Cartesian product, say $X = X_1 \times X_2 \times \ldots \times X_n$. Then we can quantify P over each factor X_i one at a time. Quantifying over all n variables again results in a proposition.

For instance, with $n = 2$, we recognize that

$$(\forall x_1 \in X_1)(\exists x_2 \in X_2)P(x_1, x_2)$$

is a proposition, i.e. it is either true or false. We will see many such examples in later chapters. For now, notice that this one can have a different truth value than a proposition with the same quantifiers but a different order, e.g.,

$$(\exists x_2 \in X_2)(\forall x_1 \in X_1)P(x_1, x_2).$$

For example, take $X_1 = X_2 = \{$"people who have ever lived"$\}$ and let $P(x_1, x_2) =$ $\{$"x_2 is the mother of x_1}." Then the first proposition above is true but the second is false.

Part II

Background Material

Appendix A

Logic

In this appendix we will give a brief introduction to the "grammar" of mathematics and the mechanics of writing proofs.

A.1 Statements and logical operations

In mathematics, we study **statements**, sentences that are either true or false but not both. For example,

6 is an even integer

and

4 is an odd integer

are statements. The first one is true, and the second one is false.

In this appendix, we will use letters such as 'p' and 'q' to denote statements. You can think of these letters as being analagous to algebraic variables, with several critical differences. First, logical variables (or "Boolean" variables) can only take two values - true or false - whereas algebraic variables can represent any number. Second, the manipulations we define for logical variables are very different from those we use in arithmetic. In arithmetic, we can combine or modify numbers with operations such as '$+$', '$\times$', etc. Likewise, in logic, we have certain operations for combining or modifying statements, such as 'and', 'or', 'not', and 'if...then'. In mathematics, these words have precise meanings, which are given below. In some cases, the mathematical meanings of these words differ slightly from, or are more precise than, common English usage.

The following two logical operations are perhaps the most ubiquitous.

If...then. Most statements can be presented in this form. For instance:

If $x = 6$ then x is even.

If that person is a rockette, then that person is employed.

In general, this conditional statement can be represented schematically as

If p then q

where p and q are two logical variables, each of which can be either true or false. In this context, p is called the "antecedent" and q is called the "consequent". Now, there are clearly four possible situations in which such a statement can occur: $p = q =$ true, $p = q =$ false, $p =$ false, $q =$ true, and $p =$ true, $q =$ false. A consideration of each case leads to the following definition:

If p and q are statements, then the statement 'if p then q' is defined to be

- true, when p and q are both true or p is false;
- false, when p is true and q is false.

which should reflect what you know already from "common sense."

We sometimes abbreviate the statement 'if p then q' by 'p implies q', or '$p \Longrightarrow q$'. If p is false, then we say that $p \Longrightarrow q$ is **vacuously true**. Defining $p \Longrightarrow q$ to be true in this case may seem like a strange convention, or at least an arbitrary one, but this will eventually make perfect sense.

If and only if. If p and q are statements, then the statement 'p if and only if q' is defined to be

- true, when p and q are both true or both false;
- false, when one of p, q is true and the other is false.

The symbol for 'if and only if' is ' $\Longleftrightarrow$ '. When $p \iff q$ is true, we say that p and q are **logically equivalent**.

The following logical operators are used

Not. The simplest logical operation is 'not'. If p is a statement, then 'not p' is defined to be

- true, when p is false;
- false, when p is true.

The statement 'not p' is called the **negation** of p.

And. If p and q are two statements, then the statement 'p and q' is defined to be

- true, when p and q are both true;
- false, when p is false or q is false or both p and q are false.

Or. If p and q are two statements, then the statement 'p or q' is defined to be

- true, when p is true or q is true or both p and q are true;
- false, when both p and q are false.

In English, sometimes "p or q" means that p is true or q is true, but not both. However, this is *never* the case in mathematics. We always allow for the possibility that both p and q are true, unless we explicitly say otherwise.

Exercises

1. Why does the symbol for 'if and only if' look the way it does?

A.2 Quantifiers

Consider the sentence

x is even.

This is not what we have been calling a statement; we can't say whether it is true or false, because we don't know what x is.

There are three basic ways to turn this sentence into a statement. The first is to say exactly what x is:

When $x = 6$, x is even.

The following are two more interesting ways of turning the sentence into a statement:

For every integer x, x is even.

There exists an integer x such that x is even.

The phrases 'for every' and 'there exists' are called **quantifiers**.

As an example of the use of quantifiers, we can give precise definitions of the terms 'even' and 'odd'.

Definition A.1 *An integer x is* **even** *if there exists an integer y such that $x = 2y$.*

(The 'if' in this definition is really an 'if and only if'. Mathematical literature tends to misuse the word 'if' this way when making definitions, and we will do this too.)

Definition A.2 *An integer x is* **odd** *if there exists an integer y such that $x = 2y + 1$.*

Notation for quantifiers. We will call a sentence such as 'x is even' that depends on the value of x a "statement about x". We can denote the sentence 'x is even' by '$P(x)$'; then $P(5)$ is the statement '5 is even', $P(72)$ is the statement '72 is even', and so forth.

If S is a set and $P(x)$ is a statement about x, then the notation

$$(\forall x \in S)\ P(x)$$

means that for every x in the set S, $P(x)$ is true. (See §B for a discussion of sets.) The notation

$$(\exists x \in S)\ P(x)$$

means that there exists at least one element x of S for which $P(x)$ is true.

We denote the set of integers by '$\mathbb{Z}$'. Using the above notation, the definition of 'x is even' given previously becomes

$$(\exists y \in \mathbb{Z})\ x = 2y.$$

Of course, this is still a statement about x. We can turn this into a statement by using a quantifier to say what x is. For instance, the statement

$$(\forall x \in \mathbb{Z})\ (\exists y \in \mathbb{Z})\ x = 2y$$

says that all integers are even. (This is false.) The statement

$$(\exists x \in \mathbb{Z})\ (\exists y \in \mathbb{Z})\ x = 2y$$

says that there exists at least one even integer. (This is true.)

The sentence

$$(\exists y \in \mathbb{Z})\ x = 2y + 1$$

means that x is odd. The statement

$$(\forall x \in \mathbb{Z})\ \Big((\exists y \in \mathbb{Z})\ x = 2y\Big)\ \text{ or }\ \Big((\exists y \in \mathbb{Z})\ x = 2y + 1\Big)$$

says that every integer is even or odd.

Exercises

1. How can you write the sentence 'x is a prime number' in logic notation?

A.3 How to prove things

Let us start with a silly example. Consider the following conversation between mathematicians Alpha and Beta.

ALPHA: I've just discovered a new mathematical truth!

BETA: Oh really? What's that?

ALPHA: For every integer x, if x is even, then x^2 is even.

BETA: Hmm...are you sure that this is true?

ALPHA: Well, isn't it obvious?

BETA: No, not to me.

ALPHA: OK, I'll tell you what. You give me any integer x, and I'll show you that the sentence 'if x is even, then x^2 is even' is true. *Challenge* me.

BETA (eyes narrowing to slits): All right, how about $x = 17$.

ALPHA: That's easy. 17 is not even, so the statement 'if 17 is even, then 17^2 is even' is vacuously true. Give me a harder one.

BETA: OK, try $x = 62$.

ALPHA: Since 62 is even, I guess I have to show you that 62^2 is even.

BETA: That's right.

ALPHA (counting on her fingers furiously): According to my calculations, $62^2 = 3844$, and 3844 is clearly even...

BETA: Hold on. It's not so clear to me that 3844 is even. The definition says that 3844 is even if there exists an integer y such that $3844 = 2y$. If you want to go around saying that 3844 is even, you have to *produce* an integer y that works.

ALPHA: How about $y = 1922$.

BETA: Yes, you have a point there. So you've shown that the sentence 'if x is even, then x^2 is even' is true when $x = 17$ and when $x = 62$. But there are *billions* of integers that x could be. How do you know you can do this for every one?

ALPHA: Let x be any integer.

BETA: Which integer?

ALPHA: Any integer at all. It doesn't matter which one. I'm going to show you, using only the fact that x is an integer and nothing else, that if x is even then x^2 is even.

BETA: All right... go on.

ALPHA: So suppose x is even.

BETA: But what if it isn't?

ALPHA: If x isn't even, then the statement 'if x is even, then x^2 is even' is vacuously true. The only time I have anything to worry about is when x is even.

BETA: OK, so what do you do when x is even?

ALPHA: By the definition of 'even', we know that there exists at least one integer y such that $x = 2y$.

BETA: Only one, actually.

ALPHA: I think so. Anyway, let y be an integer such that $x = 2y$. Squaring both sides of this equation, we get $x^2 = 4y^2$. Now to prove that x^2 is even, I have to exhibit an integer, twice which is x^2.

BETA: Doesn't $2y^2$ work?

ALPHA: Yes, it does. So we're done.

BETA: And since you haven't said anything about what x is, except that it's an integer, you know that this will work for any integer at all.

ALPHA: Right.

BETA: OK, I understand now.

ALPHA: So here's another mathematical truth. For every integer x, if x is odd, then x^2 is...

This dialogue illustrates several important points. First, a **proof** is an explanation which convinces other mathematicians that a statement is true. A good proof also helps them *understand* why it is true. The dialogue also illustrates several of the basic techniques for proving that statements are true.

Table A.1 summarizes just about everything you need to know about logic. It lists the basic ways to prove, use, and negate every type of statement. In boxes with multiple items, the first item listed is the one most commonly used. Don't worry if some of the entries in the table appear cryptic at first; they will make sense after you have seen some examples.

In our first example, we will illustrate how to prove 'for every' statements and 'if...then' statements, and how to use 'there exists' statements. These ideas have already been introduced in the dialogue.

Statement	Ways to Prove it	Ways to Use it	How to Negate it
p	• Prove that p is true. • Assume p is false, and derive a contradiction.	• p is true. • If p is false, you have a contradiction.	not p
p and q	• Prove p, and then prove q.	• p is true. • q is true.	(not p) or (not q)
p or q	• Prove that p is true. • Prove that q is true. • Assume p is false, and deduce that q is true. • Assume q is false, and deduce that p is true.	• If $p \Longrightarrow r$ and $q \Longrightarrow r$ then r is true. • If p is false, then q is true. • If q is false, then p is true.	(not p) and (not q)
$p \Longrightarrow q$	• Assume p is true, and deduce that q is true. • Assume q is false, and deduce that p is false.	• If p is true, then q is true. • If q is false, then p is false.	p and (not q)
$p \iff q$	• Prove $p \Longrightarrow q$, and then prove $q \Longrightarrow p$. • Prove p and q. • Prove (not p) and (not q).	• Statements p and q are interchangeable.	(p and (not q)) or ((not p) and q)
$(\exists x \in S)\ P(x)$	• Find an x in S for which $P(x)$ is true.	• Say "let x be an element of S such that $P(x)$ is true."	$(\forall x \in S)$ not $P(x)$
$(\forall x \in S)\ P(x)$	• Say "let x be any element of S." Prove that $P(x)$ is true.	• If $x \in S$, then $P(x)$ is true. • If $P(x)$ is false, then $x \notin S$.	$(\exists x \in S)$ not $P(x)$

Table A.1: Logic in a nutshell.

Example A.3 Write a proof that for every integer x, if x is odd, then $x+1$ is even.

This is a 'for every' statement, so the first thing we do is write

> Let x be any integer.

We have to show, using only the fact that x is an integer, that if x is odd then $x+1$ is even. So we write

> Suppose x is odd.

We must somehow use this assumption to deduce that $x+1$ is even. Recall that the statement 'x is odd' means that there exists an integer y such that $x = 2y+1$. Also, we can give this integer y any name we like; so to avoid confusion below, we are going to call it 'w'. So to use the assumption that x is odd, we write

> Let w be an integer such that $x = 2w+1$.

Now we want to prove that $x+1$ is even, i.e., that there exists an integer y such that $x+1 = 2y$. Here's how we do it:

> Adding 1 to both sides of this equation, we get $x+1 = 2w+2$. Let $y = w+1$; then y is an integer and $x+1 = 2y$, so $x+1$ is even.

We have completed our proof, so we can write

> Q.E.D.

which stands for something in Latin which means "that which was to be shown". A common typographical convention is to draw a box instead:

□

In the next example, we will illustrate the use of 'and' statements.

Example A.4 Write a proof that for every integer x and for every integer y, if x is odd and y is odd then xy is odd.

(Note that the first 'and' in this statement is not a logical 'and'; it is just there to smooth things out when we translate the symbols

$$(\forall x \in \mathbb{Z})\ (\forall y \in \mathbb{Z})$$

into English.)

First, following the standard procedure for proving statements that begin with 'for every', we write

Let x and y be any integers.

We need to prove that if x is odd and y is odd then xy is odd. Following the standard procedure for proving 'if...then' statements, we write

Suppose x is odd and y is odd.

This is an 'and' statement. We can use it to conclude that x is odd. We can then use the statement that x is odd to give us an integer w such that $x = 2w + 1$. In our proof, we write

Since x is odd, choose an integer w such that $x = 2w + 1$.

We can also use our 'and' statement to conclude that y is odd. We write

Since y is odd, choose an integer v such that $y = 2v + 1$.

Now we need to show that xy is odd. We can do this as follows:

Then $xy = 4vw+2v+2w+1$. Let $z = 2vw+v+w$; then $xy = 2z+1$, so xy is odd.

□

Next, we will illustrate how to prove and use 'if and only if' statements. The proof of a statement of the form $p \iff q$ usually looks like this:

($\Longrightarrow$) [proof that $p \Longrightarrow q$]

($\Longleftarrow$) [proof that $q \Longrightarrow p$]

□

Example A.5 Write a proof that for every integer x, x is even if and only if $x + 1$ is odd.

Let x be any integer. We must show x is even if and only if $x + 1$ is odd.

($\Longrightarrow$) Suppose x is even. Choose an integer y such that $x = 2y$. Then y is also an integer such that $x + 1 = 2y + 1$, so $x + 1$ is odd.

($\Longleftarrow$) Suppose $x + 1$ is odd. Choose an integer y such that $x + 1 = 2y + 1$. Then y is also an integer such that $x = 2y$, so x is even.

□

Now we can conclude that for any integer x, the statements 'x is even' and '$x+1$ is odd' are *interchangeable*; this means that we can take any true statement and replace some occurrences of the phrase 'x is even' with the phrase '$x+1$ is odd' to get another true statement. For example, mathematicians Alpha and Beta proved in the dialogue that

For every integer x, if x is even then x^2 is even

So the following is also a true statement:

For every integer x, if $x+1$ is odd then x^2 is even.

We will consider next how to make use of 'or' statements. The first entry in the box in the table is what we call "proof by cases". This is best explained by an example.

Example A.6 For every integer x, the integer $x(x+1)$ is even.

Proof.
Let x be any integer. Then x is even or x is odd. (Some people might consider this too obvious to require a proof, but one can be given using the Division Theorem, which is introduced in an exercise in Appendix C.) We will prove that in both of these cases, $x(x+1)$ is even.

Case 1: suppose x is even. Choose an integer k such that $x = 2k$. Then $x(x+1) = 2k(2k+1)$. Let $y = k(2k+1)$; then y is an integer and $x(x+1) = 2y$, so $x(x+1)$ is even.

Case 2: suppose x is odd. Choose an integer k such that $x = 2k+1$. Then $x(x+1) = (2k+1)(2k+2)$. Let $y = (2k+1)(k+1)$; then $x(x+1) = 2y$, so $x(x+1)$ is even.

□

(One can make this proof a little more elegant, but we are just trying to illustrate how proof by cases works.)

Finally, notice that near the top of the chart, we mention that one can prove a statement by assuming that it is false and deducing a contradiction. This is a useful technique called "proof by contradiction". Many examples of this are given in the main text; see, for instance, §**??**.

How to negate statements. We often need to find the negations of statements. The rules for doing this are given in the right-hand column of the table.

For example, suppose we want to negate the statement

$$(\forall x \in \mathbb{Z})\ \Big((\exists y \in \mathbb{Z})\ x = 3y+1\Big) \Longrightarrow \Big((\exists y \in \mathbb{Z})\ x^2 = 3y+1\Big).$$

First, we put a 'not' in front of it:

$$\text{not } (\forall x \in \mathbb{Z}) \Big((\exists y \in \mathbb{Z})\ x = 3y + 1 \Big) \Longrightarrow \Big((\exists y \in \mathbb{Z})\ x^2 = 3y + 1 \Big).$$

Using the rule for negating a 'for every' statement, we get

$$(\exists x \in \mathbb{Z}) \text{ not } \left(\Big((\exists y \in \mathbb{Z})\ x = 3y + 1 \Big) \Longrightarrow \Big((\exists y \in \mathbb{Z})\ x^2 = 3y + 1 \Big) \right).$$

Using the rule for negating an 'if...then' statement, we get

$$(\exists x \in \mathbb{Z}) \Big((\exists y \in \mathbb{Z})\ x = 3y + 1 \Big) \text{ and not } (\exists y \in \mathbb{Z})\ x^2 = 3y + 1.$$

Using the rule for negating a 'there exists' statement, we get

$$(\exists x \in \mathbb{Z}) \Big((\exists y \in \mathbb{Z})\ x = 3y + 1 \Big) \text{ and } (\forall y \in \mathbb{Z})\ x^2 \neq 3y + 1.$$

The rules for negating statements all make intuitive sense; please take a moment to think over each one until you understand it.

In the following exercises, try to prove the given statements from scratch, using only Definitions A.1 and A.2 and the rules of logic.

Exercises

1. Prove the following statements:

   (a) For every integer x, if x is even, then for every integer y, xy is even.

   (b) For every integer x and for every integer y, if x is odd and y is odd then $x + y$ is even.

   (c) For every integer x, if x is odd then x^3 is odd.

   What is the negation of each of these statements?

2. Prove that for every integer x, $x + 4$ is odd if and only if $x + 7$ is even.

3. Figure out whether the statement we negated at the end of this section is true or false, and prove it (or its negation).

4. Prove that for every integer x, if x is odd then there exists an integer y such that $x^2 = 8y + 1$.

Appendix B

Sets

In this appendix we review some basic concepts of set theory, and we give some simple examples of mathematical proofs.

B.1 Sets

Intuitively, a **set** is a collection of objects. Some commonly used sets are:

$\mathbb{R}$ = the set of real numbers,

$\mathbb{Q}$ = the set of rational numbers,

$\mathbb{Z}$ = the set of integers,

$\mathbb{N}$ = the set of natural numbers (nonnegative integers),

$\mathbb{Z}^+$ = the set of positive integers.

One can describe a set by listing, in curly braces, all the objects that the set contains. For example, the statement

$$S = \{1, 2, 3\}$$

defines S to be the set containing the numbers 1, 2, and 3. Sometimes we use an ellipsis $(\ldots)$ to save ink, especially for sets with infinitely many elements; for example,

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

The objects that a set contains are called the **elements**, or **members**, of that set. So 1 is an element of $\mathbb{N}$, while -4 is not. The notation '$x \in A$' means that x is an element of the set A. The notation '$x \notin A$' means that x is *not* an element of A. For example, $5 \in \mathbb{N}$ and $\pi \in \mathbb{R}$, while $3/2 \notin \mathbb{Z}$ and $\sqrt{2} \notin \mathbb{Q}$. (A proof of the last assertion is given in §**??**.)

The elements of a set can be other sets; for example, $\{1, \{2\}\}$ is the set whose elements are 1 and $\{2\}$. So $1 \in \{1, \{2\}\}$ and $\{2\} \in \{1, \{2\}\}$, but $2 \notin \{1, \{2\}\}$.

The **empty set**, denoted $\emptyset$, is a special set which doesn't have any elements; in other words, $\emptyset = \{\}$. One can think of the empty set as a box with nothing inside.

Another way to describe a set is to give a rule for deciding whether or not an object is an element of the set. For example, the set of natural numbers could be defined as follows:

$$(\forall x)\ x \in \mathbb{N} \iff x \in \mathbb{Z} \text{ and } x \geq 0.$$

If $P(x)$ is a statement about x, we use the notation $\{x \mid P(x)\}$ to indicate the set of all x for which $P(x)$ is true. For example,

$$\mathbb{N} = \{x \mid x \in \mathbb{Z} \text{ and } x \geq 0\}.$$

Another notation for this is

$$\{x \in \mathbb{Z} \mid x \geq 0\}.$$

This reads, "the set of integers x such that $x \geq 0$." Some more examples:

$$\begin{aligned} \mathbb{Q} &= \{x \in \mathbb{R} \mid (\exists a, b \in \mathbb{Z})\ b \neq 0 \text{ and } x = a/b\}, \\ \emptyset &= \{x \mid x \neq x\}, \\ \{1,2,3\} &= \{x \in \mathbb{N} \mid x > 0 \text{ and } x < 4\} \\ \text{the set of even integers } &= \{x \in \mathbb{Z} \mid (\exists y \in \mathbb{Z})\ x = 2y\}. \end{aligned}$$

If A and B are sets, and if every element of A is also an element of B, we say that A is a **subset** of B, and we write $A \subset B$. In symbols,

$$A \subset B \iff (\forall x)\ x \in A \Longrightarrow x \in B$$

For example, $\mathbb{Z}$ is a subset of $\mathbb{R}$, but $\mathbb{R}$ is not a subset of $\mathbb{Z}$. Every set is a subset of itself. Also, the empty set is a subset of every set; for any set A, the statement

$$(\forall x)\ x \in \emptyset \Longrightarrow x \in A$$

is vacuously true, since the statement "$x \in \emptyset$" is always false. On the other hand, the empty set is the only set that is a subset of the empty set.

Two sets are equal if and only if they have the same elements; in terms of subsets,

$$A = B \iff A \subset B \text{ and } B \subset A$$

For example,

$$\{1,2,3\} = \{2,3,1\},$$

but

$$\{1,\{2\}\} \neq \{1,2\}.$$

Exercises

1. List separately the elements and the subsets of $\{\{1,\{2\}\},\{3\}\}$. (There are 2 elements and 4 subsets.)
2. Explain why if $A \subset B$ and $B \subset C$, then $A \subset C$.
3. If a set has exactly n elements, how many subsets does it have? Why?
4. We have repeatedly used the words, '*the* empty set'. Is this justified? If A and B are both sets that contain no elements, then is A necessarily equal to B?

B.2 Unions and intersections

The **union** of two sets A and B, denoted by $A \cup B$, is the set of all objects that are in A, or B, or both:

$$A \cup B \stackrel{\text{def}}{=} \{x \mid x \in A \text{ or } x \in B\}.$$

The **intersection** of A and B is the set of all objects that are in both A and B:

$$A \cap B \stackrel{\text{def}}{=} \{x \mid x \in A \text{ and } x \in B\}.$$

For example,

$$\{1,2,3\} \cup \{2,3,4\} = \{1,2,3,4\},$$
$$\{1,2,3\} \cap \{2,3,4\} = \{2,3\}.$$

Venn diagrams provide a nice way to visualize these and other set-theoretic concepts. In Figure B.1(a), the inside of the circle on the left represents the contents of A, while the inside of the circle on the right represents B. The shaded region is $A \cup B$. In Figure B.1(b), the shaded region is $A \cap B$. How would you demonstrate the meaning of "$A \subset B$" with a Venn diagram?

The following are some basic properties of the union and intersection operations. We will leave the proofs of most of these facts as exercises.

Commutative properties.

$$A \cup B = B \cup A \qquad A \cap B = B \cap A$$

Associative properties.

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

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

Figure B.1: (a) Venn diagram for $A \cup B$. (b) Venn diagram for $A \cap B$.

Distributive properties.

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

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

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

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

Other facts.

$$A \cup A = A = A \cap A$$

$$A \cup \emptyset = A$$

$$A \cap \emptyset = \emptyset$$

$$A \cap B \subset A \subset A \cup B$$

$$A \cap B \subset B \subset A \cup B$$

A proof that two sets are equal usually consists of two parts: in the first part, labeled '($\subset$)', we show that the first set is a subset of the second; in the second part of the proof, labeled '($\supset$)', we show that the second set is a subset of the first.

Example B.1 Prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

($\subset$) Suppose $x \in A \cup (B \cap C)$. We wish to show that $x \in (A \cup B) \cap (A \cup C)$. By definition of union, $x \in A$ or $x \in B \cap C$.

Case 1: Suppose $x \in A$. Then $x \in A$ or $x \in B$, so $x \in A \cup B$. Likewise, $x \in A \cup C$. Thus $x \in A \cup B$ and $x \in A \cup C$, so $x \in (A \cup B) \cap (A \cup C)$.

Case 2: Suppose $x \in B \cap C$. Then $x \in B$ and $x \in C$. Since $x \in B$, it follows that $x \in A \cup B$. Since $x \in C$, it follows that $x \in A \cup C$. Thus $x \in (A \cup B) \cap (A \cup C)$.

($\supset$) Suppose $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$. We wish to show that $x \in A \cup (B \cap C)$, i.e., $x \in A$ or $x \in B \cap C$. Suppose $x \notin A$. It is enough to show that $x \in B \cap C$. Since $x \in A \cup B$ and $x \notin A$, it follows that $x \in B$. Likewise, since $x \in A \cup C$, $x \in C$. Thus $x \in B \cap C$. $\square$

In this example we have written down a lot of the details, but not every single one. For example, at the bottom of the proof, we write

> Since $x \in A \cup B$ and $x \notin A$, it follows that $x \in B$. Likewise, since $x \in A \cup C$, $x \in C$. Thus $x \in B \cap C$.

If we wanted to include every single detail, we would write

> Since $x \in A \cup B$, $x \in A$ or $x \in B$. Since $x \notin A$, it follows that $x \in B$. Since $x \in A \cup C$, $x \in A$ or $x \in C$. Since $x \notin A$, it follows that $x \in C$. Thus $x \in A$ and $x \in C$, so $x \in B \cap C$.

However, we prefer to be concise and omit obvious steps, provided that the reader can easily follow the argument. Usually a proof is centered around a few simple ideas, and excessive writing will tend to obscure them.

Before passing to the exercises, we would like to mention one thing about the union and intersection operations. These are *binary* operations, which means that they can only operate on two sets at once. If we want to take the union of three sets A, B, and C, there are two different ways we might do this: either

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

or

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

But the associative property says that these two expressions are equal. So when we write

$$A \cup B \cup C,$$

we mean either of the two expressions above. Likewise for intersection.

Similarly, if n is any positive integer and $A_1, A_2, \ldots, A_n$ are sets, then there is no ambiguity in the expressions

$$A_1 \cup A_2 \cup \ldots \cup A_n$$

and

$$A_1 \cap A_2 \cap \ldots \cap A_n.$$

The union of $A_1, A_2, \ldots, A_n$ is the set of all things which are in at least one of these n sets; the intersection of $A_1, A_2, \ldots, A_n$ is the set of all things which are in all n sets.

Exercises

1. Which of the following statements are true, and which are false? Why?
   (a) $\{\{\emptyset\}\} \cup \emptyset = \{\emptyset, \{\emptyset\}\}$
   (b) $\{\{\emptyset\}\} \cup \{\emptyset\} = \{\emptyset, \{\emptyset\}\}$
   (c) $\{\emptyset, \{\emptyset\}\} \cap \{\{\emptyset\}, \{\{\emptyset\}\}\} = \{\emptyset\}$
   (d) $\{\emptyset, \{\emptyset\}\} \cap \{\{\emptyset\}, \{\{\emptyset\}\}\} = \{\{\emptyset\}\}$
2. Prove the commutative properties of union and intersection.
3. Prove the associative properties of union and intersection.
4. Prove the other distributive properties of union and intersection.
5. Prove the remaining facts about union and intersection that we listed.
6. Prove that if $A \subset B$ and $A \subset C$ then $A \subset (B \cap C)$.
7. Prove that if $A \subset A'$ and $B \subset B'$, then $A \cup B \subset A' \cup B'$ and $A \cap B \subset A' \cap B'$.

B.3 Set difference

The **difference** between two sets A and B, denoted by $A - B$, is defined as follows:

$$A - B \stackrel{\text{def}}{=} \{x \mid x \in A \text{ and } x \notin B\}.$$

Figure B.2 gives a Venn diagram illustrating this operation. For example, $\mathbb{Z} \setminus \mathbb{N}$ is the set of negative integers. Some literature uses the notation '$A \setminus B$' instead of $A - B$.

The following are some basic properties of the set difference operation which you should remember.

De Morgan's laws.

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

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

Figure B.2: The shaded region is $A - B$.

Other facts.

$$A - B \subset A \qquad B \cap (A - B) = \emptyset$$
$$A - B = \emptyset \iff A \subset B$$
$$A - B = A \iff A \cap B = \emptyset$$

Example B.2 Prove that $A - (B \cup C) = (A - B) \cap (A - C)$.

($\subset$) Suppose $x \in A - (B \cup C)$. Then $x \in A$, and $x \notin B \cup C$. Since it is not true that $x \in B$ or $x \in C$, we know that $x \notin B$ and $x \notin C$. Since $x \in A$ and $x \notin B$, we have $x \in (A - B)$. Likewise, $x \in (A - C)$. Thus $x \in (A - B) \cap (A - C)$.

($\supset$) Suppose $x \in (A - B) \cap (A - C)$. Then $x \in A$, $x \notin B$, and $x \notin C$. It is not true that $x \in B$ or $x \in C$, so $x \notin (B \cup C)$. Thus $x \in A - (B \cup C)$. □

There are many more set-theoretic identities which we have not listed. However, instead of memorizing a huge list of identities, it is better to figure out and prove identities as they are needed. In mathematical writing, one usually omits proofs of simple set identities. (But don't do that for the exercises in this chapter.)

Exercises

1. Prove the other facts about set difference that we listed.
2. Show that $A - B = A - (A \cap B)$.
3. Show that $A \cap (B - C) = (A \cap B) - (A \cap C)$. Is it always true that $A \cup (B - C) = (A \cup B) - (A \cup C)$?
4. Show that if $A \subset A'$ and $B \supset B'$, then $A - B \subset A' - B'$.
5. (challenge problem) Write a computer program that can prove all of the set-theoretic identities in this chapter (and more). *Hint:* use Table A.1.

Appendix C

Induction

Mathematical induction is a useful technique for proving statements about natural numbers.

C.1 The principle of mathematical induction

Let $P(n)$ be a statement about the positive integer n. For example, perhaps

$$P(n) = \text{ “}n \text{ is a multiple of 5.”}$$

or

$$P(n) = \text{ “If } n \text{ is even, then } n^2 \text{ is divisible by 4.”}$$

Suppose we want to show that $P(n)$ is true for every positive integer n. How can we do this? One way is the following:

1. Prove that $P(1)$ is true.

2. Prove that for every $n \in \mathbb{Z}^+$, if $P(n)$ is true, then $P(n+1)$ is true.

Why does this work? Well, we know that $P(1)$ is true. Since $P(1) \implies P(2)$, we know that $P(2)$ is true. Since $P(2) \implies P(3)$, we know that $P(3)$ is true. Since $P(3) \implies P(4)$, we know that $P(4)$ is true. We can continue this indefinitely, so we see that $P(n)$ is true for every positive integer n.

By analogy, suppose we have a chain of dominoes standing on end. If we push over the first domino, and if each domino knocks over the next domino as it falls, then eventually every domino will fall. This reasoning is called the principle of **mathematical induction.** As we will see later in this chapter, it can be regarded as one of the axioms defining the natural numbers. Let us state it precisely.

Principle of Mathematical Induction (PMI). Let $P(n)$ be a statement about the positive integer n. If the following are true:

1. $P(1)$,
2. $(\forall n \in \mathbb{Z}^+)\, P(n) \Longrightarrow P(n+1)$,

then $(\forall n \in \mathbb{Z}^+)\, P(n)$.

A proof by induction consists of two parts. In the first part, called the **base case**, we show that $P(1)$ is true. In the second part, called the **inductive step**, we assume that $P(n)$ is true, where n is a positive integer (although we don't know what it is), and we deduce that $P(n+1)$ is true. The assumption that $P(n)$ is true is called the **inductive hypothesis.**

Example C.1 For every positive integer n,

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

Proof. We will use induction on n.

Base case: When $n = 1$, $1 + \cdots + n = 1$, and $n(n+1)/2 = 1 \cdot 2/2 = 1$.

Inductive step: Suppose that for a given $n \in \mathbb{Z}^+$,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \qquad \text{(inductive hypothesis)}$$

Our goal is to show that

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

i.e.,

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

Adding $(n+1)$ to both sides of the inductive hypothesis, we get

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

□

We can also use induction to complete the proof of the Closed Set Theorem of Chapter 2.

Example C.2 If $A_1, \ldots, A_n$ are closed sets, then $A_1 \cup \cdots \cup A_n$ is closed.

Proof. We will use induction on n.

Base case: When $n = 1$, this is trivial.

Inductive step: Assume that the statement is true for n. We wish to show that the statement is true for $n+1$. Let $A_1, \ldots, A_n, A_{n+1}$ be closed sets. By inductive hypothesis, $A_1 \cup \cdots \cup A_n$ is closed. By Axiom C2,

$$\mathbf{K}((A_1 \cup \cdots \cup A_n) \cup A_{n+1}) = \mathbf{K}(A_1 \cup \cdots \cup A_n) \cup \mathbf{K}A_{n+1}$$

$$= (A_1 \cup \cdots \cup A_n) \cup A_{n+1},$$

so $A_1 \cup \cdots \cup A_{n+1}$ is closed. □

Recall that if a and b are real numbers and $ab = 0$, then $a = 0$ or $b = 0$. Using induction, we can extend this to the following:

Example C.3 If $a_1, a_2, \ldots, a_n$ are real numbers and $a_1 a_2 \cdots a_n = 0$, then for some i with $1 \leq i \leq n$, $a_i = 0$.

Proof. We will use induction on n.

Base case: For $n = 1$, this is trivial.

Inductive step: Suppose the statement is true for n. We wish to show that the statement is true for $n+1$. Suppose $a_1, \ldots, a_n, a_{n+1}$ are real numbers such that $a_1 a_2 \cdots a_n a_{n+1} = 0$. Since $(a_1 \cdots a_n)a_{n+1} = 0$, it follows that $a_1 \cdots a_n = 0$ or $a_{n+1} = 0$.

If $a_1 \cdots a_n = 0$, then by inductive hypothesis, $a_i = 0$ for some i with $1 \leq i \leq n$, and we are done. If $a_{n+1} = 0$, we are also done. □

In mathematical writing, simple induction proofs like this are often omitted. For example, in proving the Closed Set Theorem, one could first prove that the union of two closed sets is closed, and then say, "It follows by induction that the union of n closed sets is closed." (But don't do that for the exercises in this chapter.)

Exercises

1. Prove that for all positive integers n,

$$1 + 4 + 9 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

2. Fix a number $x \neq 1$. Show that for every positive integer n,

$$1 + x + x^2 + \ldots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

3. Guess a formula for

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)}$$

and prove it by induction. *Hint:* Compute the above expression for some small values of n.

4. (requires §1.1) Let $(X, \mathbf{K})$ be a topological space, and suppose $A \subset X$. The operator $\mathbf{K}^n$ is defined as follows:

$$\mathbf{K}^n A \stackrel{\text{def}}{=} \underbrace{\mathbf{K} \cdots \mathbf{K}}_{n \text{ times}} A$$

Show that $\mathbf{K}^n = \mathbf{K}$ for all positive integers n.

5. (requires §1.4) Let $(X, \mathbf{K})$ be a topological space, and suppose $A_1, \ldots, A_n \subset X$. Show that:

   (a) $\mathbf{K}(A_1 \cup \cdots \cup A_n) = \mathbf{K}A_1 \cup \cdots \cup \mathbf{K}A_n$

   (b) $\mathbf{K}(A_1 \cap \cdots \cap A_n) \subset \mathbf{K}A_1 \cap \cdots \cap \mathbf{K}A_n$

6. Find another proof of Example C.1. (There are quite a few of them.)

7. Show that a $2^n \times 2^n$ checkerboard with one square removed can be tiled with L-tetrominoes. (An **L-tetromino** is a shape consisting of three squares joined in an 'L'-shape.)

8. (challenge problem) What is the largest number of regions into which 5 planes can divide $\mathbb{R}^3$?

C.2 The Well-Ordering Principle

The following may seem obvious.

Well-Ordering Principle (WOP). Any nonempty set of positive integers has a least element.

However, it is not true for negative integers, rational numbers, or real numbers. For example, $\{x \in \mathbb{R} \mid x > 0\}$ has no least element.

The well-ordering principle is equivalent to the principle of mathematical induction. To see this, we will first prove that the principle of induction implies the well-ordering principle. In other words, we will prove WOP by induction.

PMI$\Longrightarrow$WOP. Let S be a set of positive integers with no least element. We will show that S is empty. To do this, we will prove by induction on n that for every positive integer n, S does not contain any numbers less than n.

Base case: S cannot contain any numbers smaller than 1, since S is a set of positive integers.

Inductive step: Suppose S does not contain any numbers smaller than n. We wish to show that S does not contain any numbers smaller than $n+1$. It is enough to show that $n \notin S$. If $n \in S$, then n is a least element of S, since S contains no numbers less than n. But we assumed that S has no least element, so this is a contradiction. □

We will leave the proof of WOP$\Longrightarrow$PMI as an exercise. As a hint, here is another proof of Example C.1, using the well-ordering principle instead of induction.

Example C.4 For every positive integer n,

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

Proof. Suppose not. Then by the well-ordering principle, there is a least positive integer m such that

$$1 + 2 + \cdots + m \neq \frac{m(m+1)}{2}.$$

Now $m \neq 1$, since $1 = 1 \cdot 2/2$. So $m > 1$, and thus $m - 1$ is a positive integer. By definition of m,

$$1 + 2 + \cdots + [m-1] = \frac{[m-1]([m-1]+1)}{2} = \frac{(m(m-1)}{2}.$$

Adding m to both sides of this equation, we get

$$1 + 2 + \cdots + m = \frac{m(m-1)}{2} + \frac{m \cdot 2}{2} = \frac{m(m+1)}{2}.$$

This is a contradiction. □

Exercises

1. Prove that WOP$\Longrightarrow$PMI.

2. Show that the smallest element of a nonempty set of positive integers is unique.

3. Prove the Division Theorem: if a and b are positive integers, then there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < b$. (q is the quotient when a is divided by b, and r is the remainder.) *Hint:* Use the well-ordering principle to select the smallest nonnegative integer in the set

$$\{a - 0 \cdot b, a - 1 \cdot b, a - 2b, \ldots\}.$$

4. The following is an incorrect "proof" that PMI$\Longrightarrow$WOP. Where is the mistake?

> We will prove by induction on n that if n is a positive integer and if S is a set of n positive integers, then S has a least element. If $n = 1$, this is obvious. Now suppose the statement is true for n, and let S be a set of $n + 1$ positive integers. We must find a least element of S. Choose any element $x \in S$. By inductive hypothesis, $S - \{x\}$ has a least element, which we'll call y. If $x < y$, then x is a least element of S. Otherwise, y is a least element of S. □

Hint: every sentence in the above paragraph is true.

5. Show that there do not exist positive integers x, y, and z such that $x^2+y^2 = 3z^2$. *Hint:* By looking at the remainders when $x^2 + y^2$ and $3z^2$ are divided by 4, show that if $x^2+y^2 = 3z^2$, then x, y, and z are all divisible by 2. This leads to a contradiction as in Theorem **??**.

C.3 Everything you always wanted to know about the natural numbers, but were afraid to ask

Have you ever wondered how to prove a statement such as '1+1=2'? The main difficulty is in defining what '1', '2', and '+' mean. In this section, we will see how to prove many basic facts about the natural numbers, starting from five simple axioms.

What are the natural numbers, anyway? Well, 0 is a natural number. Every natural number has a **successor**, which is also a natural number. For example, the successor of 0 is ordinarily referred to as '1', the successor of '1' is '2', etc. We denote the successor of x by $S(x)$, or Sx for short. If we start from 0 and keep taking successors, we never run into the same number twice. In other words, different natural numbers have different successors, and 0 is not the successor of any natural number. Also, if we start with 0 and keep taking successors, we will eventually reach all of the natural numbers. One way to say this, more or less (see the remarks at the end of this section), is that if $P(x)$ is a statement about the natural number x, if $P(0)$ is true, and if $P(x) \Longrightarrow P(S(x))$ for all

natural numbers x, then $P(x)$ is true for all natural numbers x. In other words, induction works. (It doesn't really matter that we are starting from 0 instead of from 1.)

These statements are sufficient to prove most true statements about the natural numbers. They are called the **Peano axioms.** Here is a formal restatement of them:

Peano Axioms.

(Axiom P1) $0 \in \mathbb{N}$.

(Axiom P2) $(\forall x \in \mathbb{N})\ S(x) \in \mathbb{N}$.

(Axiom P3) $(\forall x \in \mathbb{N})\ S(x) \neq 0$.

(Axiom P4) $(\forall x, y \in \mathbb{N})\ x \neq y \Longrightarrow S(x) \neq S(y)$.

(Axiom P5) If $P(0)$ and $(\forall x \in \mathbb{N})\ P(x) \Longrightarrow P(S(x))$, then $(\forall x \in \mathbb{N})\ P(x)$.

One can think of these axioms as a *definition* of the natural numbers. (But see the remarks at the end of this section.)

Our next goal is to define addition. Suppose x is a fixed natural number. For each natural number y, what should $x + y$ be? We can give a **recursive definition** as follows:

Axioms for Addition. For every natural number x and y,

(Axiom A1) $x + 0 = x$.

(Axiom A2) $x + Sy = S(x + y)$.

Axiom A1 is like the base case of an induction proof; it shows how to find $x + y$ when $y = 0$. Axiom A2 is like an inductive step; it shows how to find $x + Sy$, assuming we know what $x + y$ is.

For example, suppose we want to compute $2 + 2$, or in our notation, $SS0 + SS0$. We have:

$$\begin{aligned} SS0 + SS0 &= S(SS0 + S0) && \text{(by Axiom A2)} \\ &= SS(SS0 + 0) && \text{(by Axiom A2)} \\ &= SS(SS0). && \text{(by Axiom A1)} \end{aligned}$$

So the answer is $SSSS0$, otherwise known as '4'. The general case works, informally, as follows:

$$\underbrace{S \cdots S}_{m \text{ times}} 0 + \underbrace{S \cdots S}_{n \text{ times}} 0 = \underbrace{S \cdots S}_{n \text{ times}} (\underbrace{S \cdots S}_{m \text{ times}} 0 + 0)$$

$$= \underbrace{S \cdots S}_{n \text{ times}}(\underbrace{S \cdots S}_{m \text{ times}} 0) = \underbrace{S \cdots S}_{m+n \text{ times}} 0.$$

This makes intuitive sense, but if we want to be rigorous about our definition of addition, there are two questions we must answer. First, do the axioms for addition make sense? In other words, does there exist an addition function with these properties? It is conceivable that we have designed our axioms foolishly and that they in fact lead to some contradiction. Second, do our axioms completely determine the nature of addition? In other words, is it possible that there exists more than one addition function with these properties? Both of these worries are settled by the following theorem. This is a special case of a general "principle of recursive definition".

Theorem C.5 *There exists a unique addition function satisfying Axioms A1 and A2.*

Proof. It is enough to prove that for each x, there exists a unique way to define $x + y$ so that the addition axioms are satisfied. We will prove this by induction on x.

Base case: Define $0 + y = y$. This satisfies Axiom because $0 + 0 = 0$ and Axiom A2 because $0 + Sy = Sy = S(0 + y)$. To prove uniqueness, suppose that $+'$ is another addition function, defined for $x = 0$ and any y, satisfying the addition axioms. Then I claim that $0 +' y = 0 + y$ for all natural numbers y. This is a simple proof by induction which we will leave to the reader.

Inductive step: Suppose addition is uniquely defined for a given x and satisfies the axioms. Define

$$Sx + y \stackrel{\text{def}}{=} S(x + y).$$

Axiom A1 is satisfied because

$$\begin{array}{rcll} Sx + 0 & = & S(x + 0) & \text{(by definition)} \\ & = & Sx. & \text{(by inductive hypothesis)} \end{array}$$

Axiom A2 is satisfied because

$$\begin{array}{rcll} Sx + Sy & = & S(x + Sy) & \text{(by definition)} \\ & = & S(S(x + y)) & \text{(by inductive hypothesis)} \\ & = & S(Sx + y). & \text{(by definition)} \end{array}$$

The uniqueness proof is essentially the same as before and will be left to the reader. □

We will now prove some of the basic properties of addition. First, let us prove that the successor of a number is just that number plus one.

Theorem C.6 *If $x \in \mathbb{N}$, then $x + S0 = Sx$.*

Proof.

$$\begin{aligned} x + S0 &= S(x+0) && \text{(by Axiom A2)} \\ &= Sx. && \text{(by Axiom A1)} \end{aligned}$$

□

It is also true that $S0 + x = Sx$, and to prove this we will use induction.

Theorem C.7 *If $x \in \mathbb{N}$, then $S0 + x = Sx$.*

Proof. We will use induction on x. The base case is immediate from Axiom A1. For the inductive step, assume that $S0 + x = Sx$. Then

$$\begin{aligned} S0 + Sx &= S(S0 + x) && \text{(by Axiom A2)} \\ &= S(Sx). && \text{(by inductive hypothesis)} \end{aligned}$$

□

We will now prove that addition is commutative. We will use two lemmas, which are like the addition axioms in reverse.

Lemma C.8 *If $x \in \mathbb{N}$, then $0 + x = x$.*

Proof. We will use induction on x. The base case is immediate from Axiom A1. For the inductive step, assume that $0 + x = x$; then

$$\begin{aligned} 0 + Sx &= S(0 + x) && \text{(by Axiom A2)} \\ &= S(x). && \text{(by inductive hypothesis)} \end{aligned}$$

□

Lemma C.9 *If $x, y \in \mathbb{N}$, then $Sy + x = S(y + x)$.*

Proof. Let y be any natural number; we will prove that $Sy + x = S(y + x)$ for all natural numbers x, by induction on x. The base case is proved by using Axiom A1 twice. For the inductive step, assume that $Sy + x = S(y + x)$; then

$$\begin{aligned} Sy + Sx &= S(Sy + x) && \text{(by Axiom A2)} \\ &= SS(y + x) && \text{(by inductive hypothesis)} \\ &= S(y + Sx). && \text{(by Axiom A2)} \end{aligned}$$

□

Theorem C.10 (Commutativity of Addition) *If $x, y \in \mathbb{N}$, then*

$$x + y = y + x.$$

Proof. Let x be any natural number; we will prove that $x + y = y + x$ for all natural numbers y, by induction on y.

Base case:

$$\begin{aligned} x+0 &= x && \text{(by Axiom A1)} \\ &= 0+x. && \text{(by Lemma C.8)} \end{aligned}$$

Inductive step: Suppose $x+y=y+x$. Then

$$\begin{aligned} x+Sy &= S(x+y) && \text{(by Axiom A2)} \\ &= S(y+x) && \text{(by inductive hypothesis)} \\ &= Sy+x. && \text{(by Lemma C.9)} \end{aligned}$$

□

We can also prove that addition is associative.

Theorem C.11 (Associativity of Addition) *If $a, b, c \in \mathbb{N}$, then*

$$(a+b)+c = a+(b+c).$$

Proof. Let a and b be any natural numbers; we will prove by induction on c that $(a+b)+c = a+(b+c)$.

Base case:

$$\begin{aligned} (a+b)+0 &= a+b && \text{(by Axiom A1)} \\ &= a+(b+0). && \text{(by Axiom A1)} \end{aligned}$$

Inductive step: Suppose $(a+b)+c = a+(b+c)$. Then

$$\begin{aligned} (a+b)+Sc &= S((a+b)+c) && \text{(by Axiom A2)} \\ &= S(a+(b+c)) && \text{(by inductive hypothesis)} \\ &= a+S(b+c) && \text{(by Axiom A2)} \\ &= a+(b+Sc). && \text{(by Axiom A2)} \end{aligned}$$

□

Our proofs have made heavy use of Axiom P5, and none of the above means anything without Axioms P1 and P2. But so far we have not used Axioms P3 and P4 anywhere. For example, you may be familiar with arithmetic mod n, or "clock arithmetic", which does not satisfy P3, but for which all the statements we have proved so far are true.

The following is an example of the use of Axiom P4. Axiom P3 is required for some of the exercises at the end of this section.

Theorem C.12 (Right Cancellation Law for Addition) *If $x, y, z \in \mathbb{N}$ and $x+z = y+z$, then $x = y$.*

Proof. We will use induction on z. The base case follows easily from Axiom A1. For the inductive step, assume that the theorem is true for z. Suppose

$$x + Sz = y + Sz.$$

Applying Axiom A2 twice, we get

$$S(x + z) = S(y + z).$$

By Axiom P4,

$$x + z = y + z.$$

By inductive hypothesis, $x = y$. □

Using the addition function, we can give a recursive definition of multiplication.

Axioms for Multiplication. If $x, y \in \mathbb{N}$, then:

(Axiom M1) $x \cdot 0 = 0$.

(Axiom M2) $x \cdot Sy = (x \cdot y) + x$.

The proof that there is a unique multiplication function with these properties is similar to the proof of Theorem C.5 and will be left to the reader. The exercises below give hints on how to prove some of the basic arithmetic properties of multiplication.

Before concluding, it is only fair to mention that the Peano axioms do not entirely characterize the integers. Gödel's Incompleteness Theorem says that either the Peano axioms are self-contradictory (and we hope this is not true), or there is a statement that can be neither proved nor disproved using the axioms. What's more, there are two different "models" (universes, like the natural numbers, satisfying the axioms), one in which this statement is true, and another in which this statement is false. In other words, *it is impossible to say exactly what a natural number is using axioms alone*. You can learn more about these subtleties in a course on mathematical logic.

Exercises

1. Fill in the details in the proof of Theorem C.5.
2. Prove that there exists a unique multiplication function satisfying axioms M1 and M2. (You might want to do the other exercises first.)
3. Give a formal proof that $3 \cdot 2 = 6$.

4. Prove the "left distributive law": if $x, y \in \mathbb{N}$, then

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z).$$

Hint: use induction on z and the fact that addition is associative.

5. Prove that multiplication is associative; that is, if $x, y, z \in \mathbb{N}$, then

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

Hint: use induction on z and Exercise 4.

6. (a) Prove that if $x \in \mathbb{N}$ then $0 \cdot x = 0$.
   (b) Prove that if $x, y \in \mathbb{N}$ then $Sx \cdot y = (x \cdot y) + y$. *Hint:* use induction on y and associativity and commutativity of addition.
   (c) Prove that multiplication is commutative.

7. Prove that if x is a natural number and $x \neq 0$, then there exists a natural number y such that $x = Sy$. (This is a rather strange proof by induction.)

8. Prove that if x and y are natural numbers and $x + y = 0$, then $x = 0$ and $y = 0$. *Hint:* use Exercise 7 and Axiom P3.

9. Define a relation '$\leq$' on the natural numbers as follows:

$$x \leq y \iff (\exists z \in \mathbb{N})\ y = x + z.$$

Prove the following:

   (a) If $x \leq y$ and $y \leq z$, then $x \leq z$.
   (b) If $x \leq y$ and $y \leq x$, then $x = y$.
   (c) If $x \in \mathbb{N}$, then $x + S0 \not\leq x$.
   (d) If $x \leq x'$ and $y \leq y'$, then $x + y \leq x' + y'$ and $x \cdot y \leq x' \cdot y'$.
   (e) If $x, y \in \mathbb{N}$, then $x \leq y$ or $y \leq x$. *Hint:* use induction on y and Exercise 7.
   (f) If $x \leq y$ and $y \leq x + S0$, then $y = x$ or $y = x + S0$.

10. (a) Prove that if $x \neq 0$ and $y \neq 0$, then $x \cdot y \neq 0$. (See Exercise 7.)
    (b) Prove the Left Cancellation Law for Multiplication: if $x \neq 0$ and $x \cdot y = x \cdot z$, then $y = z$. *Hint:* use induction on y and part (a).