Introduction to Mathematical Proof

Math 299 Lecture Notes

Ken Monks - Spring 2021

Introduction to Mathematical Proof

Dr. Monks - University of Scranton

Contents

0 Introduction **3**

1 What is a proof? **4**
1.1 Formal Proof Systems . . . 5
1.2 Environments and Statements . . . 6

2 The Language of Mathematics **8**
2.1 Identifiers, Variables, and Constants . . . 8
2.2 Expressions and Statements . . . 9
2.3 Substitution and Lambda Expressions . . . 10

3 Rules of Inference in Mathematics **11**
3.1 Template Notation for Rules of Inference . . . 11

4 Propositional Logic **13**
4.1 The Statements of Propositional Logic . . . 13
4.2 The Rules of Propositional Logic . . . 14
4.3 Formal Proof Style . . . 16

5 Predicate Logic **19**
5.1 Quantifiers . . . 19
5.2 Statements . . . 20
5.3 Declarations . . . 20
5.4 Rules of Inference . . . 20
5.5 Equality . . . 21

6 Proof Shortcuts and Semiformal Proofs **26**
6.1 Use Theorems as Rules of Inference . . . 26
6.2 Substitute Logically Equivalent Expressions . . . 27
6.3 Use Famous Logic Theorems Freely . . . 27
6.4 Identify Certain Statements . . . 28
6.5 Skip Some Logical Rules of Inference . . . 29
6.6 Omit Most Premise Citations, Line Labels, and End-of-Subproof Symbols . . . 31
6.7 Eliminate Extra Parentheses for Associative Binary Operators . . . 31
6.8 Combine consecutive ∀+ rules . . . 31
6.9 Use Transitive Chains! . . . 33
6.10 Use Derived Rules of Inference . . . 34

7 The Natural Numbers **36**
7.1 The Peano Postulates . . . 36

7.2 Strong Induction . . . 36
7.3 Number Theory . . . 37
7.4 Applications: Cardinal and Ordinal Numbers . . . 39

8 Sequences **42**
8.1 Finite and Infinite Sequences . . . 42
8.2 Representations of Sequences . . . 42
8.3 Reindexing . . . 44
8.4 Recursive Definitions and Sequences . . . 45

9 Integer, Rational, and Real Numbers **50**
9.1 Notation . . . 50
9.2 The Axioms for Real Numbers . . . 50
9.3 Basic Properties of Real Numbers . . . 52
9.4 Integers . . . 54
9.5 Extending Definitions . . . 55
9.6 Infinite Series and Decimal Representation . . . 57

10 Sets, Functions, Numbers **58**
10.1 Basic Definitions from Set theory . . . 58
10.2 Shortcuts involving sets . . . 62
10.2.1 Use Typed Declarations . . . 62
10.2.2 Use Extended Set-Builder Notation . . . 63
10.3 Famous Sets of Numbers . . . 64
10.4 Functions . . . 66
10.5 Relations . . . 72

11 Expository Proofs **77**
11.1 Traditional Proofs . . . 78
11.2 Specific Rules for Mathematical Writing . . . 78
11.3 Notation . . . 78
11.4 Syntax . . . 79
11.5 Equations and Formulas . . . 81
11.6 Writing Technique . . . 82
11.7 Mathematical Typesetting . . . 83

12 Combinatorial Proofs **84**
12.1 Combinatorics . . . 84
12.2 Combinatorical Collections and Expressions . . . 84
12.3 Combinatorial Proofs . . . 85
12.4 Combinatorial subtraction, division, and inequality . . . 86

0 Introduction

The development of logic and mathematics over thousands of years is one of the great achievements of human cognition.

On the one hand, its usefulness and practical importance in the modern world is hard to overstate. It provides a foundation upon which science, engineering, finance, medicine, economics, computer science, agriculture, and many other areas of human knowledge have been developed. But this fact raises an interesting question. *Why?*

Why is it that such a wide and disparate collection of applications from counting to cosmology all rely upon mathematics? Why are they built upon mathematics instead of something else like, say, music or poetry? Most of us recognize that mathematics is exceedingly useful, but *why* is it so useful?

One possible reason is that it provides us with a reliable starting point on which to build *consensus*. A group can accomplish much more by working collaboratively than they can by working as separate individuals. But cooperation and collaborative decision-making require a consensus about the assumptions, terminology, and facts that allow us to communicate and inform our decisions.

Mathematics and its underlying logic provide us with a tool that allows us to reason in a way that is reliable, objectively verifiable, and independent of our individual, personal, and subjective human biases. Mathematicians do not debate whether 5 is larger than 4, or whether $2 + 3 = 5$. The fact that mathematics can be verified objectively and reliably is what makes it a prototype for achieving consensus about mathematical facts. Other disciplines that can successfully build upon mathematics can then use it to construct a solid foundation for consensus about facts in their own subject area.

In addition to being useful, mathematics is one of the most beautiful, creative, and sublime creations of the human mind. It is inherently valuable for its own sake as a work of art, to be enjoyed and shared with others, and passed down from generation to generation for thousands of years.

For this reason, our introduction to mathematical proof must combine both the rigorous objectivity that is needed for determining and communicating mathematical facts, with the elegance and beauty that exemplifies any human art form.

The main reason mathematics and logic are so amenable to building consensus is that *anyone can check a mathematical claim for themselves*. There is no need to believe anyone, cite any book, or consult any oracle. We can each take personal ownership of our mathematics by proving all of it ourselves.

The goal of this course is to do exactly that. It will guide you on a personal journey to build and verify most of elementary mathematics from the ground up. It is a quest to objectively prove for yourself all of the basic elementary mathematical facts about logic, natural numbers, sequences, real numbers, set theory, functions, relations, and combinatorics.

To accomplish this, we must begin by slowly and carefully defining exactly what constitutes a mathematical proof, how to construct them ourselves, and how to express them up in a way that allows them to be accurately shared them with others.

1 What is a proof?

Simply stated

> A *proof* is an **explanation** of why a statement is **objectively correct**.

Thus, we have two goals for our proofs.

- **Veracity** - we want to verify that a statement is *objectively correct*.
- **Exposition** - we want to be able to effectively and elegantly *explain why* it is correct.

However, these two goals are sometimes in conflict. So how to achieve both?

The Proof Spectrum

To be certain that our proof is correct, we need to be exceedingly careful and rigorous. To be clear in our exposition, we need to be succinct and elegant.

To obtain elegant clarity without sacrificing correctness, we will begin with proofs that are objectively correct by virtue of the fact that they can be verified by a machine. This style of proof is called a *formal proof*. Then we will use a well-defined set of *proof shortcuts* to eliminate tedious, repetitive, and uninteresting parts of our proofs. Thus, we will construct a bridge between our formal proofs and the more *traditional proofs* found in journals, textbooks, and problem solutions.

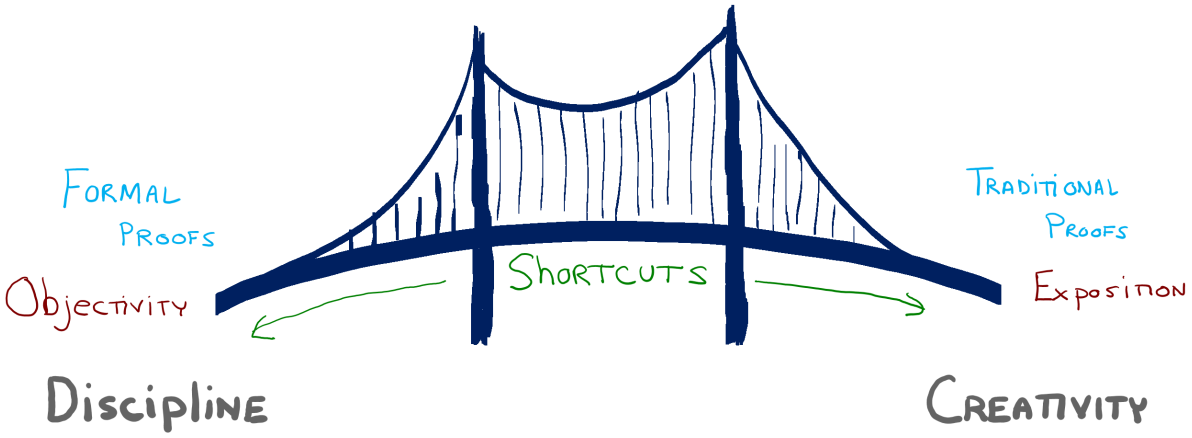


Figure 1: The Proof Spectrum

Rigor and Elegance

On the one hand, mathematical proofs need to be rigorous. Whether submitting a proof to a math contest or submitting research to a journal or science competition, we naturally want it to be correct. One way to ensure our proofs are correct is to have them checked by a computer. (Note

that checking to see if a proof is correct is much easier for a computer to do than finding a proof in the first place.)

There is much discussion in mathematics today about the value of computer verified proofs and their counterparts - rigorous, detailed, formal proofs. Mathematicians and computer scientists such as Vladimir Voevodsky and Leslie Lamport have been making a strong case for formal, rigorous, computer-verified proofs.

On the other hand, most mathematicians are attracted to mathematics because of its intrinsic beauty. A proof that communicates the key ideas of a proof to the reader in a succinct and beautiful way is very effective for its expository properties, even if it is not as rigorous as a formal proof. The legendary mathematician Paul Erdös always spoke of "The Book", an imaginary book in which God had written down the best and most elegant proofs for mathematical theorems. When he saw any particularly inspiring proof, he would exclaim "That proof is from 'The Book'!"

We will strive for both rigor and elegance in our proofs by building a bridge between highly rigorous formal proofs and more elegant traditional proofs. We begin with formal proofs.

> "*Math is a cross between art and law. Law is about the reasoning and proving. And the art is because what we're trying to prove are statements that are somehow elegant. That's where the artist decides what is art.*" - US IMO Coach Po-Shen Loh, after his team won the 2015 IMO

1.1 Formal Proof Systems

We begin on the left hand end of the bridge by defining a formal proof system that we will use in this course.

Definition 1. A *Formal Proof System* (or Formal Axiom System) consists of

1. A set of expressions called *statements*.
2. A set of rules called *rules of inference*.

Each rule of inference has zero or more inputs called *premises* and one or more outputs called *conclusions*. Most premises and all conclusions of a rule of inference are statements in the system.[1] There also may be *conditions* on when a particular rule of inference can be used.

Definition 2. An *axiom* is a conclusion of a rule of inference that has no premises.

Definition 3. A statement Q in a formal axiom system is *provable from* premises $Q_1, \ldots, Q_n$ if

1. Q is a conclusion of a rule of inference when $P_1, \ldots, P_k$ are the premises, and
2. for each $1 \leq i \leq k$, if P_i is a statement, then P_i is provable from $Q_1, \ldots, Q_n$.

In particular, if Q is an axiom, then Q is provable from no premises at all!

Definition 4. If Q follows from no premises in a formal axiom system, we say that Q is *provable* in the system. A provable statement is called a *theorem*.

[1] Other common premises are variable declarations, constant declarations, and subproofs.

And finally, the definition we've all been waiting for!

Definition 5. A *proof* of a statement in a formal axiom system is a sequence of applications of the rules of inference (i.e., *inferences*) that show that the statement is a theorem in that system.

1.2 Environments and Statements

The set of statements in the formal systems used in mathematics are generally some syntactically well-defined collection of expressions. In some systems, the statements may be purely symbolic, such as " $1 < \sqrt{2}$ " or " $(A \cap B)' = A' \cup B'$ ". In others, the statements may be English sentences, such as "The number 2021 is the product of two consecutive primes." or "Every set of natural numbers has a least element.".

We frequently organize the sentences in a book by collecting them together into nested hierarchical structures called chapters, sections, subsections, and so on. Similarly, statements in mathematics are also frequently organized by placing them into nested hierarchical structures called **environments** or **contexts**. A math textbook can also have environments such as chapters, sections, subsections, but will also frequently contain other more specialized mathematical environments, called theorems, proofs, subproofs, definitions, declarations, examples, and many others.

Environments serve two main purposes. First, as the name suggests, an environment provides a context that delineates where certain assumptions or definitions are assumed to be under consideration. For example, if the author says in Chapter 1 of a book, "In this chapter we will assume that n is a positive integer.", then the reader would not normally assume that the same assumption about n holds in Chapter 2.

Second, the rules of inference of many formal systems can also use environments as inputs and outputs in addition to statements. We will encounter several examples of this later on, but for now there is one kind of environment that will be almost immediately useful and necessary.

Notation. If Q is provable from premises $P_1, \ldots, P_n$ in a formal system we can denote this symbolically as

$$P_1, \ldots, P_n \vdash Q$$

This expression is defined to be a kind of environment, which we will call a *proposition* or *subproof*. Each of the variables in the expression can be either a statement or another environment. Such expressions can also have multiple conclusions, $Q_1, \ldots, Q_m$, in which case we can write them as

$$P_1, \ldots, P_n \vdash Q_1, \ldots, Q_m$$

You can think of such an expression as saying that Q can be proven in the current context if we temporarily add $P_1, \ldots, P_n$ as axioms to the currently available rules of inference. Note that the premises to the left of the $\vdash$ are not in any particular order and duplicates are redundant, so need not be listed (i.e., it is a set of premises, not a list). The same is true for the conclusions on the right.

Lurch

Lurch is a word processor that allows you to define your own formal axiom systems and check your proofs in that system! Check it out at lurchmath.org.

Problems

Toy Proofs

There are several examples of simple Formal Proof Systems available online at

`proveitmath.org/toyproofs`

1.1. *Scrambler!* is a formal proof system where the statements are finite sequences of colors. The Rules of Inference are permutations of these sequences (and so have one premise and one conclusion each). The goal is to apply the Rules to show that a given sequence of colors is provable from another given sequence of colors.

Try to find a strategy for reliably beating each of the difficulty levels (*Weeny*, *Easy*, *Fun*, *Three Ring Circus*, *Frogs*, *Dizzy*, *Mutant Frogs*, and *Death!*) of *Scrambler!* They are listed in increasing order of difficulty. Warning: it can be both addictive and hard!

1.2. *Trix Game* is a formal proof system where the statements are positive integers. There are only two Rules of Inference, both of which take a single positive integer as a premise, and return a single positive integer as their conclusion. This system illustrates a rule that has a condition on when you can use it. The goal is to show that a given positive integer is provable from the premise 1 in the system.

Try to find a strategy for winning. Warning: if you can prove that you will always win this game no matter what integer you have for the goal, you will win money and be famous forever!

1.3. *Circle-Dot* is a formal proof system where the statements are just finite sequences of one or more circles and dots. This formal system has many of the features in common with actual mathematical formal axiom systems. There are five rules of inference, two of which are axioms. The goal is to prove various circle-dot strings in the system.

(a) Try to prove Theorem A thru Theorem R in the *Circle-Dot* web application.

(b) Bonus: Can you explain why every circle-dot expression can be proven in the Circle-Dot toy system, or if not, determine with absolute certainty exactly those expressions which can?

1.4. Define a toy formal system as follows. The statements can be any finite string of one or more characters, and there are two rules of inference.

> Rule 0: Given no premises (inputs), we can conclude (output) the string `FLM`.
>
> Rule 1: Given any two strings as premises (inputs), we can conclude (output) their concatenation.

Notice that Rule 0 is an axiom.

(a) What are the theorems in this system?

(b) What statements can be proven from the statement `GS`?

(c) List all statements that can be proven from the `GS` and `LTR` that are less than 10 characters long.

1.5. Define a toy formal system as follows. The statements are all nonempty words that only contain the character ⋆. There are two rules of inference.

Rule 0: Given no premises, we can conclude the string ⋆⋆⋆.

Rule 1: Given no premises, we can conclude the string ⋆⋆⋆⋆⋆.

Rule 2: Given any two strings as premises, we can conclude their concatenation.

(a) Prove all theorems that are less than 12 characters long.

(b) What are all of the theorems in this system?

1.6. Define a toy formal system as follows. The statements are all words that begin with zero or more copies of the letter `Y` followed by one or more copies of the letter `X`. There are three rules of inference.

Rule 0: Given no premises, we can conclude `X`.

Rule 1: Given any premise, we can conclude the string formed by replacing every `Y` with `YY` and every `X` with `XX`.

Rule 2: Given any premise that has `XXX` either at the start of the string or immediately following a `Y`, we can conclude the string formed by replacing that occurrance of `XXX` with `Y`.

Rule 3: Given any premise that contains exactly two `X`s, we can conclude the string formed by deleting one of the two `X`s and then replacing every `Y` with `XX`.

For example, if you have `YYYXX` as a premise in Rule 3, then you could conclude `XXXXXXX`.

(a) Prove `XXXXX`.

(b) Prove `YY`.

(c) Prove `YYX`.

(d) What do you think the theorems are in this system?

2 The Language of Mathematics

We will write our proofs in the language of mathematics. In this section, we give an overview of the major building blocks of this language. These will be defined more rigorously as they come up in actual formal systems.

2.1 Identifiers, Variables, and Constants

One of the first things we learn as children is how to name things. In mathematics, the names we give to our ideas and structures are strings or symbols we will call *identifiers*. Whenever we define a formal system, we can specify which strings and symbols are the identifiers in that system. Identifiers in mathematics come in two flavors, *constants* and *variables*.

A *constant* can be thought of as an identifier that names a fixed, specific mathematical entity. Common examples of constants you have encountered in previous math courses like calculus are things like '7', "π", 'ln', 'cos', '+', and '='. They name a particular number or function or relation.

A *variable*, on the other hand, can be thought of as a name for an unspecified individual mathematical entity, usually of a certain type. The most common identifiers used for this purpose in mathematics are a single lower case letter, upper case letter, or Greek letter, such as 'x', 'P', or 'α'.

2.2 Expressions and Statements

Identifiers can also be combined in various ways to form larger mathematical expressions. A single identifier is called an *atomic expression*. A mathematical expression comprised of more than one identifier is called a *compound expression*. The same identifier might appear more than once in a compound expression. Like variables, expressions will frequently represent a mathematical object of a certain type.

For example, you may have seen expressions such as '$y = x + 1$'. This compound expression contains two variables, 'x' and 'y', and three constants, '=', '+', and '1'.

In addition to indentifiers, mathematical expressions often use punctuation and formatting to form expressions that are easier to read, or to distinguish or identify two expressions. Common punctuations used in mathematical expressions include parentheses, elipses, and commas. Common formatting used includes superscripts, subscripts, and arranging expressions into columns or grids in various ways. For example, we use expressions like '$\binom{n}{n}x^n + \binom{n}{n-1}x^{n-1} + \cdots + \binom{n}{0}$', '$a_0, a_1, \ldots, a_n$', and

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Mathematical expressions can also contain English words in addition to symbols. For example, you may have seen piecewise functions defined by an expression like

$$T(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{3n+1}{2} & \text{otherwise} \end{cases}$$

Indeed, many mathematical expressions will consist entirely of English words. For example,'The hypotenuse is the longest side of a right triangle.' is one such expression.

As we embark on our journey to build mathematics from the ground up, we will say exactly which mathematical expressions constitute the statements in the formal systems we define. Generally speaking, statements will be mathematical expressions which can be said to be true or false – expressions which if you said them in a courtroom during a trial, a lawyer could accuse you of lying or telling the truth.

For example, expressions like '$2 < 3$', '$1 + 1 = 3$', and 'Every set is a subset of itself.' are usually statements in mathematics because they are either true or false, whereas expressions like '$\frac{1}{2}$', '$2+2$', or '$\triangle ABC$' are not. Notice, however, that we do not need to know whether a statement is true or false to know that it is a statement. For example, '$x < 2$' is true if x represents the number 1 but false if it represents the number 2. Either way, we can say that the expression '$x < 2$' is either true or false, and therefore can be considered a statement.

2.3 Substitution and Lambda Expressions

We can prefix any expression E to form the expression '$\lambda x, E$' to indicate that all occurrences[2] of the variable x in E represent the same unspecified object of the same type as x. These prefixed expressions are called *lambda expressions* (or *anonymous functions*).

Such expressions can be *applied* to an expression a having the same type as x to form a new expression, $(\lambda x, E)(a)$ which has the same type as E. These can be *evaluated* to form the expression obtained by replacing all occurrences[3] of x in E with (a)[4]. If we give a name to a lambda expression, e.g., if we define f to be $\lambda x, E$ then the expression $(\lambda x, E)(a)$ is just the usual notation for function application $f(a)$. In this situation we refer to a as the *argument* of the lambda expression application.

For example, $(\lambda x, x^3)(a)$ evaluates to a^3. Indeed, in many math textbooks they will write $f(x) = x^3$ instead of writing $f = (\lambda x, x^3)$, but the latter is usually what they mean. In this example, we would have the usual evaluation of functions, e.g., $f(a) = a^3$, $f(2) = 2^3$, and $f(x + 1) = (x + 1)^3$.

Notice that simply replacing all occurrences of x in $\lambda x, E$ with another identifier that does not appear in E produces a new lambda expression which evaluates to the same thing as the original lambda expression when applied to the same argument.

Problems

2.1. Evaluate the following expressions.

(a) $(\lambda x, x^2 + x + 1)(3)$

(b) $(\lambda x, x^2 + x + 1)(s)$

(c) $(\lambda x, x^2 + x + 1)(s^2 + s + 1)$

(d) $(\lambda x, 5)(t)$

(e) $(\lambda x, 5)(t + 1)$

(f) $(\lambda x, \cos(x) + \sin(y))(1)$

(g) $(\lambda y, \cos(x) + \sin(y))(1)$

(h) $\lambda x, (\lambda y, \cos(x) + \sin(y))(1)$

(i) $(\lambda x, (\lambda y, \cos(x) + \sin(y))(1))(2)$

(j) $(\lambda T, T \text{ is isosceles})(ABC)$

(k) $(\lambda T, T \text{ is isosceles})(DEF)$

2.2. Let f be $\lambda n, 2 \cdot n$ and let g be $\lambda n, n + 2$. Evaluate the following.

(a) $f(k)$

(b) $g(k)$

(c) $f(g(k))$

(d) $g(f(k))$

(e) $f(f(k))$

(f) $g(g(k))$

(g) $f(g(k + 1))$

(h) $g(f(k + 1))$

(i) $f(f(k + 1))$

(j) $g(g(k + 1))$

[2] These refer to free occurrences – see section 5.1.

[3] Also no free identifier in a should become bound as a result of the substitution – see section 5.1.

[4] in many situations the parentheses around a can be omitted for clarity

2.3. Suppose we have the following named lambda expressions.

$$\lambda W, \lambda V, (WV, VW \vdash W) \tag{R_1}$$
$$\lambda W, \lambda (V, W, V \vdash W \bullet V) \tag{R_2}$$
$$\lambda W, \lambda V, (WV\bullet \vdash W\bigcirc) \tag{R_3}$$

Evaluate the following.

(a) $(R_1(\bullet))(\bigcirc)$

(b) $(R_2(\bullet))(\bigcirc)$

(c) $(R_3(\bullet))(\bigcirc)$

(d) $R_1(\bullet\bigcirc\bullet)$

(e) $R_2(\bullet\bigcirc\bullet)$

(f) $R_3(\bullet\bigcirc\bullet)$

3 Rules of Inference in Mathematics

In the Circle-Dot system, Axiom A is a rule of inference that says from no premises we can conclude $\bigcirc\bullet$. Rule 1, however, is technically not a rule of inference, but rather an infinite family of rules of inference, one for each choice of circle-dot strings we can substitute for the variables W and V. From this perspective, we can think of Rule 1 as the lambda expression,

$$\lambda W, \lambda V, (WV, VW \vdash W)$$

So that, for example, substituting $\bigcirc$ for W and $\bullet$ for V produces the rule

$$\begin{aligned}(\lambda W, \lambda V, (WV, VW \vdash W))(\bigcirc)(\bullet) &= (\lambda V, (\bigcirc V, V\bigcirc \vdash \bigcirc))(\bullet) \\ &= (\bigcirc\bullet, \bullet\bigcirc \vdash \bigcirc)\end{aligned}$$

which allows us to conclude $\bigcirc$ from the premises $\bullet\bigcirc$ and $\bigcirc\bullet$.

Most rules of inference in mathematics are more similar to Rule 1 than to Axiom A in this sense – they are really lambda expressions which generate an entire family of specific rules of inference, one for each choice of variable in the statement of the rule. Because this is so common, we usually omit the lambda prefixes, and use the convention that any variable W that appears in the premises or conclusion of a rule of inference can be replaced with an expression of the same type to form a particular instance of that rule of inference.

3.1 Template Notation for Rules of Inference

While the turnstile notation for rules of inference like the Circle-Dot rule above is very compact, it is helpful to write our rules of inference in notation that looks more like the way will be used in a proof. We can do this by writing thenm in the form of a template that we can fill in when using the rule to justify a statement in our proof.

To accomplish this we define another notation for the kinds of rules of inference we will encounter in mathematics.

Notation. A rule of inference having premises $P_1, \ldots, P_k$ and conclusions $Q_1, \ldots, Q_n$ can be expressed in *template notation* or *recipe notation* as

Rule Name Here	
P_1	(show)
⋮	
P_k	(show)
.....	
Q_1	(conclude)
⋮	
Q_n	(conclude)

In this notation, the rule looks like a template that we can fill in to create our proofs. In particular, the lines marked with a (show) need to be justified with a rule of inference that is supplied as a reason for that line, and those marked with (conclude) can be justified with the given rule of inference.

Some rules of inference have a premise of the form

$$(P_1, \ldots, P_k \vdash Q)$$

This is not a statement in the formal system itself, but rather the assertion that Q can be proven from $P_1, \ldots, P_k$ in the formal system. We call an expression of this form a *subproof* or *environment*. Such a premise is satisfied by including a subproof in a proof that shows that Q can be proved from the given premises (which do not need to be justified by a rule of inference). We denote this in recipe notation as an indented 'assume-block' as illustrated below.

Example 6. Suppose we have a rule of inference that justifies the following.

$$W \text{ or } V, (W \vdash U), (V \vdash U) \vdash U$$

where W, V, and U are any mathematical statements. Then we would express this rule in recipe notation as

Proof by Cases	
W or V	(show)
Assume W	
U	(show)
←	
Assume V	
U	(show)
←	
.....	
U	(conclude)

In this, everything between an Assume and the following ← (the 'end assumption' symbol) is a

subproof that demonstrates the corresponding premise in the rule of inference. We indent such assumption blocks in our proofs. Subproofs can be nested, and the level of indentation corresponds to the level of nesting. Assumptions (lines that start with Assume) do not need to be justified by a rule of inference. We say that they are *given*. Lines marked with (show) must be justified. Lines marked with (conclude) are justified by the rule itself.

Note that we do include the word "Assume " in the proof itself, but not the words "show" or "conclude" which are just instructions to the proof author (as opposed to the reader) for how to justify the indicated lines.

4 Propositional Logic

We now turn our attention to a formal axiom system that is based on one first formulated by Gerhard Gentzen in 1934 as a formal system that closely imitates the way mathematicians actually reason when writing traditional expository proofs.

4.1 The Statements of Propositional Logic

The language of propositional logic has two constants `true` and `false`. We sometimes will abbreviate these as `T` and `F` respectively. The statements in the language are all expressions of this type, namely, they all represent a *truth value* which is either `true` or `false`. Any variable can be used to represent a statement in this system. Such variables, and the constants `true` and `false` are the atomic statements in the language of propositional logic.

In addition to the atomic statements, we can form compound statements as follows.

In addition, we can form compound statements by first defining five constants, "not", "and", "or", "⇒", and "⇔", and using them to define compound statements as follows.

Definition. Let φ, ψ be statements. Then the five expressions "not φ", "φ and ψ", "φ or ψ", "$\varphi \Rightarrow \psi$", and "$\varphi \Leftrightarrow \psi$" are also statements whose truth values are completely determined by the truth values of W and ψ as shown in the following table:

φ	ψ	$\neg\varphi$	φ and ψ	φ or ψ	$\varphi \Rightarrow \psi$	$\varphi \Leftrightarrow \psi$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

We can also write '¬' for not, 'if and only if' for ⇔, and 'implies' for ⇒. A statement of the form '$\varphi \Rightarrow \psi$' is called a *conditional statement* or an *implication*, and can be written in English in several different ways: 'φ implies ψ', 'if φ then ψ', 'ψ follows from φ', or 'ψ, if φ'.

Thus, the statements of Propositional Logic consist of

1. Atomic Statements that do not contain any of the five logical operators, and
2. Compound Statements that are one of the five forms, $\neg\varphi$, φ and ψ, φ or ψ, $\varphi \Rightarrow \psi$, or $\varphi \Leftrightarrow \psi$ where φ and ψ are any statements of Propositional Logic.

Note: In compound statements we usually put parentheses around the statements φ or ψ involved. For instance if φ is the statement 'P or Q' and ψ is the statement 'R and S' then $\varphi \Rightarrow \psi$ should be written

$$(P \text{ or } Q) \Rightarrow (R \text{ and } S)$$

in order to avoid the confusion that 'P or $Q \Rightarrow R$ and S' might actually mean something like P or $(Q \Rightarrow (R \text{ and } S))$. In order to cut down on parentheses, we assign a **precedence** order for our operators, meaning we apply the operators in the following order (from highest to lowest).

Precedence of Notation
parentheses, brackets, (), {}, [] etc.
arithmetic operations* $\wedge, \cdot, +, \ldots$ etc.
set operations $\times, -, \cap, \cup, \ldots$ etc.
arithmetic and set relations $=, \subseteq, \leq, \neq, \ldots$ etc.
not
and , or
$\Rightarrow$
$\Leftrightarrow$
$\forall, \exists, \exists!$

* with the usual precedence among them

4.2 The Rules of Propositional Logic

Natural deduction generally defines a pair of rules for each definition. A 'plus' rule is used to prove statements that contain the thing being defined from statements that do not, while 'minus' rules do the opposite. In the following rules, the variables W and V can be any statement.

Rules of Propositional Logic	
Name	Rule
and+	$W, V \vdash (W \text{ and } V)$
and−	$(W \text{ and } V) \vdash W, V$
or+	$W \vdash (W \text{ or } V), (V \text{ or } W)$
or− *(proof by cases)*	$(W \text{ or } V), (W \Rightarrow U), (V \Rightarrow U) \vdash U$
$\Rightarrow$+	$(W \vdash V) \vdash (W \Rightarrow V)$
$\Rightarrow$− *(modus ponens)*	$(W \Rightarrow V), W \vdash V$

Rules of Propositional Logic (cont.)

Name	Rule
$\Leftrightarrow +$	$(W \Rightarrow V), (V \Rightarrow W) \vdash (W \Leftrightarrow V)$
$\Leftrightarrow -$	$(W \Leftrightarrow V) \vdash (W \Rightarrow V), (V \Rightarrow W)$
not+ *(proof by contradiction)*	$(W \vdash \ \rightarrow\leftarrow) \vdash \text{not}\, W$
not− *(proof by contradiction)*	$(\text{not}\, W \vdash \ \rightarrow\leftarrow) \vdash W$
$\rightarrow\leftarrow +$	$W, (\text{not}\, W) \vdash \ \rightarrow\leftarrow$

We can also list these rules in template notation that mirrors how they are used in proofs.

Propositional Logic

and +	and −
W (SHOW) V (SHOW) ..... W and V (CONCLUDE)	W and V (SHOW) ..... W (CONCLUDE) V (CONCLUDE)
$\Rightarrow +$	$\Rightarrow -$ (modus ponens)
Assume W V (SHOW) $\leftarrow$ ..... $W \Rightarrow V$ (CONCLUDE)	W (SHOW) $W \Rightarrow V$ (SHOW) ..... V (CONCLUDE)
$\Leftrightarrow +$	$\Leftrightarrow -$
$W \Rightarrow V$ (SHOW) $V \Rightarrow W$ (SHOW) ..... $W \Leftrightarrow V$ (CONCLUDE)	$W \Leftrightarrow V$ (SHOW) ..... $W \Rightarrow V$ (CONCLUDE) $V \Rightarrow W$ (CONCLUDE)
or +	or − (proof by cases)
W (SHOW) ..... W or V (CONCLUDE) V or W (CONCLUDE)	W or V (SHOW) $W \Rightarrow U$ (SHOW) $V \Rightarrow U$ (SHOW) ..... U (CONCLUDE)
not + (proof by contradiction)	not − (proof by contradiction)
Assume W $\rightarrow\leftarrow$ (SHOW) $\leftarrow$ ..... $\neg W$ (CONCLUDE)	Assume $\neg W$ $\rightarrow\leftarrow$ (SHOW) $\leftarrow$ ..... W (CONCLUDE)

Propositional Logic (cont.)

→← +	
W	(SHOW)
$\neg W$	(SHOW)
.....	
→←	(CONCLUDE)

copy	
W	(SHOW)
.....	
W	(CONCLUDE)

Remarks:

- The symbol ← is an abbreviation for "end assumption".
- The symbol →← is called "contradiction" and represents the logical constant FALSE.
- The word Assume is actually entered as part of the proof itself, it is not just an instruction in the recipe like '(SHOW)' and '(CONCLUDE)'.
- The inputs Assume - and "←" are not themselves statements that you prove or are given, but rather are inputs to rules of inference that may be inserted into a proof at any time. There is no useful reason however, to insert such statements unless you intend to use one of the rules of inference that requires them as an input.
- The statement following an Assume is the same as any other statement in the proof and can be used as an input to a rule of inference.
- Statements in an Assume-← block can be used as inputs to rules of inference whose conclusion is also inside the same block only. Once a Assume is closed with a matching ←, only the entire block can be used as an input to a rule of inference. The individual statements within a block are no longer valid outside the block. We usually indent and Assume-← block to keep track of what statements are valid under which assumptions.

Definition. A compound statement of propositional logic is called a *tautology* if it is true regardless of the truth values the atomic statements that comprise it. (Its "truth table" contains only T's.)

It can be shown that a statement can be proved with Propositional Logic if and only if the statement is a tautology.

4.3 Formal Proof Style

One way to write down the proof of a theorem is called a *formal proof*. This style of proof consists of a sequence of numbered lines containing statements, reasons, and references to premises. Every line contains exactly one statement (or declaration - see below), and the reason given on that line is the name of a rule of inference for which the statement on that line is the conclusion. If the rule of inference has premises, the reason is followed by the line numbers containing the statements (or variable declarations) which are the premises that the rule is being applied to. References to premises can only refer to lines which appear earlier in the same proof which are not contained in a subproof that has been closed. Subproofs used as a premise are cited by listing the range of line numbers comprising the subproof.

Example 7. Let P and Q be statements. Prove the following case of DeMorgan's Law, namely that

$$\neg P \text{ or } \neg Q \Rightarrow \neg(P \text{ and } Q)$$

Proof.

1.	Assume $\neg P$ or $\neg Q$	-
2.	Assume $\neg P$	-
3.	Assume P and Q	-
4.	P	by and $-$; 3
5.	$\rightarrow\leftarrow$	by $\rightarrow\leftarrow$ +; 2,4
6.	$\leftarrow$	-
7.	$\neg(P$ and $Q)$	by not+; 3,5,6
8.	$\leftarrow$	-
9.	$\neg P \Rightarrow \neg(P$ and $Q)$	by $\Rightarrow$+; 2,7,8
10.	Assume $\neg Q$	-
11.	Assume P and Q	-
12.	Q	by and $-$; 11
13.	$\rightarrow\leftarrow$	by $\rightarrow\leftarrow$ +; 10,12
14.	$\leftarrow$	-
15.	$\neg(P$ and $Q)$	by not+; 11, 13, 14
16.	$\leftarrow$	-
17.	$\neg Q \Rightarrow \neg(P$ and $Q)$	by $\Rightarrow$+; 10,15,16
18.	$\neg(P$ and $Q)$	by or $-$; 1,9,17
19.	$\leftarrow$	-
20.	$\neg P$ or $\neg Q \Rightarrow \neg(P$ and $Q)$	by $\Rightarrow$ +; 1,18

□

Notice that when a rule of inference has a subproof for a premise, we indicate this by citing the line numbers for the assumption, the conclusion, and the end of assumption block indicator ($\leftarrow$) e.g., as shown in line 7 above.

Problems

Prove the following tautologies using formal proofs. In the following, P, Q, R, S are statements. Sometimes we add additional parentheses for legibility.

Easy Warmups

4.1. (*implies plus warmup*) $P \Rightarrow P$

4.2. (*iff plus warmup*) $P \Leftrightarrow P$

4.3. (*and plus warmup*) $P \Rightarrow (P \text{ and } P)$

4.4. (*or plus warmup*) $P \Rightarrow P \text{ or } Q$

4.5. (*and minus warmup*) $(P \text{ and } P) \Rightarrow P$

4.6. (*iff minus warmup*) $(P \Leftrightarrow Q) \Rightarrow (Q \Rightarrow P)$

4.7. (*implies minus warmup*) $((P \Rightarrow Q) \text{ and } P) \Rightarrow Q$

4.8. (*or minus warmup*) $P \text{ or } Q \Rightarrow Q \text{ or } P$

4.9. (*contradiction plus warmup*) $(Q \text{ and } \neg Q) \Rightarrow \rightarrow\leftarrow$

4.10. (*not plus warmup*) $(Q \text{ and } \neg Q) \Rightarrow \neg P$

4.11. (*not minus warmup*) $(Q \text{ and } \neg Q) \Rightarrow P$

Famous Tautologies

4.12. (*a contradiction implies anything*) $\rightarrow\leftarrow \Rightarrow P$

4.13. (*double negation*) $\neg\neg P \Leftrightarrow P$

4.14. (*modus tollens*) $((P \Rightarrow Q) \text{ and } \neg Q) \Rightarrow \neg P$

4.15. (*transitivity of* $\Rightarrow$) $(P \Rightarrow Q) \text{ and } (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$

4.16. (*contrapositive*) $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

4.17. (*true!*) $\neg \rightarrow\leftarrow$

4.18. (*excluded middle*) $P \text{ or } \neg P$

4.19. (*Pierce's Law*) $((P \Rightarrow Q) \Rightarrow P) \Rightarrow P$

4.20. (*alternate* or $-$) $((P \text{ or } Q) \text{ and } \neg P) \Rightarrow Q$

4.21. (*exclusive or*) $\neg(P \Leftrightarrow Q) \Leftrightarrow (\neg P \text{ and } Q) \text{ or } (P \text{ and } \neg Q)$

4.22. (*alternate* $\Rightarrow$) $(P \Rightarrow Q) \Leftrightarrow (\neg P \text{ or } Q)$

4.23. (*not implies*) $\neg\,(P \Rightarrow Q) \Leftrightarrow (P \text{ and } \neg Q)$

4.24. (*shunting*) $((P \text{ and } Q) \Rightarrow R) \Leftrightarrow (P \Rightarrow (Q \Rightarrow R))$

4.25. (*DeMorgan's Law*) $\neg(P \text{ and } Q) \Rightarrow \neg P \text{ or } \neg Q$

4.26. (*DeMorgan's Law*) $\neg(P \text{ or } Q) \Leftrightarrow \neg P \text{ and } \neg Q$

Atomic statements aren't just letters

4.27. (g is upper semi-computable) $\Rightarrow$ (g is a finite simplicial complex) or (g is upper semi-computable)

4.28. $\Big(\big(0 < x \Rightarrow 0 < x^3\big) \text{ and } \big(x < 0 \Rightarrow x^3 < 0\big)\Big) \text{ and } (0 < x \text{ or } x < 0) \Rightarrow \big(0 < x^3 \text{ or } x^3 < 0\big)$

4.29. The claim "If you like pizza and pizza is available then you will eat pizza" is true if and only if the claim "If you like pizza, then if pizza is available then you will eat pizza" is true.

4.30. It is not the case that (M is representable over $\mathbb{F}_2$ or M has an empty cokernal) if and only if (M is not representable over $\mathbb{F}_2$) and (M does not have an empty cokernal)

Commutativity

4.31. P and $Q \Leftrightarrow Q$ and P

4.32. (*see 4.8*) P or $Q \Leftrightarrow Q$ or P

4.33. $(P \Leftrightarrow Q) \Leftrightarrow (Q \Leftrightarrow P)$

4.34. Give examples of statements, P and Q such that $(P \Rightarrow Q) \Rightarrow (Q \Rightarrow P)$ is false.

Associativity

4.35. $((P$ and $Q)$ and $R) \Leftrightarrow (P$ and $(Q$ and $R))$

4.36. $((P$ or $Q)$ or $R) \Leftrightarrow (P$ or $(Q$ or $R))$

4.37. $((P \Leftrightarrow Q) \Leftrightarrow R) \Leftrightarrow (P \Leftrightarrow (Q \Leftrightarrow R))$

Distributivity

4.38. P and $(Q$ or $R) \Leftrightarrow (P$ and $Q)$ or $(P$ and $R)$

4.39. P or $(Q$ and $R) \Leftrightarrow (P$ or $Q)$ and $(P$ or $R)$

5 Predicate Logic

We can extend Propositional Logic by adding more statements and rules of inference to those we already have in our formal system. This extended formal system is called *Predicate Logic*.

5.1 Quantifiers

The symbol λ in the lambda expression $(\lambda x, E)$ is an example of a *quantifier*. The thing that all quantifiers have in common is that they *bind variables*. If W is an expression that does not contain any quantifiers, then every occurrence of every identifier that appears in the expression is said to be a *free* occurrence of that identifier.

If a quantifier appears in an expression, there are one or more variables that it binds. All occurrences of those variables that are in the scope of the quantifier (usually everything to the right of it until a scope delimiter for that quantifier is encountered) are called *bound variables*.

Predicate logic extends propositional logic by defining two additional quantifiers.

Definition. The symbols $\forall$ and $\exists$ are *quantifiers*. The symbol $\forall$ is called "for all", "for every", or "for each". The symbol $\exists$ is called "for some" or "there exists".

We will encounter more quantifiers beyond just these two and λ.

5.2 Statements

Every statement of Propositional Logic is still a statement of Predicate Logic. In addition, we define the following statements.

Definition. If x is any variable and W is a lambda expression[5] that evaluates to a statement when applied to any expression having the same type as x, then $(\forall x, W(x))$ and $(\exists x, W(x))$ are both statements.

We say that the *scope* of the quantifier in $(\forall x, W(x))$ and $(\exists x, W(x))$ is everything inside the outer parentheses. Sometimes the outer parentheses are omitted when the scope is clear from context. All occurrences of x throughout the scope are said to be bound by the quantifier.

5.3 Declarations

Before using a free identifier for the first time in any expression in our proofs we should tell the reader what that identifier represents. There are four ways to introduce a new free identifier.

1. It can be declared to be a variable (a variable declaration).
2. It can be declared to be a constant (a constant declaration).
3. It can be defined as temporary new notation, usually as an abbreviation for a larger expression (a notational definition).
4. It can occur free in an expression preceding the proof itself, such as in the statement of the theorem, in a premise that is given, or declared globally prior to the start of the proof (globally declared).

Bound variables do not have to be declared. They can be any identifier you like, as long as that identifier is not in the scope of a constant declaration or more than one quantifier that binds it.

5.4 Rules of Inference

The rules of inference for these two quantifiers are as follows.

Rules of Inference for Predicate Logic

Name	Rule
$\forall+$	$(\text{Let } s \text{ be arbitrary} \vdash W(s)) \vdash (\forall x, W(x))$
$\forall-$	$(\forall x, W(x)) \vdash W(t)$
$\exists+$	$W(t) \vdash (\exists x, W(x))$
$\exists-$	$(\exists x, W(x)) \vdash \text{For some constant } c, W(c)$

These can also be expressed in template notation.

[5] Not containing x.

Predicate Logic*

∀+	∀−
Let s be arbitrary (variable declaration) $W(s)$ (SHOW) ← …… $\forall x, W(x)$ (CONCLUDE)	$\forall x, W(x)$ (SHOW) …… $W(t)$ (CONCLUDE)
∃+	**∃−**
$W(t)$ (SHOW) …… $\exists x, W(x)$ (CONCLUDE)	$\exists x, W(x)$ (SHOW) …… For some c, (constant declaration) $W(c)$ (CONCLUDE)

**Restrictions and Remarks*

- In ∀+, s must be a new variable in the proof, cannot appear as a free variable in any assumption or premise, and $W(s)$ cannot contain any constants which were produced by the ∃− rule inside that subproof. The indentation and ← symbol indicate the scope of the declaration of s. Variables s and x must have the same type.
- In ∀− and ∃+, no free variable in t may become bound when t is substituted for x in $W(x)$. Variable x and expression t must have the same type.
- In ∃+, t can be an expression, and $W(x)$ can be the expression obtained by replacing one or more of the occurrences of t with x. The identifier x cannot occur free in $W(t)$. Variable x and expression t must have the same type.
- In ∃−, c must be a new identifier in the proof. Also $W(c)$ must immediately follow the constant declaration for c in the proof. The scope of the declaration continues indefinitely or until the end of the scope of any subproof block or variable declaration scope that contains the constant declaration. Variable x and constant c must have the same type.

  One consequence of this is that it enforces the restriction on ∀+ that prohibits any constant declared with ∃− to appear in $W(s)$ because after the application of ∀+ any free occurrence of c is no longer in the scope of the original declaration (and therefore undeclared).

5.5 Equality

Finally, we can complete our definition of logic by adding the rules of inference for equality.

Definition. The equality symbol, =, is defined by the following two rules of inference.

Rules of Inference for Equality

Name	Rule
reflexivity	$\vdash (x = x)$
substitution	$(x = y)$, $W \vdash$ (W with one or more free occurrences of x replaced by y)

Equality

Reflexivity*	Substitution*
.....	$x = y$ (show)
$x = x$	W (show)
	.....
	W with any free occurrences of x replaced by y. (conclude)

Restrictions and Remarks

- Note that in the Reflexive rule there are no inputs, so you can insert a statement of the form $x = x$ into your proof at any time.
- No free variable in y can become bound when y is substituted for x.

We can also use equality to define a useful variation of the $\exists$ quantifier.

Definition 8. If x, y are any variables of the same type and W is a lambda expression not containing x or y that evaluates to a statement when applied to any expression having the same type as x and y, we define

$$(\exists! x, W(x)) \Leftrightarrow \exists x, (W(x) \text{ and } \forall y, W(y) \Rightarrow y = x)$$

The statement $\exists! x, W(x)$ is read "There exists a unique x such that $W(x)$."

Rules of Inference for Unique Existence*

Name	Definition
$\exists!+$	$(\exists x, W(x) \text{ and } \forall y, W(y) \Rightarrow y = x) \vdash (\exists! x, W(x))$
$\exists!-$	$(\exists! x, W(x)) \vdash \exists x, W(x) \text{ and } \forall y, W(y) \Rightarrow y = x$

Rules of Inference for Unique Existence*

$\exists!+$	$\exists!-$
$W(s)$ (show)	$\exists! x, W(x)$ (show)
Let y be arbitrary (variable declaration)	.....
Assume $W(y)$	$\exists x, W(x) \text{ and } \forall y, W(y) \Rightarrow y = x$ (conclude)
$y = s$ (show)	
$\leftarrow$	
$\leftarrow$	
.....	
$\exists! x, W(x)$ (conclude)	

Rules of Inference for Unique Existence* (cont.)

$\neq +$		$\neq -$	
$\neg(x = y)$	(SHOW)	$x \neq y$	(SHOW)
.....		.....	
$x \neq y$	(CONCLUDE)	$\neg(x = y)$	(CONCLUDE)

Example 9. Let P be a lambda expression such that $P(x)$ is a statement. Prove the following case of DeMorgan's Law, namely that

$$(\exists x, \neg P(x)) \Rightarrow \neg\forall x, P(x)$$

Proof.

1.	Assume $\exists x, \neg P(x)$	-
2.	For some c,	-
3.	$\neg P(c)$	by $\exists$-; 1
4.	Assume $\forall x, P(x)$	-
5.	$P(c)$	by $\forall$-; 4
6.	$\rightarrow\leftarrow$	by $\rightarrow\leftarrow$+; 3,5
7.	$\leftarrow$	-
8.	$\neg\forall x, \neg P(x)$	by not+; 4,6
9.	$\leftarrow$	-
10.	$(\exists x, \neg P(x)) \Rightarrow \neg\forall x, P(x)$	by $\Rightarrow$+; 1,8

□

Problems

Prove each of the following theorems with a formal proof in our system of Natural Deduction. In all of these, P, Q, R are statements (or lambda expressions that return a statement) and the variables x, y, z etc. are of the same unspecified type.

Predicate Logic

5.1. (*alpha substitution*) $(\forall x, P(x)) \Rightarrow (\forall y, P(y))$

5.2. (*alpha substitution*) $(\exists x, P(x)) \Rightarrow (\exists y, P(y))$

5.3. (*distributivity*) $(\forall x, P(x) \text{ and } Q(x)) \Leftrightarrow (\forall y, P(y)) \text{ and } (\forall z, Q(z))$

5.4. (*distributivity*) $(\exists x, P(x) \text{ or } Q(x)) \Leftrightarrow (\exists y, P(y)) \text{ or } (\exists z, Q(z))$

5.5. (*distributivity*) $(\exists x, P(x) \Rightarrow Q(x)) \Leftrightarrow (\forall y, P(y)) \Rightarrow (\exists z, Q(z))$

5.6. (*equivalent predicates*) $(\forall x, P(x) \Leftrightarrow Q(x)) \Rightarrow ((\exists x, P(x)) \Rightarrow (\exists x, Q(x)))$

5.7. (*commutativity*) $(\forall x, \forall y, P(x,y)) \Rightarrow (\forall y, \forall x, P(x,y))$

5.8. (*commutativity*) $(\exists x, \exists y, P(x,y)) \Rightarrow (\exists y, \exists x, P(x,y))$

5.9. (*one for all*) $(\exists y, \forall x, P(x,y)) \Rightarrow (\forall x, \exists y, P(x,y))$

5.10. (*some are the same*) $(\forall x, \forall y, P(x,y)) \Rightarrow \forall z, P(z,z)$

5.11. (*DeMorgan*) $\neg(\exists x, P(x)) \Leftrightarrow (\forall x, \neg P(x))$

5.12. (*DeMorgan*) $\neg(\forall x, P(x)) \Leftrightarrow (\exists x, \neg P(x))$

5.13. (*quantifier fun*) $(\forall x, P(x) \Rightarrow Q(x))$ and $(\forall x, \neg Q(x)) \Rightarrow (\forall x, \neg P(x))$

5.14. (*more quantifier fun*) $(\forall x, P(x)$ or $Q(x))$ and $(\exists y, \neg P(y)) \Rightarrow (\exists z, Q(z))$

5.15. (*less than, for example*)

$$(\forall x, \neg P(x,x)) \text{ and } (\forall x, \forall y, \forall z, P(x,y) \text{ and } P(y,z) \Rightarrow P(x,z)) \Rightarrow (\forall x, \forall y, \neg(P(x,y) \text{ and } P(y,x)))$$

5.16. (*excluded middle*) $(\forall x, P(x))$ or $(\exists x, \neg P(x))$

In the next three theorems, P is a statement not containing x.

5.17. (*de-quantify*) $(\exists x, Q(x)$ and $P) \Leftrightarrow (\exists x, Q(x))$ and P

5.18. (*de-quantify*) $(\forall x, Q(x)$ or $P) \Leftrightarrow (\forall x, Q(x))$ or P

5.19. (*de-quantify*) $(\forall x, Q(x) \Rightarrow P) \Leftrightarrow (\exists x, Q(x)) \Rightarrow P$

Equality

5.20. (*symmetry of equality*) $x = y \Rightarrow y = x$

5.21. (*avoiding vacuous types*) $(\exists x, x = x)$ and $(\forall y, P(y)) \Rightarrow \exists z, P(z)$

5.22. (*alternate definition of unique existence*) $(\exists! x, P(x)) \Leftrightarrow (\exists x, P(x)$ and $\forall y, \neg(y = x) \Rightarrow \neg P(y))$

5.23. (*just logical*) Suppose 0 and $\leq$ such that $a \leq b$ is a statement for any a, b (including 0),

$$\Big((\exists! n, \forall k, n \leq k) \text{ and } (\forall m, 0 \leq m) \text{ and } (\forall m, \lambda \leq m)\Big) \Rightarrow \lambda = 0$$

5.24. Let $L(x,y)$ be the statement "x loves y" and the domain of discourse of all quantified variables be the set of all people. Write each of the following English statements using only 'and', 'or', $\neg$, $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$, $\exists!$, L, $=$, the bound variables x and y and the constants (names of people) given in the sentences. For example, we could express "Everyone loves Bob." as "$\forall x, L(x, \text{Bob})$".

(a) Alice loves everyone.

(b) Someone loves Alice.

(c) Bob loves Alice, but she does not love him.

(d) Everyone loves someone.

(e) There is only one person who loves everyone.

(f) Someone loves everyone.

(g) There is a person who is loved by only one person.

(h) Some people do not love themselves.

(i) Some people only love themselves.

(j) Nobody loves everybody.

(k) If everyone loves themselves, then everyone loves someone.

(l) If two people love each other, then everyone loves them both. (Note: In English, when "two" is used in this context it usually means "two distinct".)

5.25. Let $P(x, y)$ be the statement "x is the parent of y" and the domain of discourse of all quantified variables be the set of all people. What do each of the following say in English?

(a) $\forall x, \forall y, P(x, y)$ (e) $\forall x, \exists! y, P(x, y)$ (i) $\forall y, \forall x, P(x, y)$ (m) $\forall y, \exists! x, P(x, y)$

(b) $\forall x, \exists y, P(x, y)$ (f) $\exists! x, \forall y, P(x, y)$ (j) $\forall y, \exists x, P(x, y)$ (n) $\exists! y, \forall x, P(x, y)$

(c) $\exists x, \forall y, P(x, y)$ (g) $\exists x, \exists! y, P(x, y)$ (k) $\exists y, \forall x, P(x, y)$ (o) $\exists y, \exists! x, P(x, y)$

(d) $\exists x, \exists y, P(x, y)$ (h) $\exists! x, \exists! y, P(x, y)$ (l) $\exists y, \exists x, P(x, y)$ (p) $\exists! y, \exists! x, P(x, y)$

5.26. (a) Prove the following with a formal proof.

$$(\forall x, \exists! y, M(x, y)) \text{ and } \neg(a = b) \Rightarrow \neg(M(c, a) \text{ and } M(c, b))$$

(b) Suppose we are talking about people, and $M(x, y)$ means "the mother of x is y", and a, b, c are "Alice", "Beth", and "Carl". What does the theorem in part (a) say in English with this interpretation?

5.27. Given the first two statements, is the conclusion valid? If not, describe a situation where the conclusion is false. If it is, formalize the argument and give a formal proof.

Everyone fears Dracula.
Dracula only fears me.
Therefore, I *am* Dracula!

5.28. A function f that maps the positive real numbers to other positive real numbers is said to be *continuous* (C) if and only if

$$\forall \varepsilon, \forall x, \exists \delta, \forall y, \left|x - y\right| < \delta \Rightarrow \left|f(x) - f(y)\right| < \varepsilon$$

Similarly, f is said to be *uniformly continuous* (UC) if and only if

$$\forall \varepsilon, \exists \delta, \forall x, \forall y, \left|x - y\right| < \delta \Rightarrow \left|f(x) - f(y)\right| < \varepsilon$$

(all identifiers other than f have type "positive real").

(a) Give a formal proof that every uniformly continuous function is continuous.

(b) Find an example of a function f that is continuous but not uniformly continuous.

(You can use the fact that the real numbers are closed under multiplication, that constants like, 3, π, $\sqrt{2}$, $4/5$ are real numbers and properties of real number arithmetic, like $1 + 1 = 2$, or $x + x = 2x$, justifying these with the black-box reason 'by arithmetic'.)

6 Proof Shortcuts and Semiformal Proofs

When writing formal proofs we quickly find that the perfect rigor they provide is quickly offset by the extreme length and tediousness of the proofs. Indeed, this aspect of formal proofs is often counter to our goal of elegant and effective exposition. So how can we retain the objective validity and rigor of a formal proof and make our proofs more elegant and expository at the same time?

One way is to use well-defined *shortcuts* that eliminate the tedious, obvious aspects of our proofs, while retaining the rigor and important concepts. In this book we will list some of the shortcuts that mathematicians use in writing their proofs in order to shorten the proofs, make them more readable, and eliminate parts of the proof that are repetitive or uninteresting.

A proof that utilizes one or more shortcuts, but still has (a) at most one statement per line with optional justification as needed and (b) does not have to be written in complete, grammatically correct, English sentences, is called a *semiformal proof*.

6.1 Use Theorems as Rules of Inference

Once we have proved a theorem, we can use it as a new rule of inference. To use a theorem or definition as a rule of inference, we can just insert it as a line in our proof and justify it with the name of the theorem and no premises. Doing so leaves the set of provable statements unaltered, i.e., no statement that could be proved with the new rules of inference could be proved without them, because we can always replace the new rule of inference with its proof.

So for example, if we prove the following simple theorem

Theorem 10. $P \Rightarrow P$

Then in a proof we can simply insert a line such as

`12.` $P \Rightarrow P$ `by Theorem 1.`

But we can do better.

A free variable that appears in a premise or conclusion of a Rule of Inference is called a *metavariable*. Metavariables in a rule can be replaced with any statement of the appropriate type before using the rule.

Similarly, we can interpret the free variables in any Theorem as metavariables, and allow them to be replaced by an expression of the same type before inserting the theorem into our proof.

Interpreting Theorem 1 as a Rule of Inference in this way, we can thus insert a line in our proof like this

`18.` $\neg(Q \text{ or } R) \Rightarrow \neg(Q \text{ or } R)$ `by Theorem 1.`

This shortcut can also be applied to formal definitions, which can be thought of as a theorem whose proof is one line. These theorems can be used as a rule of inference in several ways.

6.2 Substitute Logically Equivalent Expressions

Whenever we have a theorem or definition that is an equivalence of the form $P \Leftrightarrow Q$, we can substitute occurrences of P with Q and vice versa whenever they appear as a subexpression in a statement in our proof. Equivalent statements have the same truth value, so replacing one with the other does not affect the validity of the statement where the substitution takes place.

For example, since we can prove that $\neg\neg P \Leftrightarrow P$, if we have a statement such as

$$\forall x, \exists y, \neg\neg\neg(y = x) \text{ and } f(y) = f(x)$$

We can immediately simplify this to

$$\forall x, \exists y, \neg(y = x) \text{ and } f(y) = f(x)$$

by substituting the subexpression $\neg(y = x)$ for the equivalent subsexpression $\neg\neg\neg(y = x)$.

6.3 Use Famous Logic Theorems Freely

The following theorems about logic are quite well-known, and can usually be used in an expository proof without proving them or even justifying them with a reason (although you should in a formal or semiformal proof). Since most of these are equivalences, they are frequently useful when combined with the previous shortcut.

Theorems of Logic	
excluded middle	P or $\neg P$
double negative	$\neg\neg P \Leftrightarrow P$
idempotency	P and $P \Leftrightarrow P$ P or $P \Leftrightarrow P$
commutativity	P and $Q \Leftrightarrow Q$ and P P or $Q \Leftrightarrow Q$ or P $(P \Leftrightarrow Q) \Leftrightarrow (Q \Leftrightarrow P)$ $(\forall x, \forall y, P(x, y)) \Leftrightarrow (\forall y, \forall x, P(x, y))$ $(\exists x, \exists y, P(x, y)) \Leftrightarrow (\exists y, \exists x, P(x, y))$
associativity	$(P$ and $Q)$ and $R \Leftrightarrow P$ and $(Q$ and $R)$ $(P$ or $Q)$ or $R \Leftrightarrow P$ or $(Q$ or $R)$ $((P \Leftrightarrow Q) \Leftrightarrow R) \Leftrightarrow (P \Leftrightarrow (Q \Leftrightarrow R))$
distributivity	P and $(Q$ or $R) \Leftrightarrow (P$ and $Q)$ or $(P$ and $R)$ P or $(Q$ and $R) \Leftrightarrow (P$ or $Q)$ and $(P$ or $R)$ $(\forall x, P(x))$ and $(\forall x, Q(x)) \Leftrightarrow (\forall x, P(x)$ and $Q(x))$ $(\exists x, P(x))$ or $(\exists x, Q(x)) \Leftrightarrow (\exists x, P(x)$ or $Q(x))$

Theorems of Logic (cont.)	
transitivity	$(P \Rightarrow Q)$ and $(Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$ $(P \Leftrightarrow Q)$ and $(Q \Leftrightarrow R) \Rightarrow (P \Leftrightarrow R)$
alpha substitution	$(\forall x, P(x)) \Leftrightarrow (\forall y, P(y))$ $(\exists x, P(x)) \Leftrightarrow (\exists y, P(y))$
alternate implies	$(P \Rightarrow Q) \Leftrightarrow (\neg P$ or $Q)$
alternate or-	$(P$ or $Q)$ and $\neg P \Rightarrow Q$ $(P$ or $Q)$ and $\neg Q \Rightarrow P$
not implies	$\neg\,(P \Rightarrow Q) \Leftrightarrow (P$ and $\neg Q)$
contrapositive	$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$
DeMorgan's Law	$\neg\,(P$ and $Q) \Leftrightarrow (\neg P$ or $\neg Q)$ $\neg\,(P$ or $Q) \Leftrightarrow (\neg P$ and $\neg Q)$ $(\neg\forall x, P(x)) \Leftrightarrow \exists x, \neg P(x)$ $(\neg\exists x, P(x)) \Leftrightarrow \forall x, \neg P(x)$
contradiction	$\rightarrow\leftarrow \Rightarrow Q$
alternate substitution	$x = y$ and $W \Rightarrow W$ with the nth free occurrence of y replaced by x.
alternate $\exists!$	$(\exists! x, W(x)) \Leftrightarrow \exists c, \forall z, W(z) \Leftrightarrow z = c$

6.4 Identify Certain Statements

In some cases, even using Shortcut 6.2 can still be too tedious. For example, if we have P and Q in our proof, but require Q and P as a premise, we might skip the substitution as a separate step, and instead do something like this:

⋮

11. P and Q `for some reason`
12. $(Q$ and $P) \Rightarrow R$ `for some other reason`
13. R `by ⇒ − ; 11,12`

⋮

Statements that typically can be identified without much trouble are given in the following table.

the statement	*can be identified with*
P and Q	Q and P

the statement	*can be identified with*
P or Q	Q or P
$P \Leftrightarrow Q$	$Q \Leftrightarrow P$
$\neg\neg P$	P
$x = y$	$y = x$
$x \neq y$	$\neg(x = y)$
$x > y$	$y < x$
$x \geq y$	$y \leq x$

6.5 Skip Some Logical Rules of Inference

While proof by contradiction, proof by cases, and other methods of proof are usually explicitly stated in a proof, some rules of inference are often skipped in an expository proof because they are so obvious to the reader. This can be accomplished by allowing an expression to be used as a premise in place of some statement that can be logically derived from it.

For example, we usually skip the '$\ldots$ and $+$' or '$\ldots$ and $-$' rules by allowing P and Q to be used as a premise whenever P or Q are required, e.g.,

$\vdots$

11. P and Q `for some reason`
12. $P \Rightarrow R$ `for some other reason`
13. R `by` $\Rightarrow -$ `; 11,12`

$\vdots$

Similar shortcuts can be used to avoid '$\ldots$ and $+$', e.g.,

$\vdots$

10. P `for some reason`
11. Q `for some other reason`
12. (P and Q) $\Rightarrow R$ `for yet another reason`
13. R `by` $\Rightarrow -$ `; 10,11,12`

$\vdots$

Notice that in this case we can specify three premises even though the '$\Rightarrow +$' only normally requires two premises. These examples can naturally be extended to expressions such as P and Q and R, and so on, even when using such an expression in place of, say, Q would normally require more than one application of the '$\ldots$ and $-$' rule.

A particularly common use of this shortcut is with the '$\Leftrightarrow$ +' rule. This is frequently abbreviated as follows.

Example 11. Suppose we have a theorem in this form (for some appropriate P and Q).

Theorem 12. $P \Leftrightarrow Q$

Then we will frequently abbreviate the proof like this.

Proof

($\Rightarrow$)		
1.	Assume P	-
⋮	⋮	⋮
11.	Q	for some reason
12.	$\leftarrow$	-
($\Leftarrow$)		
13.	Assume Q	-
⋮	⋮	⋮
33.	P	for some other reason
34.	$\leftarrow$	-
35.	$P \Leftrightarrow Q$	by $\Leftrightarrow$ + ; 1,11,12,13,33,34

□

The notation ($\Leftarrow$) and ($\Rightarrow$) are just comments to indicate to the reader that we are proving an equivalence.

Another common use of this shortcut is to eliminate the use of the *reflexivity of* = rule of inference. In particular, if we have $a = b$ and want to conclude $P(a) = P(b)$ for some expression $P(x)$ we can prove it without this shortcut like this.

⋮	⋮	⋮
11.	$a = b$	for some reason
12.	$P(a) = P(a)$	by reflexivity of =
13.	$P(a) = P(b)$	by substitution; 11, 12
⋮	⋮	⋮

But using this shortcut we can simply omit the application of reflexivity.

⋮	⋮	⋮
11.	$a = b$	for some reason

12.	$P(a) = P(b)$	by substitution; 11
⋮	⋮	⋮

6.6 Omit Most Premise Citations, Line Labels, and End-of-Subproof Symbols

A somewhat sophisticated mathematical reader who is familiar with the premises needed to justify a statement with a given reason, can simply look for the required premises in the proof. Indeed, quite frequently one or more of the premises required immediately precede the line being justified in the proof.

We can thus remove some of the clutter by omitting references to premises that are obvious and easy to find. Similarly, this reduces or eliminates the need to label or number each line in the proof.

Mathematicians do label important statements and equations in their proofs and do refer to them when justifying statements. The rule of thumb to follow when deciding whether to explicitly label or reference a particular statement in your proof is whether it makes it improves the exposition for the reader. A non-obvious, or important statement that is referred to later on as a premise should still be labeled and referenced in order to make the proof easier to follow for the reader.

In traditional mathematical writing it is also not common to indicate the end of a subproof, assumption scope, or 'Let' declaration scope with the symbol $\leftarrow$ that we have been using in our proofs. Instead, in semiformal proofs, careful indentation can be used to indicate this to the reader, and comment lines can be inserted to show the reader where the end of an assumption occurs, to make it more legible.

6.7 Eliminate Extra Parentheses for Associative Binary Operators

A special case of Shortcut 6.4 is that we can eliminate extra parentheses for associative binary operators and allow the expression represent all possible ways of including the parentheses.

For example, if we write

$$P \text{ or } Q \text{ or } R \text{ or } S$$

this expression can be identified with any of the expressions

$$P \text{ or } (Q \text{ or } (R \text{ or } S))$$
$$P \text{ or } ((Q \text{ or } R) \text{ or } S)$$
$$(P \text{ or } Q) \text{ or } (R \text{ or } S)$$
$$(P \text{ or } (Q \text{ or } R) \text{ or } S$$
$$((P \text{ or } Q) \text{ or } R) \text{ or } S$$

6.8 Combine consecutive $\forall+$ rules

Frequently we would like to use the $\forall+$ rule consecutively several times in a row. For example we might be asked to prove something like

$$\forall x, \forall y, \forall z, x = y \text{ and } y = z \Rightarrow x = z$$

A full formal proof of that might look like this:

Proof.

1.	Let x be arbitrary.	-
2.	Let y be arbitrary.	-
3.	Let z be arbitrary.	-
4.	Assume $x = y$ and $y = z$	-
5.	$x = y$	by and -; 4
6.	$y = z$	by and -; 4
7.	$x = z$	by substitution; 6,5
8.	$\leftarrow$	-
9.	$x = y$ and $y = z \Rightarrow x = z$	by $\Rightarrow$+; 4,7
10.	$\leftarrow$	-
11.	$\forall z, x = y$ and $y = z \Rightarrow x = z$	by $\forall$+; 3,9
12.	$\leftarrow$	-
13.	$\forall y, \forall z, x = y$ and $y = z \Rightarrow x = z$	by $\forall$+; 2,11
14.	$\leftarrow$	-
15.	$\forall y, \forall z, x = y$ and $y = z \Rightarrow x = z$	by $\forall$+; 1,13

□

However, no rigor would be lost if we allow the shortcut of doing all three declarations and $\forall$+ rules at the same time. Using this shortcut would simplify the proof like this.

Proof.

1.	Let x, y, z be arbitrary.	-
2.	Assume $x = y$ and $y = z$	-
3.	$x = y$	by and -; 2
4.	$y = z$	by and -; 2
5.	$x = z$	by substitution;4,3
6.	$\leftarrow$	-
7.	$x = y$ and $y = z \Rightarrow x = z$	by $\Rightarrow$+; 2,5
8.	$\leftarrow$	-
9.	$\forall x, \forall y, \forall z, x = y$ and $y = z \Rightarrow x = z$	by $\forall$+; 1,7

□

Indeed, applying several of the shortcuts above results in a much more compact semiformal proof.

Proof.

Let x, y, z be arbitrary.

Assume $x = y$ and $y = z$	
$x = z$	by substitution
$\forall x, \forall y, \forall z, x = y$ and $y = z \Rightarrow x = z$	by $\forall+$

□

6.9 Use Transitive Chains!

Let $\langle r_1, r_2, \ldots, r_n \rangle$ be a sequence of binary operators on a set A. We say such a sequence is *mutually transitive* if and only if for every $a, b, c \in A$, and for every $1 \leq i \leq j \leq n$,

$$ar_i b \text{ and } br_j c \Rightarrow ar_j c$$

and

$$ar_j b \text{ and } br_i c \Rightarrow ar_j c$$

Examples of mutually transitive operator sequences on the set of integers include: $\langle = \rangle$, $\langle =, \leq \rangle$, $\langle =, < \rangle$, $\langle =, \leq, < \rangle$, $\langle >, \geq \rangle$, $\langle =, \equiv \rangle$ and $\langle =, | \rangle$. An example of a sequence of mutually transitive logical operators is $\langle \Leftrightarrow, \Rightarrow \rangle$.

Given such a sequence we can often shorten our proofs by using the *transitive chain* notation

$$\begin{aligned} x_1 \, & r_{i_1} \, x_2 \\ & r_{i_2} \, x_3 \\ & r_{i_3} \, x_4 \\ & \vdots \\ & r_{i_k} \, x_{k+1} \end{aligned}$$

which is defined to be an abbreviation for

$$\begin{aligned} x_1 \, & r_{i_1} \, x_2 \\ x_2 \, & r_{i_2} \, x_3 \\ x_3 \, & r_{i_3} \, x_4 \\ & \vdots \\ x_k \, & r_{i_k} \, x_{k+1} \end{aligned}$$

Because the operators are mutually transitive we can use this entire block as a single premise to justify for any s, t such that $1 \leq s \leq k$ and any $s < t \leq k+1$ that $x_i r_\alpha x_j$ where α is the largest subscript among $i_s, \ldots, i_{t-1}$. As a shortcut, any such deduction can be omitted and the entire block of lines used as in its place in the proof.

Example 13. In the following transitive chain, the sequence of operators, $\langle =, \leq, < \rangle$, is mutually transitive.

$$\begin{aligned} 0 &\leq (a+1)^2 \\ &= a^2 + 2a + 1 \\ &< (a^2 + 2a + 1) + 1 \\ &= a^2 + 2(a+1) \end{aligned}$$

Thus, we can conclude from this transitive chain that $0 < a^2 + 2(a+1)$ (and other things, like $0 \leq a^2 + 2a + 1$).

6.10 Use Derived Rules of Inference

A more advanced way to avoid tedious repetitive steps of logic is to derive rules of inference from a theorem or definition. Frequently a useful rule of inference is one that eliminates as many occurrences of quantifiers and logical operators as possible.

For example, if the theorem is an implication, i.e. of the form

Theorem (some famous implication)**.** $P \Rightarrow Q$

then we can use it to justify the rule of inference $P \vdash Q$. (Can you see why?) Then instead of using the theorem directly like this

some famous implication	
$P \Rightarrow Q$	(conclude)

we obtain a new rule

some famous implication	
P	(show)
Q	(conclude)

which is frequently more useful. Similarly if a theorem is a logical equivalence, i.e. has the form

Theorem (some famous equivalence)**.** $P \Leftrightarrow Q$

then we can use it to justify two rules of inference, namely

some famous equivalence		some famous equivalence	
P	(show)	Q	(show)
Q	(conclude)	P	(conclude)

We say such rules of inference are *derived* or *expanded* from the theorem.

There are other useful ways to expand rules of inference. It is frequently useful to make the following replacements.

Deriving Rules from Definitions and Theorems

If the rule has:		*You can replace that with:*	
P and Q	(show)	P Q	(show) (show)
$P \Rightarrow Q$	(show)	Assume P Q $\leftarrow$	 (show)
$P \Leftrightarrow Q$	(show)	Assume P Q $\leftarrow$ Assume Q P $\leftarrow$	 (show) (show)
$\forall x, P(x)$	(show)	Let s be arbitrary $P(s)$ $\leftarrow$	 (show)
$P \Rightarrow Q$	(conclude)	P Q	(show) (conclude)
$P \Leftrightarrow Q$	(conclude)	P (show) Q (conclude)	Q (show) P (conclude)
P and Q	(conclude)	P Q	(conclude) (conclude)
$\forall x, P(x)$	(conclude)	$P(z)$	(conclude)
$\exists x, P(x)$	(conclude)	For some constant c, $P(c)$ *these lines must be consecutive in the proof	 (conclude)

Similarly if we have a premise P of a rule for which P is the conclusion of a previously expanded rule, we can replace that line with the premises needed to conclude P. Continuing in this way we can expand our theorems and definitions into useful rules of inference that omit unnecessary repetitive steps in our proofs.

7 The Natural Numbers

Together, the formal system that includes Propositional Logic, Predicate Logic, and Equality will be simply called *Logic*. We can extend the Logic mathematical system by adding the definition of the natural numbers.

7.1 The Peano Postulates

It is possible to define the Natural Numbers and addition, multiplication, and < for those numbers from scratch. One famous way of doing that is with the following axioms which were developed by Giuseppe Peano at the end of the 19th century.

Peano Axioms	
Axiom Name	Definition
(N0) existence of zero	0 is a *natural number* (constant declaration)
(N1) existence of successors	$\forall n, \sigma(n)$ is a *natural number*
(N2) uniqueness of predecessor	$\forall n, \forall m, \sigma(n) = \sigma(m) \Rightarrow m = n$
(N3) zero is first	$\forall n, 0 \neq \sigma(n)$
(N4) induction	$P(0)$ and $(\forall k, P(k) \Rightarrow P(\sigma(k))) \Rightarrow \forall n, P(n)$
(A0) additive identity	$\forall n, n + 0 = n$
(A1) successor addition	$\forall n, \forall m, m + \sigma(n) = \sigma(m + n)$
(M0) multiplication by zero	$\forall n, n \cdot 0 = 0$
(M1) successor multiplication	$\forall n, \forall m, m \cdot \sigma(n) = m + m \cdot n$
(I) order	$\forall n, \forall m, m \leq n \Leftrightarrow \exists k, m + k = n$

The symbols 0 and σ are constants. Zero is a constant of natural number type, and sigma is a lambda expression which returns a natural number when applied to a natural number, i.e., $\sigma(n)$ is a natural number whenever n is. In all of the axioms, the quantified variables have natural number type, so that in particular we can only apply the $\forall-$ rule for expressions which also are type natural number. In N4 above and in the rest of this chapter, $P(n)$ is a statement about a natural number variable n (i.e., P is a lambda expression that returns a statement when applied to a natural number variable n). Axiom N4 is called *mathematical induction*, or simply *induction*. While not strictly necessary, the following definitions are useful.

Definition (**base ten representation**)**.** We define the usual base ten representations of natural numbers such that $1 = \sigma(0)$, $2 = \sigma(1)$, $3 = \sigma(2)$, $4 = \sigma(3)$,. . . and so on.

7.2 Strong Induction

Another form of induction is called *strong induction*. It is stated as follows:

Theorem (Strong Induction)**.** *Let $P(n)$ be any statement about a natural number variable n. Then*

$$P(0) \text{ and } \Big(\forall k, \Big(\forall j, j \leq k \Rightarrow P(j)\Big) \Rightarrow P(\sigma(k))\Big) \Rightarrow \forall n, P(n)\,.$$

It can be shown that Strong Induction and ordinary Induction are logically equivalent. Namely, we can prove Strong Induction as a theorem in the axiom system defined above, and also if we replace the induction axiom with strong induction, we can prove ordinary induction holds as a theorem.

7.3 Number Theory

Once we have determined the basic properties that follow from our definitions, we can move on to deeper theorems that provide us with important non-obvious insights into the nature of the natural numbers. The study of such theorems is called *Number Theory*. We begin with some additional definitions. All variables are arbitrary natural numbers.

Additional Definitions for Number Theory

Name	Definition
less than	$m < n \Leftrightarrow m \leq n$ and $m \neq n$
positive	m is positive $\Leftrightarrow m \leq n$ and $m \neq n$
divides	$m \mid n \Leftrightarrow \exists k, n = m \cdot k$
not divides	$m \nmid n \Leftrightarrow \neg\exists k, n = m \cdot k$
prime	n is prime $\Leftrightarrow n > 1$ and $\neg\exists k, (1 < k < n$ and $k \mid n)$

Templates for Number Theory

We can use our shortcuts of expanding theorems and definition to derived rules of inference to make useful rules in template format for the Peano axioms and related definitions.

Peano Axioms

uniqueness of predecessor (N2)	zero is first (N3)
$\sigma(n) = \sigma(m)$ (SHOW) ..... $m = n$ (CONCLUDE)	..... $0 \neq \sigma(n)$ (CONCLUDE)
additive identity (A0)	**successor addition (A1)**
..... $n + 0 = n$ (CONCLUDE)	..... $m + \sigma(n) = \sigma(m + n)$ (CONCLUDE)
multiplication by zero (M0)	**successor multiplication (M1)**
..... $n \cdot 0 = 0$ (CONCLUDE)	..... $m \cdot \sigma(n) = m + m \cdot n$ (CONCLUDE)

Peano Axioms (cont.)

inequality+ (I)		inequality− (I)	
$\exists k, m + k = n$	(show)	$m \leq n$	(show)
.....		.....	
$m \leq n$	(conclude)	For some k, $m + k = n$	(conclude)

induction (N4)	
$P(0)$	(show)
Let k be arbitrary	(variable declaration)
Assume $P(k)$	
$P(\sigma(k))$	(show)
←	
←	
.....	
$\forall n, P(n)$	(conclude)

We also have some useful variants of induction.

Flavors of Induction

induction		strong induction	
$P(0)$	(show)	$P(0)$	(show)
Let k be arbitrary	(variable declaration)	Let k be arbitrary	(variable declaration)
Assume $P(k)$		Assume $\forall j, j \leq k \Rightarrow P(j)$	
$P(k + 1)$	(show)	$P(k + 1)$	(show)
←		←	
←		←	
.....		.....	
$\forall n, P(n)$	(conclude)	$\forall n, P(n)$	(conclude)

We can also make some useful definitions about natural numbers. Note that these rules only apply to natural numbers, i.e., the variables that appear all have natural number type.

Definitions of Number Theory

less than		less than	
$m \leq n$	(show)	$m < n$	(show)
$m \neq n$	(show)	.....	
.....		$m \leq n$	(conclude)
$m < n$	(conclude)	$m \neq n$	(conclude)

Definitions of Number Theory (cont.)

positive	positive
$0 < m$ (SHOW)	m is positive (SHOW)
m is positive (CONCLUDE)	$0 < m$ (CONCLUDE)
divides	divides
$n = m \cdot k$ (SHOW)	$m \mid n$ (SHOW)
$m \mid n$ (CONCLUDE)	For some k, (constant declaration) $n = m \cdot k$ (CONCLUDE)
not divides	not divides
$\forall k, n \neq m \cdot k$ (SHOW)	$m \nmid n$ (SHOW)
$m \nmid n$ (CONCLUDE)	$n \neq m \cdot k$ (CONCLUDE)
prime	prime
$n > 1$ (SHOW) $\neg\exists k, 1 < k < n$ and $k \mid n$	n is prime (SHOW)
n is prime (CONCLUDE)	$n > 1$ (CONCLUDE) $\neg\exists k, 1 < k < n$ and $k \mid n$ (CONCLUDE)

From now on, we will sometimes to use the usual convention of using concatenation to represent the product of two numbers, e.g., we will write mn instead of $m \cdot n$ wherever it makes sense. All variable names will be single letters.

7.4 Applications: Cardinal and Ordinal Numbers

The natural numbers have two very different but very useful applications in mathematics (and outside of mathematics in general).

On the one hand, they are useful for *counting*. For that we use natural numbers to indicate how many items are in some collection. Natural numbers used in this way are examples of *cardinal* numbers, which are used to measure the relative sizes, or *cardinality* of collections of items. The branch of mathematics that studies cardinality and counting is called *combinatorics*. We will discuss that in detail later in the course.

On the other hand, natural numbers are useful for *numbering* items to put them in some order, a first item, second item, and so on. Natural numbers used in this way are examples of *ordinal* numbers and are used to indicate the relative positions of items in an ordered list of items. Such ordered lists are called *sequences*, which we study next.

Problems

The following theorems can be proved in the order shown. Therefore, you can use an earlier theorem as a rule of inference in the proof of a later theorem but not vice versa. These should be proved with a semiformal proof using the shortcuts described in chapter 6 above.

Strong Induction

7.1. Prove that the original statement of the principle of induction is equivalent to strong induction.

Properties of the successor function

7.2. (*Nonzero implies successor*) $\forall n, n \neq 0 \Rightarrow \exists m, n = \sigma(m)$

7.3. (*No number is its own successor*) $\forall n, n \neq \sigma(n)$

Properties of addition

7.4. (*Alternate definition of σ*) $\forall m, \sigma(m) = m + 1$

7.5. (*Associativity of addition*) $\forall m, \forall n, \forall p, m + (n + p) = (m + n) + p$

7.6. (*Additive Identity*) $\forall m, 0 + m = m = m + 0$

7.7. (*Commutativity of Adding 1*) $\forall m, 1 + m = m + 1$

7.8. (*Commutativity of addition*) $\forall m, \forall n, m + n = n + m$

7.9. (*Zero sums*) $\forall m, \forall n, m + n = 0 \Rightarrow m = n = 0$

7.10. (*Cancellation Law of addition*) $\forall p, \forall m, \forall n, m + p = n + p \Rightarrow m = n$

Properties of multiplication

7.11. (*Left multiplication by 0*) $\forall m, 0 \cdot m = 0$

7.12. (*Multiplicative identity*) $\forall m, 1 \cdot m = m = m \cdot 1$

7.13. (*Left Distributive Law*) $\forall n, \forall m, \forall p, p \cdot (m + n) = p \cdot m + p \cdot n$

7.14. (*Right Distributive Law*) $\forall p, \forall n, \forall m, (m + n) \cdot p = m \cdot p + n \cdot p$

7.15. (*Commutativity of multiplication*) $\forall m, \forall n, m \cdot n = n \cdot m$

7.16. (*Associativity of multiplication*) $\forall p, \forall m, \forall n, (m \cdot n) \cdot p = m \cdot (n \cdot p)$

7.17. (*Zero divisors*) $\forall m, \forall n, m \neq 0$ and $m \cdot n = 0 \Rightarrow n = 0$

7.18. (*Cancellation Law of multiplication*) $\forall p, p \neq 0 \Rightarrow \forall m, \forall n, p \cdot m = p \cdot n \Rightarrow m = n$

Properties of order

7.19. (*Nonzero is positive*) $\forall n, 0 \leq n$ and $(0 < n \Leftrightarrow n \neq 0)$

7.20. (*Successors are bigger*) $\forall n, n < \sigma(n)$.

7.21. (*Alternate definition of $<$*) $\forall m, \forall n, m < n \Leftrightarrow \exists k, k \neq 0$ and $m + k = n$

7.22. (*Minimum difference*) $\forall m, \forall n, m < n \Leftrightarrow \sigma(m) \leq n$

7.23. (*Reflexivity of* $\leq$) $\forall n, n \leq n$

7.24. (*Antisymmetry of* $\leq$) $\forall m, \forall n, m \leq n$ and $n \leq m \Rightarrow m = n$

7.25. (*Transitivity of* $\leq$) $\forall m, \forall n, \forall p, m \leq n$ and $n \leq p \Rightarrow m \leq p$

7.26. (*Irreflexivity of* $<$) $\forall n, \neg(n < n)$

7.27. (*Transitivity of* $<$) $\forall m, \forall n, \forall p, m < n$ and $n < p \Rightarrow m < p$

7.28. (*Trichotomy*) $\forall m, \forall n, m < n$ or $m = n$ or $n < m$

7.29. (*Translation*) $\forall m, \forall n, \forall p, m < n \Leftrightarrow m + p < n + p$

This also holds if $<$ *is replaced by* $\leq$ *or if* $m + p < n + p$ *is replaced by* $p + m < p + n$.

7.30. (*Scaling*) $\forall m, \forall n, \forall p, p \neq 0 \Rightarrow (m < n \Leftrightarrow p \cdot m < p \cdot n$

This also holds if $<$ *is replaced by* $\leq$ *or if* $p \cdot m < p \cdot n$ *is replaced by*

$$m \cdot p < n \cdot p$$

Some Number Theory

7.31. (*Divisibility of differences*) $\forall b, b \neq 0 \Rightarrow \forall m, \forall n, \forall r, b \cdot m = b \cdot n + r \Rightarrow \exists p, r = b \cdot p$.

7.32. (*Division Algorithm - existence*) $\forall b, b \neq 0 \Rightarrow \forall a, \exists q, \exists r, a = b \cdot q + r$ and $0 \leq r < b$

Note that technically we do not need to state that $0 \leq r$ *since every natural number is greater than or equal to zero, but we include it here because the theorem also holds for the set of integers.*

7.33. (*Division Algorithm - Uniqueness*) For all $b \neq 0$ and all a, q, r, s, t, if

1. $a = bq + r$ and $0 \leq r < b$
2. $a = bs + t$ and $0 \leq t < b$

then $q = s$ and $r = t$.

7.34. (*Everything divides zero*) $\forall m, m \mid 0$

7.35. (*Every number divides itself*) $\forall m, 1 \mid m$ and $m \mid m$

7.36. (*Divisors are smaller*) $\forall m, \forall n, n \neq 0$ and $m \mid n \Rightarrow m \leq n$

7.37. (*Divisors divide products*) $\forall m, \forall n, \forall p, m \mid n \Rightarrow m \mid n \cdot p$

7.38. (*Common divisors divide sums*) $\forall m, \forall n, \forall p, p \mid m$ and $p \mid n \Rightarrow p \mid (m + n)$

7.39. (*Common divisors divide differences*) $\forall m, \forall n, \forall p, p \mid m$ and $p \mid m + n \Rightarrow p \mid n$

7.40. (*Divisibility is transitive*) $\forall m, \forall n, \forall p, m \mid n$ and $n \mid p \Rightarrow m \mid p$

7.41. (*Mutual divisors are equal*) $\forall m, \forall n, m \mid n$ and $n \mid m \Leftrightarrow m = n$

8 Sequences

8.1 Finite and Infinite Sequences

Just as the concept of a number is fundamental in mathematics, so is the concept of an ordered list of items. We extend the system of logic and natural numbers defined thus far by adding to it the concept of two basic kinds of ordered lists.

A *finite sequence of length n* (also called an *n-tuple*) is a numbered list of items, one for each of the natural numbers less than n. A *infinite sequence* is numbered list of items, one for each of the natural numbers. In both cases, we will refer to the number assigned to a given item in the sequence as its *standard index*. Thus, the first item in a sequence will always have a standard index of 0.

The items in a sequence are called its *terms*. The the same item can appear more than once, i.e., terms with different standard indices can be equal. Two sequences are equal if and only if all of their corresponding terms (those with the same standard index) are equal. The *length* of a finite sequence is the same as the number of terms.

One consequence of this is that every sequence that has terms must have a term with index 0 which must come before every other term in the sequence. This is called the first (1^{st}) term. Similarly if there is a term with index 1, we call it the second (2^{nd}) term, and so on with a term of index k called the $(k+1)^{\text{st}}$ term of the sequence.

Thus, every sequence that has terms has a first term. Additionally, no term of an infinite sequence can be preceded in the list by infinitely many terms. Indeed, every term has an index m and must have exactly m terms that precede it (one for each natural number less than m).

8.2 Representations of Sequences

Listing Terms

Finite sequences are frequently denoted by simply listing their terms in order from left to right separated by commas, with the whole thing enclosed in parentheses.

For example,

$$(S, E, Q, U, E, N, C, E)$$

is a sequence of length 8 whose first term is S, second term is E, and so on. These can be numbered in order from left to right with the natural numbers less than 8 as shown:

$$(\underset{0}{S}, \underset{1}{E}, \underset{2}{Q}, \underset{3}{U}, \underset{4}{E}, \underset{5}{N}, \underset{6}{C}, \underset{7}{E})$$

Infinite sequences cannot be completely denoted in this manner, but are often informally (and somewhat ambiguously) written by writing their first few terms followed by an ellipsis. For example, we might write the infinite sequence of odd natural numbers as

$$(1, 3, 5, 7, \ldots)$$

This sequence can be numbered in order with the natural numbers as indicated

$$(\underset{0}{1}, \underset{1}{3}, \underset{2}{5}, \underset{3}{7}, \ldots)$$

Infinite sequences written in this manner are ambiguous because the reader must make assumptions about what terms are omitted, and so this notation is only used informally.

A similar informal notation can be used for finite sequences when there are too many terms to conveniently list them all, by using an ellipsis in place of missing terms. For example, we might denote the sequence of even integers less than 100 as

$$(0, 2, 4, 6, \ldots, 96, 98)$$

which are indexed

$$(\underset{0}{0}, \underset{1}{2}, \underset{2}{4}, \underset{3}{6}, \ldots, \underset{48}{96}, \underset{49}{98})$$

Note that the ellipsis can represent as many terms as we like since the notation is informal. Since the sequence of length 0 has no terms, it can be denoted ( ). For sequences with one or more terms, the surrounding parentheses are frequently omitted when it is clear from the context that it is a sequence, for example,

$$S, E, Q, U, E, N, C, E$$

or

$$x_1, x_3, x_5, x_7, \ldots$$

or

$$0, 2, 4, \ldots, 96, 98$$

Lambda Expressions

Another way to represent a sequence is with a lamba expression $\lambda k, E$ where k is either a natural number or a natural number less than some natural number n. If $a = (\lambda k, E)$ is such an expression it defines a sequence such that $a(k)$ is the term of the sequence with index k.

One big advantage to this representation is that it allows us to represent infinite sequences unambiguously. It is so useful that we define several special new expressions to represent such sequences.

Notation 14. If n is a natural number and $a = (\lambda k, E)$ we define $a_k = a(k)$. We write $(a_k)_{k=0}^{\infty}$ for the infinite sequence whose term with index k is a_k. Similarly, we write $(a_k)_{k=0}^{n}$ for the finite sequence of length n whose term with index k is a_k.

Comparing this notation to the listing notation we have

$$(a_k)_{k=0}^{n} = (a_0, a_1, a_2, \ldots, a_n)$$

and

$$(a_k)_{k=0}^{\infty} = (a_0, a_1, a_2, \ldots)$$

In particular, we can express the sequence of all odd integers both rigorously and unambigously as

$$(2k + 1)_{k=0}^{\infty} = (1, 3, 5, 7, \ldots)$$

and the sequence of even numbers less than 100 as

$$(2k)_{k=0}^{49} = (0, 2, 4, \ldots, 96, 98)$$

8.3 Reindexing

In everyday use, and in mathematics in particular, we often place items in order by numbering them with consecutive natural numbers that do not necessarily start with zero. For example it is frequently natural to index the first element of sequence with 1 instead of zero so that the k^{th} term has index k.

Thus, while we always use a sequence of consecutive natural number for the indices of a sequence, it is sometimes convenient to *reindex* a sequence so that its first term has an index other than 0.

Notation 15. Let m, n be a natural numbers. Then

$$(a_k)_{k=m}^{\infty} = (a_m, a_{m+1}, a_{m+2}, \ldots) = (a_{m+k})_{k=0}^{\infty}$$

Furthermore, if $m + j = n$ then

$$(a_k)_{k=m}^{n} = (a_m, a_{m+1}, \ldots, a_n) = (a_{m+k})_{k=0}^{j}$$

Finally if $n < m$ then $(a_k)_{k=m}^{n} = (\,)$.

Reindexing and Induction

Sometimes a statement is not true for all naturals but rather is true for all sufficiently large natural numbers.

Exercise 16. Prove the following for of induction is equivalent to the original form in which we stated induction. Let a be a natural number and P be some statement about natural numbers. Then

$$(P(a) \text{ and } \forall k, k \geq a \Rightarrow (P(k) \Rightarrow P(k+1))) \Rightarrow (\forall n, n \geq a \Rightarrow P(n))$$

We can expand this to a more useful rule of inference.

Induction from a

Induction from a

$P(a)$ (SHOW)
    Let k BE ARBITRARY (variable declaration)
        Assume $k \geq a$
            ASSUME $P(k)$
            $P(k+1)$ (SHOW)
            ←
        ←
    ←
.....
$\forall n, n \geq a \Rightarrow P(n)$ (CONCLUDE)

The situation in the previous recipe comes up quite often, namely where we declare an arbitrary

variable and then immediately assume it has some property.

Notation 17 (Let-assume). We define the proof block starting with

Let $k \geq a$

to be an abbreviation for the nested blocks starting with

Let k be arbitrary
  Assume $k \geq a$

and similarly for any property of x that starts with x (so it is clear what is being declared).

8.4 Recursive Definitions and Sequences

One kind of definition that frequently goes hand-in-hand with such sequences and induction, are *recursive definitions* in which some sequence of entities is defined for some base case(s) first, and then new entities are defined in terms of previously defined objects of the same kind.

One convenient way to write such definitions is to use *cases notation*.

$$E = \begin{cases} v_1 & \text{if } P_1 \\ v_2 & \text{if } P_2 \\ \vdots & \vdots \\ v_k & \text{otherwise} \end{cases} \tag{1}$$

where E is the expression being defined, $v_1, \ldots, v_k$ are the values of the expression, and $P_1, \ldots, P_k$ are statements which specify the conditions for which E has the given values. The final condition '*otherwise*' is optional and is an abbreviation for $P_k = \neg(P_1 \text{ or } P_2 \text{ or } \cdots \text{ or } P_{k-1})$. The entire equation given in (1) is an abbreviation for the statement

$$(P_1 \Rightarrow E = v_1) \text{ and } (P_2 \Rightarrow E = v_2) \cdots (P_k \Rightarrow E = v_k)$$

Similarly, we can define sequences recursively by lambda expressions, a for which a_n is defined in terms of one or more values of a_k for $k < n$.

Here are a few common definitions related to recursively defined sequences. In the following table, a is a lambda expression which produces terms which can be any type, and k, m, n are natural numbers.

Sequences and Recursive Definitions

Name	Definition
Subscript notation:	$a_n = a(n)$
Finite Sequence:	$(a_k)_{k=0}^{n} = (a_0, a_1, \ldots, a_n)$
Reindexed Finite Sequence:	$(a_k)_{k=m}^{n+m} = (a_{k+m})_{k=0}^{n}$

Sequences and Recursive Definitions (cont.)

Name	Definition
Infinite Sequence:	$(a_k)_{k=0}^{\infty} = (a_0, a_1, a_2, \ldots)$
Reindexed Infinite Sequence:	$(a_k)_{k=m}^{\infty} = (a_{k+m})_{k=0}^{\infty}$
Summation:	$\sum_{k=0}^{0} a_k = a_0$ and $\sum_{k=0}^{n+1} a_k = a_{n+1} + \sum_{k=0}^{n} a_k$
Reindexed Summation:	$\sum_{k=m}^{m} a_k = a_m$ and $\sum_{k=m}^{n+1+m} a_k = a_{n+1+m} + \sum_{k=m}^{n+m} a_k$
Powers:	$z^0 = 1$ and $z^{n+1} = z \cdot z^n$
Factorial:	$0! = 1$ and $(n+1)! = (n+1) \cdot n!$
Fibonacci Numbers:	$F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$
Binomial coefficients (horizontal):	$\binom{n}{0} = \binom{0}{m} = 1$ and $\binom{n+1}{m+1} = \binom{n+1}{m} + \binom{n}{m+1}$
Binomial coefficients:	$\binom{n+m}{n} = \binom{n}{m}$

Remarks:

- In the definition of summation, the values of a can be natural numbers or any other type which is closed under addition, such as the real numbers in Chapter 9. In the definition of powers, z can be a natural number or any other type of expression which is closed under multiplication, such as the real numbers in Chapter 9. Fibonacci numbers, factorials, and binomial coefficients are all natural numbers.
- In the definition of the Fibonacci numbers, F is a constant, as is the ! in the definition of factorial.
- Note that $\sum$ has higher precedence than +, but lower than $\cdot$. For example,

  $$\sum_{k=0}^{n} a_k \cdot b_k + \sum_{j=0}^{m} c_j \cdot d_j$$

  means

  $$\left(\sum_{k=0}^{n} a_k \cdot b_k\right) + \left(\sum_{j=0}^{m} c_j \cdot d_j\right)$$

  Also factorial has a higher precedence that multiplication, so that e.g., $m \cdot n!$ means $m \cdot (n!)$ and not $(m \cdot n)!$

Shortcut: by arithmetic

From now on, we will allow 'by arithmetic' as a shortcut for justifying facts about natural number *constants* that could be checked on an ordinary calculator. Thus, we can justify facts like $2 + 3 = 5$ or $5 < 13$ with the reason 'by arithmetic' and no premises. This shortcut only applies to constants, not variables or expressions involving variables.

Shortcut: Given-style proofs

As we make the transition to more traditional proofs and theorem statements, we will begin to replace most of the formal symbols $\Rightarrow$, $\Leftrightarrow$, $\forall$, and $\exists$ in our theorem statements with English phrases and sentences as illustrated in the following table.

Some English Equivalents for Formal Symbols

A theorem such as...	... can be expressed
Theorem: $P \Rightarrow Q$	Theorem: *Given P. Then Q.* Theorem: *If P then Q.* Theorem: *Suppose P. Then Q.*
Theorem: $P \Leftrightarrow Q$	Theorem: *P if and only if Q.*
Theorem: $\forall n, P(n)$	Theorem: *Let n be a natural number. Then P(n).*
Theorem: $\forall n, P(n) \Rightarrow Q(n)$	Theorem: *Let n be a natural number such that P(n). Then Q(n).*
Theorem: $\exists n, P(n)$	Theorem: *There exists a natural number n such that P(n).*

In each case, since we have eliminated the corresponding formal symbol, we no longer need to end the proof with a $\forall+$ or $\Rightarrow$ + statement. Since each of these have a subproof as a premise, the proof of a theorem stated in this form need not indent the subproof and can indicate that any assumptions needed are justified by saying that they are 'given' in the reason column. We will refer to this as the *Given* style of proof.

Problems

Prove the following theorems.

8.1. The natural number $k!$ is always positive.

8.2. (*Power laws*) If m, n, w, z are natural numbers then

(a) $z^1 = z$

(b) $z^m \cdot z^n = z^{m+n}$

(c) $(z^m)^n = z^{m \cdot n}$

(d) $(w \cdot z)^n = w^n \cdot z^n$

8.3. For all natural numbers $n \geq 5$,

$$n^2 < 2^n$$

8.4. (*Basic sum properties*) Suppose n and s are natural numbers, and $(a)_{k=0}^{n}$ and $(b)_{k=0}^{n}$ are finite sequences of natural numbers. Then

(a) $\displaystyle\sum_{k=0}^{n}(a_k + b_k) = \sum_{k=0}^{n} a_k + \sum_{k=0}^{n} b_k$

(b) $\displaystyle\sum_{k=0}^{n} s \cdot a_k = s \cdot \sum_{k=0}^{n} a_k$

(c) $\displaystyle\sum_{k=0}^{n} s = (n+1) \cdot s$

8.5. Let n be a natural number. Then

$$F_{n+3} + F_n = 2 \cdot F_{n+2}$$

8.6. (*Symmetry of binomial coefficients*) For any natural numbers n and m,

$$\binom{n+m}{n} = \binom{n+m}{m}$$

.

8.7. (*Sum of the first n odd numbers*) The sum of the first n odd numbers is n^2, i.e.,

$$\sum_{k=0}^{n}(2k+1) = (n+1)^2$$

8.8. For all natural numbers $n \geq 4$,

$$2^n < n!$$

8.9. (*Gauss's Formula*) For every natural number n,

$$2 \cdot \sum_{k=0}^{n} k = n \cdot (n+1)$$

.

8.10. (*Closed formula for binomial coefficients*) For all natural numbers n and m,

$$n! \cdot m! \cdot \binom{n+m}{n} = (n+m)!$$

.

8.11. (*Transposing summations*) Given natural numbers m, n, and sequences $(a)_{k=0}^{m}$ and $(b)_{j=0}^{n}$,

$$\sum_{k=0}^{m}\sum_{j=0}^{n} a_k b_j = \sum_{j=0}^{n}\sum_{k=0}^{m} a_k b_j$$

8.12. For all natural numbers n,

$$F_{2(n+1)} = F_{n+1} \cdot (F_{n+2} + F_n)$$

8.13. Let n be a natural number. Then

$$1 + \sum_{k=0}^{n} F_k = F_{n+2}$$

8.14. (*Row sum in Pascal's triangle*) Given a natural number n,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

8.15. Define a to be the infinite sequence satisfying

$$a_0 = 1 \text{ and } a_{n+1} = a_n + 8n$$

for all natural numbers n. Then for all $n \neq 0$,

$$a_{n+1} = (2n+1)^2$$

8.16. Suppose n is a natural number. Then

$$\sum_{k=0}^{n} \binom{n}{k} \cdot F_k = F_{2n}$$

8.17. For all natural numbers n,

$$F_n < 2^n$$

8.18. If n is a natural number and $k \leq n$, then

$$(k+1) \cdot \binom{n+1}{k+1} = (n+1) \cdot \binom{n}{k}$$

8.19. For any natural number n,

$$1 + \sum_{k=0}^{n} k \cdot k! = (n+1)!$$

8.20. For any natural number n,

$$\sum_{k=0}^{n+1} k^2 \cdot (k+1)! = n \cdot (n+3)! + 2$$

8.21. (*Hockey Stick identity*) For all natural number n,

$$\sum_{k=m}^{n} \binom{k}{m} = \binom{n+1}{m+1}$$

8.22. Define a recursive sequence a such that $a_0 = 1$, $a_1 = 2$ and for all natural numbers n we have $a_{n+2} = 3 \cdot a_n + 2$ Then

$$2 \cdot a_n = 3^n + 1$$

8.23. For any natural numbers x and n,

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^k$$

9 Integer, Rational, and Real Numbers

9.1 Notation

We have defined the natural numbers via the Peano Postulates, and now would like to turn our attention to other famous sets of numbers, namely the integers, rationals, and real numbers.

Natural numbers, integers, and rational numbers all turn out to be special kinds of real numbers so it suffices to define the real numbers first, and then specify which real numbers are considered to be natural, integers, and rational numbers.

In addition to defining the real numbers themselves, we would like our real numbers to be ordered so that we can tell when one real number is less than another. If x, y are real numbers, we will write $x < y$ as usual to indicate that x is less than y.

We would also like to be able to add and multiply any two real numbers. As usual, if x, y are real numbers, we will write $x + y$ for their sum and $x \cdot y$ as their product. With this notation in hand we can now define the real numbers.

9.2 The Axioms for Real Numbers

In the following axioms, 0 and 1 are constants, the variables x, y, z, m, M are real numbers, and a is an infinite sequence of real numbers.

The Axioms for Real Numbers	
Axiom Name	Definition
Axioms of Addition	
closure of +	$x + y$ is a real number
identity of +	0 is a real number and $x + 0 = 0 + x = x$
inverse for +	^-x is a real number and $x + (^-x) = {}^-x + x = 0$

The Axioms for Real Numbers (cont.)

Axiom Name	Definition
commutativity of +	$x + y = y + x$
associativity of +	$(x + y) + z = x + (y + z)$
Axioms of Multiplication	
closure of ·	$x \cdot y$ is a real number
identity of ·	1 is a real number, $1 \neq 0$, and $1 \cdot x = x \cdot 1 = x$
inverse for ·	if $x \neq 0$ then x^- is a real number and $x \cdot x^- = x^- \cdot x = 1$
commutativity of ·	$x \cdot y = y \cdot x$
associativity of ·	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
Axioms of Order	
irreflexive	$\neg(x < x)$
transitive	$x < y$ and $y < z \Rightarrow x < z$
trichotomy	$x = y$ or $x < y$ or $y < x$
complete	*Every sequence of real numbers which has an upper bound has a least upper bound.* [6]
Axioms Relating +, ·, and <	
distributivity	$x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$
translation	$x < y \Rightarrow x + z < y + z$
product of positives	$0 < x$ and $0 < y \Rightarrow 0 < x \cdot y$

It is also helpful to make some convenient definitions. In the following definitions, let x, y, z be real numbers.

Definitions for Real Numbers

Name	Definition
$\leq$	$x \leq y \Leftrightarrow x < y$ or $x = y$
$>$	$y > x \Leftrightarrow x < y$
$\geq$	$x > y$ or $x = y$
positive	x is positive $\Leftrightarrow 0 < x$
negative	x is negative $\Leftrightarrow x < 0$
nonnegative	x is nonnegative $\Leftrightarrow 0 \leq x$
nonzero	x is nonzero $\Leftrightarrow x \neq 0$

[6] $(\exists M, \forall k, a_k \leq M) \Rightarrow (\exists m, (\forall k, a_k \leq m)$ and $\forall M, (\forall k, a_k \leq M) \Rightarrow m \leq M)$

Definitions for Real Numbers (cont.)

Name	Definition
subtraction	$x - y = x + (^{-}y)$
quotient	if $y \neq 0$ then $\frac{x}{y} = x/y = x \cdot y^{-}$
absolute value	$\lvert x \rvert = \begin{cases} x & \text{if } 0 \leq x \\ ^{-}x & \text{otherwise} \end{cases}$
distance	the distance from x to y is $\lvert x - y \rvert$
increasing	$(a_n)_{n=0}^{\infty}$ is *increasing* $\Leftrightarrow \forall k, a_k < a_{k+1}$
nondecreasing	$(a_n)_{n=0}^{\infty}$ is *nondecreasing* $\Leftrightarrow \forall k, a_k \leq a_{k+1}$
decreasing	$(a_n)_{n=0}^{\infty}$ is *decreasing* $\Leftrightarrow \forall k, a_k > a_{k+1}$
nonincreasing	$(a_n)_{n=0}^{\infty}$ is *nonincreasing* $\Leftrightarrow \forall k, a_k \geq a_{k+1}$

We also interchangeably use the abbreviations $x \not< y$, $x \nleq y$, $x \not> y$, and $x \ngeq y$ to say that x is not less than y, not less than or equal to y, not greater than y, and not greater than or equal to y respectively. As before, we will also use the shortcut of identifying the statements $x \leq y$ with $y \geq x$, and $x < y$ with $y > x$, without the need to justify it as a separate step.

9.3 Basic Properties of Real Numbers

Armed with the axioms and definitions above, we can now prove a lot of properties of real numbers.

Problems

Prove each of the following facts about the real numbers.

9.1. (*Product with zero*) $x \cdot 0 = 0 \cdot x = 0$

9.2. (*Warm up facts*) We know from the axioms that $0 \neq 1$. Now prove the following.

(a) $^{-}0 = 0$

(b) $^{-}1 \neq 1$

(c) $0 < 1$

(d) $^{-}1 \cdot {}^{-}1 = 1$

9.3. (*Cancellation for addition*) If $x + z = y + z$ then $x = y$.

9.4. (*Cancellation for multiplication*) If $z \neq 0$ and $z \cdot x = z \cdot y$ then $x = y$.

9.5. (*Additive inverses are unique*) If $z + x = 0$ and $z + y = 0$ then $x = y$.

9.6. (*Multiplicative inverses are unique*) If $z \cdot x = 1$ and $z \cdot y = 1$ then $x = y$.

9.7. (*Inverse of additive inverse*) If x is a real number then $^{-}(^{-}x) = x$.

9.8. (*Reciprocals are nonzero*) If $x \neq 0$ then $x^{-} \neq 0$.

9.9. (*Inverse of multiplicative inverse*) If x is a real number and $x \neq 0$ then $(x^{-})^{-} = x$.

9.10. (*Alternate additive inverse*) If x is a real number then $^{-}x = {}^{-}1 \cdot x$.

9.11. (*Alternate multiplicative inverse*) If x is a real number and $x \neq 0$ then $(x^{-}) = \frac{1}{x}$.

9.12. (*Generalized additive inverse*) If x, y are any real numbers then there exists a unique real number z such that $x + z = y$.

9.13. (*Generalized multiplicative inverse*) If x, y are any nonzero real numbers then there exists a unique nonzero real number z such that $x \cdot z = y$.

9.14. **Signed products** For any real numbers x, y,

$$^{-}x \cdot y = x \cdot {}^{-}y = {}^{-}(x \cdot y)$$

and

$$^{-}x \cdot {}^{-}y = x \cdot y$$

9.15. **Signed quotients** For any real numbers x, y, z

$$\frac{^{-}x}{y} = \frac{x}{^{-}y} = {}^{-}\left(\frac{x}{y}\right)$$

and

$$\frac{^{-}x}{^{-}y} = \frac{x}{y}$$

9.16. (*Trichotomy Law*) For all real numbers x, y exactly one of the following is true:

a. $x < y$
b. $x = y$
c. $y < x$

9.17. (*Asymmetry*) If $x < y$ then $y \not< x$.

9.18. (*Generalized translation*) If $w < x$ and $y < z$ then $w + y < x + z$.

9.19. (*Product of signs*) For all nonzero real numbers x, y

a. $0 < x$ and $0 < y \Rightarrow 0 < x \cdot y$
b. $x < 0$ and $y < 0 \Rightarrow 0 < x \cdot y$
c. $0 < x$ and $y < 0 \Rightarrow x \cdot y < 0$
d. $x < 0$ and $0 < y \Rightarrow x \cdot y < 0$

9.20. (*Inverses are opposite*) $(^{-}x < 0 \Leftrightarrow 0 < x)$ and $(x < 0 \Leftrightarrow 0 < {}^{-}x)$

9.21. (*Negating an inequality*) $x < y$ if and only if $^{-}y < {}^{-}x$.

9.22. (*Scaling by a positive*) If $0 < z$ and $x < y$ then $z \cdot x < z \cdot y$.

9.23. (*Scaling by a negative*) If $z < 0$ and $x < y$ then $z \cdot y < z \cdot x$.

9.24. (*Properties of* $\leq$) For all real numbers x, y, z,

a. **connexive** $x \le y$ or $y \le x$
b. **antisymmetric** $x \le y$ and $y \le x \Rightarrow x = y$
c. **transitive** $x \le y$ and $y \le z \Rightarrow x \le z$
d. **negating** If $x \le y$ then $^-y \le {}^-x$.
e. **multiplying by a positive** If $0 \le z$ and $x < y$ then $z \cdot x < z \cdot y$.
f. **multiplying by a negative** If $z < 0$ and $x < y$ then $z \cdot y < z \cdot x$.

9.25. (*Squares are nonnegative*) If x is a real number then $0 \le x^2$.

9.26. (*Zero divisors*) If $x \cdot y = 0$ then $x = 0$ or $y = 0$.

9.27. (*Difference of two squares*) Let x, y be real numbers. Then

$$x^2 - y^2 = (x + y) \cdot (x - y)$$

9.4 Integers

Every natural number can be considered to be a real number. To see this, define the successor $\sigma(x)$ of a real number x to be the real number $x + 1$ and recursively define the sequence $(N_k)_{k=0}^{\infty}$ by

$$N_0 = 0 \text{ and } N_{k+1} = \sigma(N_k)$$

It can be shown that the terms of N, σ, 0, +, $\cdot$, and $\le$ satisfy the Peano Axioms (see problem #9.32 below). Therefore, anything we can prove about the natural numbers is true about the real numbers of the form N_k for some natural number k. This prompts the following new (but equivalent) definition of the natural numbers as a collection of certain real numbers.

Definition (**Natural Numbers**)**.** A real number n is said to be a *natural number* if and only if $n = N_k$ for some (Peano) natural number k.

Notice that the natural number we called 1 is $\sigma(N_0) = 0 + 1 = 1$ in the reals. So both 0 and 1 in the reals correspond to what we refer to as 0 and 1 in natural numbers. Similarly, we can refer to the rest of the natural numbers in the reals as we did before, namely $N_0 = 0$, $\sigma(0) = 1$, $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 4$, and so on.

But there are many more real numbers than just the natural numbers. For example, there is no natural number that when added to 2 gives 1. But there is such a real number. This allows us to define the integers.

Definition (**Integers**)**.** A real number is an *integer* if and only if it is either (a) a natural number or (b) the additive inverse of a natural number.

These are the ordinary integers that we have all come to know and love. But there are many more real numbers besides the integers. For example, there is no integer that you can multiply by 5 to get 3. But there is such a real number. This allows us to define the rational numbers.

Definition (**Rational Numbers**)**.** A real number is *rational* if and only if some integer multiple of it is an integer, i.e., a real number r is rational if and only if there is some nonzero integer m such that $r \cdot m$ is an integer.

Indeed, in this definition if we define $k = r \cdot m$ then we can show that $r = \frac{k}{m}$, i.e., the quotient of two integers. Thus, once again, the rational numbers are the familiar quotients of integers we all know and love.

Problems

Prove each of the following facts about the real numbers.

9.28. (*Unnatural integers*) There exist integers which are not natural numbers.

9.29. (*Additive inverses in the integers*) For every integer m there exists a unique integer n such that $m + n = n + m = 0$.

9.30. (*Closure in the integers*) For any integers m, n both $m + n$, $m - n$, and $m \cdot n$ are integers.

9.31. (*Closure in the rationals*) For any rational numbers m, n, both $m + n$ and $m \cdot n$ are also rational number. Furthermore, if $n \neq 0$ then $\frac{m}{n}$ is also a rational number.

9.32. (*Every natural is real*) The terms of the sequence N, 0, $+$, $\cdot$, $<$ and σ together satisfy the Peano Axioms.

9.33. (*Every natural is an integer*) Every natural number is also an integer.

9.34. (*Every integer is rational*) Every integer is also a rational number.

9.35. (*Alternate definition of rational*) A real number r is rational if and only if for some integer m and some nonzero integer n,

$$r = \frac{m}{n}$$

9.36. (*Equivalent fractions*) If k, m, n are nonzero integers, the

$$\frac{k \cdot m}{k \cdot n} = \frac{m}{n}$$

9.37. (*No gaps*) There is a rational number strictly between any two distinct rational numbers, i.e., if s, t are rational number with $s < t$ then there exists a rational number r such that

$$s < r < t$$

9.38. (*Completeness for lower bounds*) Every infinite sequence of real numbers that has a lower bound has a greatest lower bound.

9.39. (*Existence of floor and cieling*) For every real number x there are unique integers m and M such that $m \leq x \leq M$.

9.5 Extending Definitions

Having developed the real numbers, we can extend many of the definitions about natural numbers to integers, and many of the definitions about sequences to apply to reals as mentioned in Chapter 8. In particular, the definitions of summation and powers extend to sums and products of integers, rational and real numbers. We can also extend the definition of powers to include negative integer exponents.

Definition (negative integer exponents)**.** If z is a real number and n is a natural number then

$$z^{-n} = (z^n)^-$$

Many of the definitions for natural numbers can be extended to include all integers, along with adding some new definitions that apply to integers only. In the following, all single letter variables have type integer unless otherwise specified.

Extended Definitions for Integers

Name	Definition
Division Algorithm[7]	$\forall a, \forall b > 0, \exists! q, \exists! r, a = qb + r$ and $0 \leq r < b$
Quotient	$\forall a, \forall b \neq 0, \forall q, \forall r, a = qb + r$ and $0 \leq r < b \Leftrightarrow q = (a \operatorname{quo} b)$
Remainder	$\forall a, \forall b \neq 0, \forall q, \forall r, a = qb + r$ and $0 \leq r < b \Leftrightarrow r = (a \bmod b)$
Divides	$\forall a, b, a \mid b \Leftrightarrow \exists q, b = a \cdot q$
Divisor (or factor)	a is a divisor (or factor) of $b \Leftrightarrow a \mid b$
Even	a is even $\Leftrightarrow 2 \mid a$
Odd	a is odd $\Leftrightarrow a$ is not even
Prime	p is prime $\Leftrightarrow |p| > 1$ and $\forall a, a \mid p \Rightarrow |a| = 1$ or $|a| = |p|$
Composite	n is composite $\Leftrightarrow \exists a, a \mid n$ and $1 < a < |n|$
Greatest Common Divisor	$d = \gcd(a, b) \Leftrightarrow$ $d > 0$ and $d \mid a$ and $d \mid b$ and $\forall c > 0, c \mid a$ and $c \mid b \Rightarrow c \leq d$
Least Common Multiple	$d = \operatorname{lcm}(a, b) \Leftrightarrow$ $d > 0$ and $a \mid d$ and $b \mid d$ and $\forall c > 0, a \mid c$ and $b \mid c \Rightarrow d \leq c$
GCD (alt version)	$d = \gcd(a, b) \Leftrightarrow$ $d > 0$ and $d \mid a$ and $d \mid b$ and $\forall c > 0, c \mid a$ and $c \mid b \Rightarrow c \mid d$
LCM (alt version)	$d = \operatorname{lcm}(a, b) \Leftrightarrow$ $d > 0$ and $a \mid d$ and $b \mid d$ and $\forall c > 0, a \mid c$ and $b \mid c \Rightarrow d \mid c$
Relatively Prime	a, b are relatively prime $\Leftrightarrow \gcd(a, b) = 1$
Congruent mod m	$\forall m, \forall a, b, a \underset{m}{\equiv} b \Leftrightarrow m \mid (a - b)$

Remarks: It is also commonplace to require that prime numbers and composite numbers be positive.

9.40. (*ninety one*) The natural number 91 is not prime.

9.41. (*perfect squares mod* 8) Any integer that is a perfect square has a remainder of 0, 1, or 4 when divided by 8. Note that an integer is a perfect square if and only if it is equal to the square of some integer.

9.42. (*same gcd*) If a and b are integers then $\gcd(a, b) = \gcd(a, a + b)$.

[7] this one is actually a theorem

9.43. (*consecutives are relatively prime*) The greatest common divisor of two consecutive integers is 1.

9.44. (*binary fun*) Define a sequence of natural numbers by $a_0 = 1$ and for all natural numbers n,

$$a_{n+1} = 2 \cdot a_n + 1$$

Then for all natural numbers n, we have $a_n = 2^{n+1} - 1$.

9.45. (*somewhat odd*) Let a be a sequence of natural numbers such that $a_0 = 1$, $a_1 = 3$, and for all natural numbers n,

$$a_{n+2} = 2 \cdot a_{n+1} - a_n$$

Then for all natural numbers n,

$$a_n = 2 \cdot n + 1$$

9.46. (*interesting multiples of* 25) For all $n \in \mathbb{N}$, the number $6^n - 5 \cdot n - 1$ is divisible by 25.

9.6 Infinite Series and Decimal Representation

As we have seen above, natural numbers can be expressed in the form $0, 1, 2, 3, \ldots$. Similiarly, integers can be expressed as $\ldots, {}^-3, {}^-2, {}^-1, 0, 1, 2, 3, \ldots$. As seen above, the rational numbers can all be represented as quotients of integers. But what about arbitrary real numbers?

For these we have their *decimal* or *base ten* representations. These can be defined in terms as a special kind of *infinite series*.

Definition 18. Let $(a)_{k=0}^{\infty}$ be a sequence of nonnegative real numbers such that the sequence of *partial sums*

$$\left(\sum_{k=0}^{n} a_k\right)_{n=0}^{\infty} = a_0,\ a_0 + a_1,\ a_0 + a_1 + a_2,\ \ldots$$

is bounded above. For such sequences we define the *infinite series*

$$\sum_{n=0}^{\infty} a_k$$

to be the least upper bound of the sequence of partial sums.

This allows us to define the decimal representation of any real number.

Definition 19. Let x be a nonnegative real number. A *digit* is one of the numbers $0, 1, 2, \ldots, 9$. If $(d_{n-k})_{k=0}^{\infty}$ is a sequence of digits such that

$$x = \Sigma_{k=0}^{\infty} d_{n-k} \cdot 10^{n-k}$$

then the expression

$$d_n d_{n-1} \cdots d_0 . d_{-1} d_{-2} d_{-3} \cdots$$

is called a *decimal representation* of x. In this situation a decimal representation of ${}^-x$ is just

$${}^-d_n d_{n-1} \cdots d_0 . d_{-1} d_{-2} d_{-3} \cdots$$

Problems

Prove the following theorems about the real numbers.

9.47. (*Finite Geometric Series*) For every natural number n and every real number r other than 1,

$$\sum_{k=0}^{n} r^k = \frac{1 - r^{n+1}}{1 - r}$$

9.48. (*Geometric Series*) For every every real number r, if $^-1 < r < 1$ then

$$\sum_{k=0}^{\infty} r^k = \frac{1}{1 - r}$$

9.49. (*One third*) The decimal representation of $\frac{1}{3}$ is 0.333333..., i.e., $d_0 = 0$ and $d_k = 3$ for all negative integers k.

9.50. (*Decimal representation of rationals*) We say a decimal representation

$$d_n d_{n-1} \cdots d_0 . d_{^-1} d_{^-2} d_{^-3} \cdots$$

(or its additive inverse) is *eventually repeating* if there exists positive integers k and p such that for all j greater than k, $d_{^-j} = d_{^-(j+p)}$. The decimal representation of a real number x is eventually repeating if and only if x is a rational number.

10 Sets, Functions, Numbers

10.1 Basic Definitions from Set theory

We can extend the language of mathematics we have developed thus far by including a new constant $\in$ which is called "is an element of" (or "is a member of" or "is in") and a new variable and constant type called a 'set'. The expression $x \in A$ is a statement is read "x is an element of A" where A has type 'set' and x can have any type. The constant $\emptyset$ is a set called the empty set. Many of the definitions below are informal definitions that are sufficient for our purposes.

Basic Set Notation and Operations

Name	Definition
Finite set notation	$x \in \{ x_1, \ldots, x_n \} \Leftrightarrow x = x_1$ or $\cdots$ or $x = x_n$
Set builder notation	$x \in \{ y : P(y) \} \Leftrightarrow P(x)$
Subset	$A \subseteq B \Leftrightarrow \forall x, x \in A \Rightarrow x \in B$
Set equality	$A = B \Leftrightarrow A \subseteq B$ and $B \subseteq A$
Def. of $\notin$	$x \notin A \Leftrightarrow \neg (x \in A)$

Basic Set Notation and Operations (cont.)

Name	Definition
Empty set	$A = \emptyset \Leftrightarrow \forall x, x \notin A$
Power set	$\mathcal{P}(A) = \{ B : B \subseteq A \}$
Intersection	$x \in A \cap B \Leftrightarrow x \in A$ and $x \in B$
Union	$x \in A \cup B \Leftrightarrow x \in A$ or $x \in B$
Relative Complement	$x \in B - A \Leftrightarrow x \in B$ and $x \notin A$
Complement	$x \in A' \Leftrightarrow x \notin A$
Indexed Intersection	$x \in \bigcap_{i \in I} A_i \Leftrightarrow \forall i, i \in I \Rightarrow x \in A_i$
Indexed Union	$x \in \bigcup_{i \in I} A_i \Leftrightarrow \exists i, i \in I$ and $x \in A_i$
Two convenient abbreviations	$(\forall x \in A, P(x)) \Leftrightarrow \forall x, x \in A \Rightarrow P(x)$ $(\exists x \in A, P(x)) \Leftrightarrow \exists x, x \in A$ and $P(x)$
Ordered Pairs	$(x, y) = (u, v) \Leftrightarrow x = u$ and $y = v$
Ordered n-tuple	$(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \Leftrightarrow x_1 = y_1$ and $\cdots$ and $x_n = y_n$
Cartesian Product	$A \times B = \{ (x, y) : x \in A$ and $y \in B \}$
Cartesian Product	$A_1 \times \cdots \times A_n = \{ (x_1, \ldots, x_n) : x_1 \in A_1$ and $\cdots$ and $x_n \in A_n \}$
Power of a Set	$A^n = A \times A \times \cdots \times A$ where there are n "A's" in the Cartesian product

Remarks:

- set complement has a higher precedence than all other set operations, so that, e.g., $A \cap B'$ means $A \cap (B')$ and not $(A \cap B)'$.
- An n-tuple is just another name for a finite sequence of length n.

As usual, in addition to using the above definitions in our proofs, we can also derive many useful rules of inference from them.

Basic Set Theory

Finite set notation+		Finite set notation−	
$x = a_1$ or $x = a_2$ or $\cdots$ or $x = a_n$	(SHOW)	$x \in \{ a_1, \ldots, a_n \}$	(SHOW)
$x \in \{ a_1, \ldots, a_n \}$	(CONCLUDE)	$x = a_1$ or $x = a_2$ or $\cdots$ or $x = a_n$	(CONCLUDE)

Basic Set Theory (cont.)

Set builder+		Set builder−	
$P(x)$	(show)	$x \in \{ y : P(y) \}$	(show)
.....		.....	
$x \in \{ y : P(y) \}$	(conclude)	$P(x)$	(conclude)

Subset+		Subset−	
Let $x \in A$	(variable declaration)	$A \subseteq B$	(show)
$x \in B$	(show)	$x \in A$	(show)
$\leftarrow$		.....	
.....		$x \in B$	(conclude)
$A \subseteq B$	(conclude)		

Set equality+		Set equality−
Let $x \in A$	(variable declaration)	(see Substitution)
$x \in B$	(show)	
$\leftarrow$		
Let $x \in B$	(variable declaration)	
$x \in A$	(show)	
$\leftarrow$		
.....		
$A = B$	(conclude)	

Empty Set+		Empty Set−	
Let x	(variable declaration)	.....	
$x \notin A$	(show)	$x \notin \emptyset$	(conclude)
$\leftarrow$			
.....			
$A = \emptyset$	(conclude)		

Power Set+		Power Set−	
$B \subseteq A$	(show)	$B \in \mathcal{P}(A)$	(show)
.....		.....	
$B \in \mathcal{P}(A)$	(conclude)	$B \subseteq A$	(conclude)

Intersection+		Intersection−	
$x \in A$	(show)	$x \in A \cap B$	(show)
$x \in B$	(show)	.....	
.....		$x \in A$	(conclude)
$x \in A \cap B$	(conclude)	$x \in B$	(conclude)

Basic Set Theory (cont.)

Union+

$x \in A$ (show)

$x \in A \cup B$ (conclude)

$x \in B \cup A$ (conclude)

Union−

$x \in A \cup B$ (show)

$x \in A$ or $x \in B$ (conclude)

Relative Complement+

$x \in B$ (show)

$x \notin A$ (show)

$x \in B - A$ (conclude)

Relative Complement−

$x \in B - A$ (show)

$x \in B$ (conclude)

$x \notin A$ (conclude)

Complement+

$x \notin A$ (show)

$x \in A'$ (conclude)

Complement−

$x \in A'$ (show)

$x \notin A$ (conclude)

Indexed Intersection+

Let $k \in I$ (variable declaration)

$x \in A_k$ (show)

$\leftarrow$

$x \in \bigcap_{i \in I} A_i$ (conclude)

Indexed Intersection−

$x \in \bigcap_{i \in I} A_i$ (show)

$k \in I$ (show)

$x \in A_k$ (conclude)

Indexed Union+

$\exists k \in I, x \in A_k$ (show)

$x \in \bigcup_{i \in I} A_i$ (conclude)

Indexed Union−

$x \in \bigcup_{i \in I} A_i$ (show)

For some $k \in I$, (constant declaration)

$x \in A_k$ (conclude)

Ordered pair+

$x = u$ (show)

$y = v$ (show)

$(x, y) = (u, v)$ (conclude)

Ordered pair−

$(x, y) = (u, v)$ (show)

$x = u$ (conclude)

$y = v$ (conclude)

Ordered n-tuple+

Let $k \in \{1, 2, \ldots, n\}$ (variable declaration)

$x_k = y_k$ (show)

$\leftarrow$

$(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ (conclude)

Ordered n-tuple−

$(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ (show)

$k \in \{1, 2, \ldots, n\}$ (show)

$x_k = y_k$ (conclude)

Basic Set Theory (cont.)

Cartesian Product+	Cartesian Product−
$x \in A$ (SHOW) $y \in B$ (SHOW) …… $(x, y) \in A \times B$ (CONCLUDE)	$z \in A \times B$ (SHOW) …… For some $x \in A$ and some $y \in B$, (constant declaration) $z = (x, y)$ (CONCLUDE)
Cartesian Product+(n sets)	**Cartesian Product−(n sets)**
Let $k \in \{1, 2, \ldots, n\}$ (variable declaration) $x_k \in A_k$ (SHOW) ← …… $(x_1, \ldots, x_n) \in A_1 \times A_2 \times \cdots \times A_n$ (CONCLUDE)	$z \in A_1 \times A_2 \times \cdots \times A_n$ (SHOW) …… For some $x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n$, (constant declaration) $z = (x_1, \ldots, x_n)$ (CONCLUDE)
Power of a set+	**Power of a Set−**
Let $k \in \{1, 2, \ldots, n\}$ (variable declaration) $x_k \in A$ (SHOW) ← …… $(x_1, \ldots, x_n) \in A^n$ (CONCLUDE)	$z \in A^n$ (CONCLUDE) …… For some $x_1, \ldots, x_n \in A_n$, (constant declaration) $z = (x_1, \ldots, x_n)$ (CONCLUDE)

Remarks:

- The expression "*Let $x \in A$*" is an abbreviation for "*Let x be arbitrary. Assume $x \in A$.*". Thus, there is a hidden assumption to keep track of when using this shortcut. Rules of inference treat these nested subproofs as a single subproof block. See below.
- As usual, we will just use $x \notin A$ and not $x \in A$ interchangeably in our proofs without invoking separate "Not an element of" rules.
- The expression "For some $x \in A$ and $y \in B$" is an abbreviation for two applications of the $\exists-$ rule, namely it is declaring two constants x, y and further declaring that they are elements of set A and set B respectively.

10.2 Shortcuts involving sets

10.2.1 Use Typed Declarations

We define "Let $x \in A$" to be an abbreviation for:

Let x be arbitrary.
Assume $x \in A$

Notice that this destroys our careful indentations because there is a hidden assumption in the statement. Usually this is not a problem.

We also define "$\forall x \in A, P(x)$" as an abbreviation for "$\forall x, x \in A \Rightarrow P(x)$" and "$\exists x \in A, P(x)$" as an abbreviation for "$\exists x, x \in A$ and $P(x)$". Once again, these are used interchangeably in the proof, i.e. treated as if they are the same statement. Thus there is no need to convert form one form to the other. We can think of this as declaring the type of the bound variable in the quantifier in each case.

Thus, in particular if you have the statement $\exists x \in A, P(x)$ in your proof, you can apply the $\exists-$ rule directly as shown.

	⋮	⋮
5.	$\exists x \in A, P(x)$	`for some reason`
6.	`For some` $c \in A$	-
7.	$P(c)$	`by` $\exists-$ `;` 5
	⋮	⋮

which in turn is equivalent to

	⋮	⋮
5.	$\exists x \in A, P(x)$	`for some reason`
6.	`For some` c	-
7.	$c \in A$ and $P(c)$	`by` $\exists-$ `;` 5
	⋮	⋮

Note that a line such as "For some $c \in A$ is both a statement and a constant declaration.

This idea can be extended to other predicates after the quantifier, i.e., "$\forall Q(x), P(x)$" as an abbreviation for "$\forall x, Q(x) \Rightarrow P(x)$" and "$\exists Q(x), P(x)$" as an abbreviation for "$\exists x, Q(x)$ and $P(x)$". For example, we might say something like $\forall f : A \to B, \forall x \in A, f(x) = 1$. (For what set B would this be true?)

Finally, we often combine multiple quantifiers into one by defining "$\forall x_0, \ldots, x_n, P(x_0, \ldots, x_n)$" as an abbreviation for "$\forall x_0, \forall x_1, \cdots \forall x_n, P(x_0, \ldots, x_n)$" and "$\exists x_0, \ldots, x_n, P(x_0, \ldots, x_n)$" as an abbreviation for "$\exists x_0, \exists x_1, \ldots \exists x_n, P(x_0, \ldots, x_n)$".

10.2.2 Use Extended Set-Builder Notation

In addition to set builder notation, $\{ x : P(x) \}$ where P is a predicate, it is quite common practice in mathematics to write sets in the form

$$\{ E(x_0, \ldots, x_n) : P(x_0, \ldots, x_n) \}$$

where $E(x_0, \ldots, x_n)$ is an expression containing the free variables $x_0, \ldots, x_n$ and P is a predicate. This is defined to be a shorthand for

$$\{ x : \exists x_0, \ldots, x_n, x = E(x_0, \ldots, x_n) \text{ and } P(x_0, \ldots, x_n) \}.$$

Example 20. When we write

$$\mathbb{C} = \{ a + bi : a, b \in \mathbb{R} \}$$

this is an abbreviation for

$$\mathbb{C} = \{ x : \exists a, b, x = a + bi \text{ and } a, b \in \mathbb{R} \}$$

or equivalently

$$\mathbb{C} = \{ x : \exists a, b \in \mathbb{R}, x = a + bi \}$$

Thus, if you need to pick an arbitrary element of $\mathbb{C}$ in your proof you should do it like this:

	⋮	⋮
5.	$\mathbb{C} = \{ a + bi : a, b \in \mathbb{R} \}$	`given`
6.	`Let` $z \in \mathbb{C}$	-
7.	`For some` $a, b \in \mathbb{R}$	-
8.	$z = a + bi$	`by the definition of` $\mathbb{C}$`;5,6`
	⋮	⋮

10.3 Famous Sets of Numbers

We can now define constants to represent sets containing all numbers of a certain type.

Famous Sets of Numbers

Name	Notation
The Natural Numbers	$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$
The Integers	$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
The Rational Numbers	$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$
The Real Numbers	$\mathbb{R} = \{ x : x \text{ can be expressed as a decimal number} \}$
The Complex Numbers	$\mathbb{C} = \{ x + yi : x, y \in \mathbb{R} \}$ where $i^2 = -1$
The positive real numbers	$\mathbb{R}^+ = \{ x : x \in \mathbb{R} \text{ and } x > 0 \}$
The negative real numbers	$\mathbb{R}^- = \{ x : x \in \mathbb{R} \text{ and } x < 0 \}$
The positive reals in a set A	$A^+ = A \cap \mathbb{R}^+$

Famous Sets of Numbers (cont.)

Name	Notation
The negative reals in a set A	$A^- = A \cap \mathbb{R}^-$
The first n positive integers	$\mathbb{I}_n = \{1, 2, \ldots, n\}$
The first $n+1$ natural numbers	$\mathbb{O}_n = \{0, 1, 2, \ldots, n\}$

Remarks: The sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all closed under addition and multiplication, and all except $\mathbb{N}$ are closed under subtraction (i.e., there is an additive inverse for every number). Thus, for example, if you know that $a, b \in \mathbb{C}$ you can say that $a \cdot b \in \mathbb{C}$ by closure of multiplication. All of the nonzero numbers in $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are *invertible*, i.e., they have a reciprocal.

Problems

In the following problems, capital letters represent sets which are all subsets of a universal set $\mathcal{U}$.

10.1. (*easy warmup*) If $x \in \{a\}$ and $y \in \{a\}$ then $x = y$

10.2. (*Order doesn't matter*) $\{a, b\} = \{b, a\}$

10.3. (*Order does matter*) $(a, b) = (b, a)$ if and only if $a = b$

10.4. (*excluded middle*) $x \in A \cup A'$

10.5. (*double negative*) $A'' = A$

10.6. (*ordered pair inequality*) $x \neq y$ if and only if $(x, y) \neq (y, x)$

10.7. (*A set of sets*) $\{1, 2\} \in \{A : \{1\} \subseteq A\}$

10.8. (*Cartesian calculation*) $\{2\} \times \{3, 5\} = \{(2, 3), (2, 5)\}$

10.9. (*Subset is reflexive*) $A \subseteq A$

10.10. (*alternate definition of subset*) $A \subseteq B$ if and only if for all x, either $x \notin A$ or $x \in B$

10.11. (*Transitivity of $\subseteq$*) $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$

10.12. (*Not a subset*) $\neg(A \subseteq B)$ if and only if $\exists x, x \in A \cap B'$

10.13. (*Double negative*) $A - (B - A) = A$

10.14. (*Substraction lessens*) $A - B \subseteq A$

10.15. (*Contravariance of complement*) $A \subseteq B \Leftrightarrow B' \subseteq A'$

10.16. (*Idempotency of $\cap$*) $A \cap A = A$

10.17. (*Idempotency of $\cup$*) $A \cup A = A$

10.18. (*Commutativity of $\cap$*) $A \cap B = B \cap A$

10.19. (*Commutativity of* $\cup$) $A \cup B = B \cup A$

10.20. (*Associativity of* $\cap$) $(A \cap B) \cap C = A \cap (B \cap C)$

10.21. (*Associativity of* $\cup$) $(A \cup B) \cup C = A \cup (B \cup C)$

10.22. (*Relative complement is not associative*) If $x \in A \cap B \cap C$ then $x \in A - (B - C)$ and $x \notin (A - B) - C$.

10.23. (*Distributivity of* $\cap$ *over* $\cup$) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C))$

10.24. (*Distributivity of* $\cup$ *over* $\cap$) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C))$

10.25. (*DeMorgan*) $(A \cap B)' = A' \cup B'$

10.26. (*DeMorgan*) $(A \cup B)' = A' \cap B'$

10.27. (*More DeMorgan*) $A - (B \cap C) = (A - B) \cup (A - C)$

10.28. (*More DeMorgan*) $A - (B \cup C) = (A - B) \cap (A - C)$

10.29. (*Even more DeMorgan*) $\left(\bigcap_{i \in I} A_i\right)' = \bigcup_{j \in I} A'_j$

10.30. (*Even more DeMorgan*) $\left(\bigcup_{i \in I} A_i\right)' = \bigcap_{j \in I} A'_j$

10.31. (*Not a subset*) $\neg(A \subseteq B) \Leftrightarrow \exists x, x \in A \cap B'$

10.32. (*Always in the power set*) $\emptyset \in \mathcal{P}(A)$

10.33. (*Always in the power set*) $A \in \mathcal{P}(A)$

10.34. (*Power sets of subsets*) $A \subseteq B \Rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$

10.35. (*Power sets of complements*) $A \subseteq B \Rightarrow \mathcal{P}(B') \subseteq \mathcal{P}(A')$

10.36. (*Subsets are contagious*) $A \subseteq C$ and $B \subseteq D \Rightarrow A \times B \subseteq C \times D$

10.37. (*Alternate definition of subset*) $A \subseteq B$ if and only if $\forall x, x \notin A$ or $x \in B$

10.38. (*Relative complement is not associative*) If $x \in A \cap B \cap C$ then $x \in A - (B - C)$ and $x \notin (A - B) - C$

10.39. (*Powerset and union*) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$

10.4 Functions

In the following definitions, A,B,C,S are sets and f, g, h are the lambda expressions in an ordered triple that is a function. We write $\lambda x : A, E : B$ to denote a lambda expression whose bound variable x has type 'element of A' for which E evaluates to an expression of type 'element of B' whenever the lambda expression is applied to an element of A.

Functions	
Name	Definition
Def of function:	(f, A, B) is a function $\Leftrightarrow f = \lambda x : A, E : B$ and $\forall a \in A, f(a) \in B$
Mapping notation:	$f : A \to B \Leftrightarrow (f, A, B)$ is a function
Graph of a function:	$f : A \to B \Rightarrow \mathcal{G}_f = \{ (x, y) \in A \times B : y = f(x) \}$
Alt. function notation	$X \xrightarrow{f} Y \Leftrightarrow f : X \to Y$
Alt. def of $f(x)$:	$f(x) = y \Leftrightarrow (x, y) \in f$
Domain & Codomain:	$\text{Domain}(f) = A$ and $\text{Codomain}(f) = B \Leftrightarrow f : A \Rightarrow B$
Image (of a subset of the domain):	$y \in f(S) \Leftrightarrow \exists x \in S, y = f(x)$
Range (or Image of f):	$\text{Range}(f) = f(\text{Domain}(f))$
Identity Map:	$\text{id}_A : A \to A$ and $\forall x, \text{id}_A(x) = x$
Composition:	$A \xrightarrow{f} B$ and $B \xrightarrow{g} C \Rightarrow A \xrightarrow{g \circ f} C$ and $\forall x, (g \circ f)(x) = g(f(x))$
Injective (one-to-one):	f is injective $\Leftrightarrow \forall x, \forall y, f(x) = f(y) \Rightarrow x = y$
Surjective (onto):	f is surjective $\Leftrightarrow \forall y, \exists x, y = f(x)$
Bijective:	f is bijective $\Leftrightarrow f$ is injective and f is surjective
Inverse:	$f^{-1} : B \to A \Leftrightarrow f : A \to B$ and $f \circ f^{-1} = \text{id}_B$ and $f^{-1} \circ f = \text{id}_A$
Inverse Image:	$f : A \to B$ and $S \subseteq B \Rightarrow f^{\text{inv}}(S) = \{ x \in A : f(x) \in S \}$

When deriving rules of inference from these definitions, it is helpful to note the following important theorem about inverse functions and bijections.

Theorem. *A function has an inverse function if and only if it is bijective.*

Functions	
Mapping notation+	Mapping notation−
(f, A, B) is a function (SHOW)	$f : A \to B$ (SHOW)
$f : A \to B$ (CONCLUDE)	(f, A, B) is a function (CONCLUDE)

Functions (cont.)

Function+

$f = \lambda x : A, E(x) : B$ (show)
  Let $a \in A$ (variable declaration)
  $f(a) \in B$ (show)
  ←
……
$f : A \to B$ (conclude)

Function−

$f : A \to B$ (show)
$a \in A$ (show)
……
$f(a) \in B$ (conclude)

Graph of a function+

$\mathcal{G} \subseteq A \times B$ (show)
  Let $x \in A$ (variable declaration)
  $\exists! y \in B, (x, y) \in \mathcal{G}$ (show)
  ←
……
For some $f : A \to B$, (constant declaration)
$\mathcal{G} = \mathcal{G}_f$ (conclude)

Graph of a function−

$f : A \to B$ (show)
$z \in G_f$ (show)
……
For some $x \in A$, (constant declaration)
$z = (x, f(x))$ (conclude)

Alternate function application+

$f : A \to B$ (show)
$(x, y) \in \mathcal{G}_f$ (show)
……
$f(x) = y$ (conclude)

Alternate function application−

$f : A \to B$ (show)
$y = f(x)$ (show)
……
$(x, y) \in \mathcal{G}_f$ (conclude)

Domain and Codomain+

$f : A \to B$ (show)
……
Domain $(f) = A$ (conclude)
Codomain $(f) = B$ (conclude)

Domain and Codomain−

Domain $(f) = A$ (show)
Codomain $(f) = B$ (show)
……
$f : A \to B$ (conclude)

Function equality+

$f : A \to B$ (show)
$g : A \to B$ (show)
  Let $x \in A$ (variable declaration)
  $f(x) = g(x)$ (show)
  ←
……
$f = g$ (conclude)

Function equality−

(see Substitution Rule)

Functions (cont.)

Image+

$\exists x \in S, y = f(x)$ (show)

$y \in f(S)$ (conclude)

Image−

$y \in f(S)$ (show)

For some $x \in S$, (constant declaration)
$y = f(x)$ (conclude)

Range+

$y = f(x)$ (show)

$y \in \text{Range}(f)$ (conclude)

Range−

$f : A \to B$ (show)
$y \in \text{Range}(f)$ (show)

For some $x \in A$, (constant declaration)
$y = f(x)$ (conclude)

Identity map+

$f : A \to A$ (show)
  Let $x \in A$ (variable declaration)
  $f(x) = x$ (show)
  ←

$f = \text{id}_A$ (conclude)

Identity map−

$\text{id}_A(x) = x$ (conclude)
$f : A \to A$ (conclude)

Composition+

$f : A \to B$ (show)
$g : B \to C$ (show)

$(g \circ f) : A \to C$ (conclude)
$(g \circ f)(x) = g(f(x))$ (conclude)

Composition−

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

$h(x) = g(f(x))$ (conclude)
$\text{Domain}(h) = \text{Domain}(f)$ (conclude)
$\text{Codomain}(h) = \text{Codomain}(g)$ (conclude)

Injective+

$f : A \to B$ (show)
  Let $x, y \in A$ (variable declaration)
    Assume $f(x) = f(y)$
    $x = y$ (show)
    ←
  ←

---

f is injective (conclude)

Injective−

f is injective (show)
$f(x) = f(y)$ (show)

$x = y$ (conclude)

Functions (cont.)

Surjective+	Surjective−
$f\colon A \to B$ (SHOW) Let $y \in B$ (variable declaration) $x \in A$ (SHOW) $y = f(x)$ (SHOW) $\leftarrow$ f IS SURJECTIVE	$f\colon A \to B$ IS SURJECTIVE (SHOW) $y \in B$ (SHOW) For some $x \in A$, (constant declaration) $y = f(x)$ (CONCLUDE)
Bijective+	**Bijective−**
f IS INJECTIVE (SHOW) f IS SURJECTIVE (SHOW) f IS BIJECTIVE (CONCLUDE)	f IS BIJECTIVE (SHOW) f IS INJECTIVE (CONCLUDE) f IS SURJECTIVE (CONCLUDE)
Inverse function+	**Inverse function−**
$f\colon A \to B$ (SHOW) $g\colon B \to A$ (SHOW) $g \circ f = \mathrm{id}_A$ (SHOW) $f \circ g = \mathrm{id}_B$ (SHOW) $g = f^{-1}$ (CONCLUDE)	$f^{-1} : B \to A$ (SHOW) f IS BIJECTIVE (CONCLUDE) $f^{-1}(f(x)) = x$ (CONCLUDE) $f\left(f^{-1}(y)\right) = y$ (CONCLUDE)
Inverse image+	**Inverse image−**
$f(x) \in T$ (SHOW) $x \in f^{\mathrm{inv}}(T)$ (CONCLUDE)	$x \in f^{\mathrm{inv}}(T)$ (SHOW) $f(x) \in T$ (CONCLUDE)

Remarks: The alternate function notation $A \xrightarrow{f} B$ and standard function notation $f\colon A \to B$ can be used interchangeably without a rule of inference as a shortcut.

Problems

In the following problems, capital letters represent sets.

10.40. (*Composition is associative*) If $h\colon A \to B$, $g\colon B \to C$, and $f\colon C \to D$ then

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

10.41. (*Nonsurjective injection*) Suppose $f\colon \mathbb{N} \to \mathbb{N}$ and for all $n \in \mathbb{N}$, $f(n) = 3n + 1$. Then f is injective but not surjective.

10.42. (*Yet this is both*) Suppose $f\colon \mathbb{R} \to \mathbb{R}$ and $f(x) = 3x + 1$ for all $x \in \mathbb{R}$. Then f is bijective.

10.43. (*Noninjective*) Suppose $f\colon \mathbb{Q} \to \mathbb{Q}$ and $f(r) = r^2$ for all rational numbers r. Then f is not injective.

10.44. (*Tiny function*) If $A = \{1\}$ and $G = \{(1,1)\}$ then there exists a function $f : A \to A$ such that G is the graph of f.

10.45. (*Image of subsets*) If $f\colon A \to B$ and $S \subseteq T$ and $T \subseteq A$ then $f(S) \subseteq f(T)$.

10.46. (*A bijection with a proper subset*) Let $E = \{n \in \mathbb{N} : n \text{ is even}\}$, and define $f\colon \mathbb{N} \to E$ such that $f(n) = 2n$ for all $n \in \mathbb{N}$. Then f is a bijection.

10.47. (*Composition of injective is injective*) If $f\colon A \to B$ and $g\colon B \to C$ are both injective then $g \circ f$ is injective.

10.48. (*Composition of surjective is surjective*) If $f\colon A \to B$ and $g\colon B \to C$ are both sujective then $g \circ f$ is surjective.

10.49. (*Composition of bijective is bijective*) If $f\colon A \to B$ and $g\colon B \to C$ are both bijective then $g \circ f$ is bijective.

10.50. (*Complement is bijective*) Let A be a set and define $f\colon \mathcal{P}(A) \to \mathcal{P}(A)$ such that $f(X) = X'$ for all $X \in \mathcal{P}(A)$. Then f is a bijection. Note that in this situation X' refers to $A - X$, i.e., A is the universal set.

10.51. (*Inverse of a composition*) If $f\colon A \to B$ and $g\colon B \to C$ are both bijective then

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

10.52. (*Identity maps are bijective*) The function id_A is bijective.

10.53. (*Inverse image of codomain*) If $f\colon A \to B$ then $f^{\mathrm{inv}}(B) = A$.

10.54. (*Image of the inverse image*) If $f\colon A \to B$ is surjective and $S \subseteq B$ then $f(f^{\mathrm{inv}}(S)) = S$.

10.55. (*Inverse image of the image*) If $f\colon A \to B$ is injective and $S \subseteq A$ then $f^{\mathrm{inv}}(f(S)) = S$.

10.56. (*Identity maps are identities*) If $f\colon A \to B$ then $f \circ \mathrm{id}_A = f$

10.57. (*Identity for composition*) If $f\colon A \to A$ then $f \circ \mathrm{id}_A = f$ and $\mathrm{id}_A \circ f = f$.

10.58. (*linear bijections*) A linear function is bijective if and only if it has nonzero slope. Here we define a linear function to be a map $f\colon \mathbb{R} \to \mathbb{R}$ such that for some $m, b \in \mathbb{R}$,

$$f(x) = m \cdot x + b$$

In this situation we say that m is the slope of f.

10.59. (*a real example*) Define $(0..1]$ to be the set $\{x \in \mathbb{R} : 0 < x \leq 1\}$ and let $f\colon \mathbb{R} \to (0..1]$ be the function such that for all real numbers x,

$$f(x) = \frac{1}{1 + x^2}$$

Then f is surjective but not injective.

10.5 Relations

We often identify a function with its graph. From that perspective, a function $f: A \to B$ is a subset of $A \times B$ that satisfies certain conditions. We can generalize this concept to other subsets of $A \times B$. Such a set is called a *relation* from A to B. In the case where $A = B$ we say that such a set defines a *relation on* A. Relations are often categorized by the properties they satisfy. Some of the more common properties of relations are described in the following table.

Relations

Name	Definition
Def of $\neq$	$x \neq y \Leftrightarrow \neg(x = y)$
Def of relation	R is a relation from A to $B \Leftrightarrow R \subseteq A \times B$
Relation on a set	R is a relation on $A \Leftrightarrow R \subseteq A \times A$
Infix notation	$xRy \Leftrightarrow (x, y) \in R$
Prefix notation	$R(x, y) \Leftrightarrow (x, y) \in R$
Reflexive relation	$R \subseteq A \times A$ is reflexive$\Leftrightarrow \forall x \in A, xRx$
Symmetric relation	$R \subseteq A \times A$ is symmetric$\Leftrightarrow \forall x \in A, \forall y \in A, xRy \Rightarrow yRx$
Transitive relation	$R \subseteq A \times A$ is transitive$\Leftrightarrow \forall x \in A, \forall y \in A, \forall z \in A, xRy$ and $yRz \Rightarrow xRz$
Irreflexive relation	$R \subseteq A \times A$ is irreflexive$\Leftrightarrow \forall x \in A, \neg(xRx)$
Antisymmetric relation	$R \subseteq A \times A$ is antisymmetric $\Leftrightarrow \forall x \in A, \forall y \in A, xRy$ and $yRx \Rightarrow x = y$
Total relation	$R \subseteq A \times A$ is total$\Leftrightarrow \forall x \in A, \forall y \in A, xRy$ or yRx
Partial order	$R \subseteq A \times A$ is a partial order $\Leftrightarrow R$ is reflexive, antisymmetric, and transitive.
Strict Partial order	$R \subseteq A \times A$ is a strict partial order $\Leftrightarrow R$ is irreflexive, antisymmetric, and transitive.
Total Order	$R \subseteq A \times A$ is total order $\Leftrightarrow R$ is antisymmetric, transitive, and total.
Equivalence Relation	$R \subseteq A \times A$ is an equivalence relation$\Leftrightarrow R$ is reflexive, symmetric, and transitive.
Equivalence Class	$R \subseteq A \times A$ is an equivalence relation and $a \in A \Rightarrow [a]_R = \{ x \in A : xRa \}$
Partition of a set	P is a partition of $A \Leftrightarrow P \subseteq \mathcal{P}(A)$ and $\emptyset \notin P$ and $A = \bigcup_{S \in P} S$ and $\forall S \in P, \forall T \in P, S = T$ or $S \cap T = \emptyset$

Relations (cont.)

Name	Definition
congruent mod m	if $m \in \mathbb{N}^+$ and $a, b \in \mathbb{Z}$ then $a \underset{m}{\equiv} b \Leftrightarrow k \mid b - a$

Rules of Inference for Relations

Not equal+

not $x = y$ (SHOW)

$x \neq y$ (CONCLUDE)

Not an element of−

$x \neq y$ (SHOW)

---

not $x = y$ (CONCLUDE)

Relation+

$R \subseteq A \times B$ (SHOW)

R is a relation from A to B (CONCLUDE)

Relation−

R is a relation from A to B (SHOW)

$R \subseteq A \times B$ (CONCLUDE)

Relation on a set+

$R \subseteq A \times A$ (SHOW)

R is a relation on A (CONCLUDE)

Relation on a set−

R is a relation on A (SHOW)

$R \subseteq A \times A$ (CONCLUDE)

Reflexive+

Let $x \in A$ (variable declaration)
xRx (SHOW)
←

R is reflexive (CONCLUDE)

Reflexive−

R is reflexive (SHOW)

---

xRx (CONCLUDE)

Symmetric+

Let $x, y \in A$ (variable declaration)
Assume xRy
yRx (SHOW)
←
←

R is symmetric (CONCLUDE)

Symmetric−

R is symmetric (SHOW)
xRy (SHOW)

---

yRx (CONCLUDE)

Rules of Inference for Relations (cont.)

Transitive+

Let $x, y, z \in A$ (variable declaration)
  Assume xRy and yRz
  xRz (show)
  ←
←
……
R is transitive (conclude)

Transitive−

R is transitive (show)
xRy (show)
yRz (show)
……
xRz (conclude)

Nonreflexive+

Let $x \in A$ (variable declaration)
not xRx (show)
←
……
R is nonreflexive (conclude)

Nonreflexive−

R is nonreflexive (show)
……
not xRx (conclude)

Antisymmetric+

Let $x, y \in A$ (variable declaration)
  Assume xRy and yRx
  $x = y$ (show)
  ←
←
……
R is antisymmetric (conclude)

Antisymmetric−

R is antisymmetric (show)
xRy (show)
$x \neq y$ (show)
……
not yRx (conclude)

OR

R is antisymmetric (show)
xRy (show)
……
$x = y$ or not yRx (conclude)

Total relation+

Let $x, y \in A$ (variable declaration)
xRy or yRx (show)
←
……
R is total (conclude)

Total relation−

R is total (show)
……
xRy or yRx (conclude)

Partial order+

R is reflexive (show)
R is antisymmetric (show)
R is transitive (show)
……
R is a partial order (conclude)

Partial order−

R is a partial order (show)
……
R is reflexive (conclude)
R is antisymmetric (conclude)
R is transitive (conclude)

Rules of Inference for Relations (cont.)

Strict partial order+

R is nonreflexive (show)
R is antisymmetric (show)
R is transitive (show)
.....
R is a strict partial order (conclude)

Strict partial order−

R is a strict partial order (show)
.....
R is nonreflexive (conclude)
R is antisymmetric (conclude)
R is transitive (conclude)

Total order+

R is antisymmetric (show)
R is transitive (show)
R is total (show)
.....
R is a total order (conclude)

Total order−

R is a total order (show)
.....
R is antisymmetric (conclude)
R is transitive (conclude)
R is total (conclude)

Equivalence relation+

R is reflexive (show)
R is symmetric (show)
R is transitive (show)
.....
R is an equivalence relation (conclude)

Equivalence relation−

R is an equivalence relation (show)
.....
R is reflexive (conclude)
R is symmetric (conclude)
R is transitive (conclude)

Equivalence class+

xRa (show)
.....
$x \in [a]_R$ (conclude)

Equivalence class−

$x \in [a]_R$ (show)
.....
xRa (conclude)

Partition+

$P \subseteq \mathcal{P}(A)$ (show)
  Let $x \in A$ (variable declaration)
  $\exists S \in P, x \in S$ (show)
  ←
  Let $S \in P$ (variable declaration)
  $S \neq \emptyset$ (show)
  ←
  Let $S, T \in P$ (variable declaration)
    Assume $x \in S$ and $x \in T$
    $S = T$ (show)
    ←
  ←
.....
P is a partition of A (conclude)

Partition−

P is a partition of A (show)
$S, T \in P$ (show)
.....
$S \neq \emptyset$ (conclude)
$S \subseteq A$ (conclude)
$S \cap T = \emptyset$ or $S = T$ (conclude)

OR

P is a partition of A (show)
$x \in A$ (show)
.....
$x \in S$ for some $S \in P$ (conclude)

Notation. We often abbreviate $[a]_R$ by $[a]$ when the relation R is clear from context.

Theorem. *Let $R \subseteq A \times A$ be an equivalence relation and $a, b \in A$. Then*

$$[a] = [b] \Leftrightarrow aRb.$$

Corollary. *Let $R \subseteq A \times A$ be an equivalence relation. Then A is a disjoint union of equivalence classes, i.e.*

$$A = \bigcup_{a \in A} [a]$$

and

$$\forall a, b \in A, [a] = [b] \text{ or } [a] \cap [b] = \emptyset.$$

Note. Thus, the set of equivalence classes of an equivalence relation on A is a partition of A. Furthermore, every partition P of A is the set of equivalence classes for the equivalence relation R on A defined by $\forall x, y \in A, xRy \Leftrightarrow \exists S \in P, x \in S \text{ and } y \in S$.

Problems

In the following problems, capital letters represent sets.

10.60. (*Not an equivalence relation*) Suppose $\sim$ is the set

$$\sim = \{ (1,1), (2,2), (3,3), (1,2), (2,1), (1,3), (3,1) \}$$

Then $\sim$ is not an equivalence relation on the set $\{1, 2, 3\}$.

10.61. (*Not not an equivalence relation*) If $\sim$ is a relation on $\mathbb{Z}$ such that for all $x, y \in \mathbb{Z}$,

$$x \sim y \Leftrightarrow x = y \text{ or } x = {}^{-}y$$

then $\sim$ is an equivalence relation.

10.62. (*equivalence relation induced by a function*) If $f : A \to B$ and $\sim$ is a relation on A such that for all $x, y \in A$,

$$x \sim y \Leftrightarrow f(x) = f(y)$$

then $\sim$ is an equivalence relation.

10.63. (*an equivalence relation?*) Let $\sim$ be the relation on $\mathcal{P}(\mathbb{Z})$ such that for all $A, B \in \mathcal{P}(\mathbb{Z})$,

$$A \sim B \Leftrightarrow \exists z \in \mathbb{Z}, z \in A \cap B$$

Prove your answer to the following questions.

(a) Is $\sim$ reflexive?

(b) Is $\sim$ symmetric?

(c) Is $\sim$ transitive?

10.64. (*an equivalence relation?*) Let $z \in \mathbb{Z}$. Define $\sim_z$ be the relation on $\mathcal{P}(\mathbb{Z})$ such that for all $A, B \in \mathcal{P}(\mathbb{Z})$,

$$A \sim_z B \Leftrightarrow z \in A \cap B$$

Prove your answer to the following questions.

(a) Is $\sim_z$ reflexive?

(b) Is $\sim_z$ symmetric?

(c) Is $\sim_z$ transitive?

10.65. (*Congruence is an equivalence relation*) Let m be a positive integer. The relation $\underset{m}{\equiv}$ is an equivalence relation on any set of integers.

10.66. (*class representatives mod m*) Let m be a positive integer. For any integer n there exists a unique integer k with $0 \leq k < m$ such that $n \underset{m}{\equiv} k$.

10.67. (*moduli are zeroish*) Let $m \in \mathbb{N}^+$ and $a, k \in \mathbb{Z}$. Then $a \underset{m}{\equiv} a + k \cdot m$

10.68. (*modular addition*) Let $m \in \mathbb{N}^+$ and $a, b, c, d \in \mathbb{Z}$. If $a \underset{m}{\equiv} b$ and $c \underset{m}{\equiv} d$ then $a + c \underset{m}{\equiv} b + d$.

10.69. (*modular multiplication*) Let $m \in \mathbb{N}^+$ and $a, b, c, d \in \mathbb{Z}$. If $a \underset{m}{\equiv} b$ and $c \underset{m}{\equiv} d$ then $a \cdot c \underset{m}{\equiv} b \cdot d$.

10.70. (*Equivalence classes are disjoint*) If $\sim$ is an equivalence relation on a set A and $x, y \in A$ then either $[x] = [y]$ or $[x] \cap [y] = \{\}$.

10.71. (*A partial order*) Let A be a set and $\sim$ be the relation on $\mathcal{P}(A)$ such that for every $S, T \in \mathcal{P}(A)$,

$$S \sim T \Leftrightarrow S \subseteq T$$

Then $\sim$ is a partial order.

10.72. (*A strict partial order*) Define $A = \{X \subseteq \mathbb{N} : 0 \in X\}$. For any $S \in A$ and $n \in \mathbb{N}$ we say S is *n-complete* if and only if $\mathbb{O}_n$ is a subset of S and $\mathbb{O}_{n+1}$ is not a subset of S. Let $\sim$ be a relation on A such that for all $S, T \in A$,

$$S \sim T \Leftrightarrow \exists m, \exists n, m < n \text{ and } S \text{ is } m\text{-complete and } T \text{ is } n\text{-complete}$$

Then $\sim$ is a strict partial order.

11 Expository Proofs

We are now ready to make the final transition to the traditional expository proofs found in most textbooks and articles about mathematics.

In Section 1 we introduced formal proofs. These proofs satisfy the first goal of a proof - they are objectively verifiable by a computer.

In practice, formal proofs of all but the most trivial theorems can be very long and tedious, and not as easy to read or understand by a human as we might like. As a result, we introduced a number of shortcuts in Section 6 to eliminate tedious, repetitive steps, shorten the proof, and emphasize the

aspects of the proof that would make it more readable to a human without sacrificing the objective correctness of the proof. This gave us what we refer to as semiformal proofs.

It is now time to make the final transition to the far right end of the proof spectrum illustrated by the bridge in Figure 1. We will refer to these proofs as *expository proofs* or *traditional proofs* or *informal proofs*.

11.1 Traditional Proofs

Because they are informal by design, and their goal is exposition, it is not easy to define precisely what constitutes a traditional proof as distinct from a formal or semiformal proof. Indeed, since the main goal of a traditional proof is exposition for human readers, defining it precisely is equivalent to defining what constitutes good expository writing in general.

That having been said, a traditional proof can be thought of as a proof obtained if you start with a semiformal proof, and modify it to conform to the following principles.

Requirements of a Traditional Proof

1. The proof must conform to all of the usual rules of grammar, punctuation, and spelling, for writing in English (or whatever language you are writing the proof in).
2. The proof should be written at the appropriate level for the intended audience. In particular, premises may be omitted or left unjustified if the intended reader will be able to fill them in themselves.
3. The wording of the proof should have an unambiguous meaning.
4. The proof can contain extra explanations and commentary that is not required for the proof to be objectively correct, but aid the reader in understanding the proof.

11.2 Specific Rules for Mathematical Writing

Mathematical writing has many features that distinguish it from other types of writing. The following is a list of guidelines to keep in mind that will help you to express your mathematical ideas in ways that will help others to more easily understand what you are trying to say.

11.3 Notation

An important part of making mathematical writing unambiguous and easy to understand is to choose good notation for the things you are writing about, and to carefully explain this notation to your readers. Some guidelines to keep in mind concerning mathematical notation are:

- *Always clearly define new notation as it's introduced.* Even if the notation seems obvious to you, it is not a good idea to assume that your reader knows what you mean by it. In particular, you should always declare new variables and constants when they are first used in the proof.

  Bad: We can see that n is odd, so $n = 2k + 1$.

  Good: We can see that n is odd, so $n = 2k + 1$ for some integer k.

Bad: If a continuous function f satisfies $f(nx) = f(x)^n$ for all x, n, is it true that f is an exponential function?

Good: If a continuous function f satisfies $f(nx) = f(x)^n$ for all real x and all positive integers n, is it true that f is an exponential function?

- *Use standard notation for common types of objects.* For instance, m and n are often used to denote integers, p denotes a prime, x can be a real number, f and g describe functions, and so on.

  The standard notation may depend on the context of your writing. For instance, in complex analysis, z is often used to denote a complex number, while in analytic number theory, s is more common. Use the notation that your readers will most readily recognize.

- *Use consistent symbols for similar objects.*

  Bad: Let x, u, ξ be real numbers.

  Good: Let x, y, z be real numbers.

  One exception to this guideline is that inconsistent symbols can be useful to denote objects that you want to distinguish in meaning to the reader:

  Okay: Let m, b be real numbers. Then the function $f : \mathbb{R} \to \mathbb{R}$ satisfying $f(x) = mx+b$ for all real numbers x is linear.

- *Don't use the same notation for different objects in the same scope.* Aside from being confusing to the reader, this usually will result in incorrect proofs.

  Bad: To show that the product of any two even integers is divisible by 4, suppose a and b are even. Then $a = 2k$ and $b = 2k$ for some integer k. Thus $ab = 2k \cdot 2k = 4k^2$ is divisible by 4.

  Good: To show that the product of any two even integers is divisible by 4, suppose a and b are even. Then $a = 2j$ for some integer j and $b = 2k$ for some integer k. Thus $ab = 2j \cdot 2k = 4jk$ is divisible by 4.

  Notice that the first 'proof' could likewise be used to prove that the product of any two even integers is a square, a claim that is obviously not true.

- *Avoid convoluted or overloaded notation.* Use several simple expressions rather than a single convoluted expression to increase clarity. Sometimes written prose can be more clear than symbolic expressions.

  Bad: Let $0 < n \in \mathbb{Z}$.

  Good: Let $n \in \mathbb{Z}$ with $n > 0$.

  Better: Let n be a positive integer.

11.4 Syntax

Mathematical symbols are a short and precise way to express mathematical ideas, but it's important to use them in ways that don't interfere with communication:

- *Don't begin a sentence with a symbol.*

Bad: x is a global maximum of f, so we have $f(x) \geq f(y)$ for every $y \in \mathbb{R}$.

Good: Since x is a global maximum of f, we have $f(x) \geq f(y)$ for every $y \in \mathbb{R}$.

Bad: Let a be a quadratic residue. $a = b^2$ for some $b \in \mathbb{Z}_n$.

Good: Let a be a quadratic residue. Then we can write $a = b^2$ for some $b \in \mathbb{Z}_n$.

- *Don't needlessly mix symbols with prose.* Many mathematical symbols have a spoken English equivalent, so it can be tempting to cleverly substitute the symbol for the corresponding English word in mathematical writing. However, this usually distracts from the meaning of the sentence and makes writing less understandable.

  Bad: Clearly, $x^2 + y^2 > 0 \Rightarrow x \neq 0 \vee y \neq 0$.

  Good: Clearly, if $x^2 + y^2 > 0$ then either $x \neq 0$ or $y \neq 0$.

  Bad: There are exactly eight primes < 20.

  Good: There are exactly eight primes less than 20.

  The logical connectors and quantifiers $\vee$, $\wedge$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$ are very easy to misuse in this way. In general, use these only in contexts where you are discussing mathematical logic, or as part of longer symbolic expressions.

  Bad: It is true $\forall$ integers that $\exists$ an even larger integer.

  Okay: Thus we can express this in formal logic as $\forall x, P(x) \wedge \neg Q(x)$.

  Okay: Let $Z = \{ n \in \mathbb{Z} : \forall k \in \mathbb{Z}, k \mid n \}$.

- *Don't use unnecessary variable names in theorem statements.* If an object needs a name in a proof, declare it in the body of the proof rather than in the theorem statement.

  Bad: Any continuous function f on the interval $[0, 1]$ is uniformly continuous.

  Good: Any continuous function on the interval $[0, 1]$ is uniformly continuous.

  This also applies for claims made in the middle of a proof.

- *When possible, use words to separate symbols which are not in a list.* This can often make statements more readable.

  Bad: If the congruence equation $n^2 \underset{p}{\equiv} a$ has a solution $n = \overline{b}$, $n = \overline{p} - \overline{b}$ is the only other solution of the equation.

  Good: If the congruence equation $n^2 \underset{p}{\equiv} a$ has a solution $n = \overline{b}$, then $n = \overline{p} - \overline{b}$ is the only other solution of the equation.

- *Write out integers used as adjectives, and use Arabic numerals to write integers describing numerical values.*

  There are exactly twenty-four elements in the symmetric group on four symbols.

  The first three positive powers of 2 are 2, 4, and 8.

  The set of prime numbers less than 20 has eight elements.

11.5 Equations and Formulas

Equations and formulas play an important role in many types of mathematical writing, so it is a good idea to present them in as clear a manner as possible. Some considerations to keep in mind are to:

- *Place important equations or formulas on their own line.* This makes the expression more visible, and indicates its importance in the writing. Such typesetting is sometimes called a 'display' style. If you need to reference the expression later in the text, give it a numbered label, as in:

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

  In general, don't label an expression like this if you don't plan to reference it later in the writing. If you only reference an expression in the few preceding or following lines, consider instead using language such as 'in the following expression' or 'by the above equation'.

- *When writing out extended computations in a display style, use transitive chain notation.*

  Bad:

$$(a+b)^3 = (a+b)(a+b)^2 = (a+b)(a^2+2ab+b^2) = a^3+3a^2b+3ab^2+b^3$$

  Bad:

$$\begin{aligned}(a+b)^3 &= (a+b)(a+b)^2\\ (a+b)^3 &= (a+b)(a^2+2ab+b^2)\\ (a+b)^3 &= x^3+3x^2+3x+1\end{aligned}$$

  Bad:

$$\begin{aligned}(a+b)^3 &= (a+b)(a+b)^2\\ (a+b)(a+b)^2 &= (a+b)(a^2+2ab+b^2)\\ (a+b)(a^2+2ab+b^2) &= x^3+3x^2+3x+1\end{aligned}$$

  Good:

$$\begin{aligned}(a+b)^3 &= (a+b)(a+b)^2\\ &= (a+b)(a^2+2ab+b^2)\\ &= a^3+3a^2b+3ab^2+b^3\end{aligned}$$

- *Use consistent punctuation after display style expressions.* Some mathematicians treat display style expressions as part of the surrounding sentence structure, ending with a comma or a period as appropriate in the writing, while others omit all punctuation after display style expressions. In these notes, for instance, we chose to omit punctuation. Either way is acceptable, but be consistent with your choice in a given piece of writing.

- *Avoid pointless parentheses in mathematical expressions.*

Bad: $(x-1)^2 = (x^2 - 2x + 1)$

Good: $(x-1)^2 = x^2 - 2x + 1$

Extra parentheses are fine if they are serving to emphasize a part of the expression to the reader as being special or grouped together. For instance, the following example indicates to the reader that the grouping of the terms on the right side deserves special attention:

Okay: $(a+b)^3 = (a^3 + b^3) + 3(a^2b + ab^2)$

- *Use parentheses to clarify between subtraction and negative signs.*

  Bad: $(x+y) \cdot -z = -xz - yz$

  Good: $(x+y)(-z) = -xz - yz$

11.6 Writing Technique

Writing mathematics is similar in many ways to any other type of writing you might do! It's about distilling your ideas down into a simple and organized form, and communicating these ideas to your readers clearly and efficiently. This is, by its nature, a somewhat messy process, but some things to keep in mind include:

- *Tell the reader where you are going.* As you are explaining the steps of your proof, include a few words to describe the bigger picture of your argument or the strategy you are using. This allows the reader to anticipate the specifics of your proof more accurately, and can greatly increase their understanding of how the pieces of your proof fit together to form a cohesive argument.

  Good: We will prove this claim by induction on n.

  Good: We now consider the converse direction.

  Good: The following will make use of compactness of the space X.

  Four situations where such comments can be valuable are

  1. announcing that you will be proving something by contradiction,
  2. announcing you are proving something by induction, announcing the base case, and announcing the inductive hypothesis or step,
  3. announcing which direction ($\Rightarrow$ or $\Leftarrow$) you are starting to prove in the proof of a logical equivalence (i.e., of an 'if and only if' statement),
  4. announcing that you will be proving something by cases, and announcing the start of the proof of each case.

- *Use key phrases to explain your reasoning.* Expressions like 'since', 'because', 'on the other hand', 'observe', and 'note' help guide the reader's attention and elaborate on the relations between different statements. Vary your word choices to avoid monotonous writing. Notice that unlike semiformal or formal proofs, we generally do not usually cite the rules of inference for logic in traditional expository proofs, although we may refer to the overall strategy being used (induction, proof by contradiction, proof by cases, etc.).

> Bad: Suppose 5 divides b^3 and 3 divides b^3. We showed that if a prime p divides a power a^k, then p divides a. Thus, 5 divides b. Thus, 3 divides b. Thus, 15 divides b.
>
> Good: Suppose 3 divides b^3 and 5 divides b^5. We showed that any prime that divides a power of a natural number, n, must also divide n. Thus, as 3 and 5 are both prime, they both divide b. Therefore their product, 15, must also divide b.

- *Plan enough time to write.* Any form of writing takes time, and the rigor and attention to detail needed in mathematical writing only magnifies this requirement.
- *Outline your ideas before you begin writing.* When writing down a mathematical proof or mathematical exposition in general, it helps to have a clear idea of what you want to say, and in what order. This gives you an opportunity to look at the big picture and make changes in the structure before you spend a lot of time hammering out the little details. Although it might feel better to just dive right into the writing phase, you'll save time and produce significantly better exposition by planning ahead.
- *Proofread!* When time is short, it may be tempting to finish the last line of your proof, throw on a quick Q.E.D., and hand in your writing, but this is a terrible idea. Math is hard to write, and it is nearly impossible to write it without at least a few typos. When you look back on what you've written, you'll be able to correct any small errors that you made, and you might also gain some additional insight into the math you were writing about, or come up with a better way of expressing the solution. Writing is an iterative process, so make sure to give your work at least a second look over to improve its quality.
- *Check your spelling, grammar, and punctuation.* People reading mathematical proofs are usually intelligent and easily bothered by spelling errors, improper use of contractions, incorrect homophones, and general grammatical sloppiness. These sorts of flaws can distract from the content of your proof, so make sure you pay attention to these kinds of errors as well when you're proofreading your work!

11.7 Mathematical Typesetting

In addition to the special rules for mathematical writing mentioned in the previous section, the requirements of correctly typesetting mathematical expressions are a challenge for most modern word processors and text editors. As a result, the de facto standard for mathematical typesetting that all mathematicians use is based on a language called LaTeX.

There are many great LaTeX tutorials on the internet, and in most cases doing a search for the thing you are trying to do will immediately answer any question that comes up. (See our course website for details.)

There are many do's and don't when using LaTeX itself, which you will learn with time and experience (usually because what you typed ends up looking terrible). But there is one beginner mistake that we will mention for you to be aware of. Resist the urge to manually format your compiled document by hand.

12 Combinatorial Proofs

12.1 Combinatorics

Combinatorics (or more precisely *enumerative combinatorics* is the branch of mathematics that studies counting. One way to try to integrate this topic into the mathematical infrastructure of logic and set theory we have discussed so far is to define the number of elements in a finite set S to be n if and only if there exists a bijection between S and $\mathbb{I}_n$.

Definition 21. Let S be a set and $n \in \mathbb{N}$. We say that S has *cardinality* n if and only if there exists a bijection $f\colon \{1, 2, \ldots, n\} \to S$. In this case, we write $\#S$ or $|S|$ for the cardinality of S.

Note that $\mathbb{I}_n = \{1, 2, \ldots, n\}$ is the empty set when $n = 0$.

Example 22. With this definition, we can formally prove that $\#\{\,\smile\,\} = 1$.

This definition leaves a bit to be desired, however. One of the first things that any preschooler learns about mathematics is the difference between none, one, and several. Fortunately, there is another kind of mathematical proof that is accepted in journals and by mathematicians as a valid proof that is better suited to this task.

12.2 Combinatorical Collections and Expressions

We begin by defining the language of a different kind of proof system that is distinct from the formal axiom system kinds of proofs that we have discussed so far. This form of proof will be based on counting, and so we need something to count.

Definition 23. A *combinatorial collection* is anything that can be counted. Each combinatorial collection has a property called its *count* (or *cardinality* or *size)* which represents the number of entities comprising the collection. Two combinatorial collections are said to be *equivalent* if they have the same count. If A is a combinatorial collection then we write $\#A$ or $|A|$ for the count of A.

Anything we can count is an example of a combinatorial collection. For example, we can count the number of elements in a finite set, or the number of ways we can accomplish some task, the number of possible outcomes from some activity, or the number of choices we have in making some decision. In each case the count can be represented by a symbolic expression.

Definition 24. A *combinatorial expression* is an expression that represents the cardinality of a combinatorial collection.

Naturally, we can define an expression for any combinatorial collection we might have. Here are some common combinatorial expressions that we will use in what follows.

Expression	Combinatorial definition (what it counts)
$0, 1, 2, 3, \ldots$	Any collection of one, two, three, ... things respectively.
n	A collection of n things where n is one of $0, 1, 2, 3, \ldots$
$a + b$	A collection that can be partitioned into two disjoint collections having size a and b respectively.
$a_1 + a_2 + \cdots + a_n$	A collection that can be partitioned into n disjoint collections of size $a_1, a_2, \ldots, a_n$ respectively.
$a \cdot b$	The number of ways of choosing two things in order if there are a ways to choose the first and b ways to choose the second.
$a_1 \cdot a_2 \cdot a_3 \cdots a_n$	The number of ways of choosing n things in order if there are a_1 ways to choose the first, a_2 ways to choose the second and so on.
$n!$	The number of ways to permute (rearrange) n distinct things in some order
n^k	The number of ways to choose k things from n things where repetition is allowed and order matters.
$(n)_k$	The number of ways to choose k things from n things where repetition is not allowed and order matters
$\binom{n}{k}$	The number ways to choose k things from n things where repetition is not allowed and order doesn't matter
$\left(\!\binom{n}{k}\!\right)$	The number of ways of choosing k things from n things where repetition is allowed and order doesn't matter

Some of the combinatorial expressions given in the previous table have common names and alternate notation in mathematics. The expression $n!$ is called "*n-factorial*". The expression $(n)_k$ is sometimes denoted ${}_nP_k$ is read "*n permute k*" and counts the number of *k-permutations* of n things. The expression $\binom{n}{k}$ is called a *binomial coefficient* and is sometimes denoted ${}_nC_k$. It is read "*n choose k*" and counts the number of *k-combinations* of n things.

Finally, we need some statements that we can prove with our new kind of proof. The simplest such statements are called combinatorial identities.

Definition 25. A *combinatorial identity* is a expression of the form

$$A = B$$

where A and B are combinatorial expressions.

12.3 Combinatorial Proofs

The fundamental assumption on which the validity of all counting relies, is that no matter how you count the same collection, if you do it correctly, you will obtain the same result. This simple idea is the foundation for a kind of mathematical proof called a *combinatorial argument*.

Definition 26. A *combinatorial proof* (or *combinatorial argument*) is proof of a combinatorial identity obtained by counting the same thing (or two equivalent things) in two different ways.

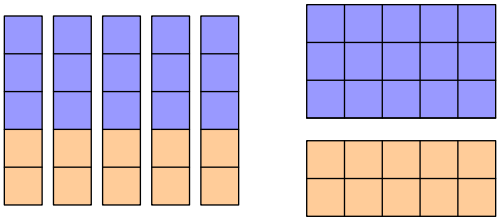
It is truly amazing the extent to which we can build up much of algebra from a combinatorial perspective, and give combinatorial proofs of many algebraic identities. Often, combinatorial interpretations are considered to be easier and more intuitive explanations of a given fact than algebraic or inductive proofs.

Example 27. The fact that

$$5 \cdot (3 + 2) = 3 \cdot 5 + 2 \cdot 5$$

can be verified by invoking the distributive law and commutative law of multiplication, but that doesn't give us a sense of what the identity says about counting.

Using a combinatorial argument, however, we can say that the left hand side counts the total number of squares in a collection consisting of 5 collections, each of which is comprised of two disjoint collections having 3 things and 2 things respectively (as illustrated in the left figure below), and the right hand side counts the same collection of squares partitioned into two collections, one consisting of 3 collections of 5 squares (the blue ones) and another consisting of 2 collections of 5 squares (the orange ones, as illustrated in the right figure below). Since we are counting the same collection of little squares in two different ways, this is a combinatorial proof of the identity above.



□

Proofs similar to the one in the above example can be generalized to give combinatorial proofs of the algebraic properties of numbers given in the axioms for the real numbers.

In this context, rather than starting with algebraic axioms such as the distributive law, we can start with tactile meanings of numbers, addition, multiplication, division, and so on. These arguments can then be pasted together to deduce all the algebraic axioms we usually work with.

While it is possible to give purely combinatorial proofs of many combinatorial identities, it is also commonplace to use both combinatorial and axiomatic algebraic arguments in the same mathematical proof. Thus, we can use combinatorial arguments even as just one part of a larger proof involving many techniques.

12.4 Combinatorial subtraction, division, and inequality

Just as in algebra, it is often convenient to be able to discuss the difference or quotient of two combinatorial expressions. The problem with doing that from a combinatorial perspective is that the difference or quotient of two combinatorial expressions is not always a combinatorial expression. So we have to take some care when defining them to take that into account.

Definition 28. Let k, m, and n be combinatorial expressions.

1. If $k + m = n$ then $k \leq n$. Also, if $k \leq n$ and $k \neq n$ then $k < n$.
2. If $k + m = n$ then we define $n - k$ to be m.
3. If $k \cdot m = n$ and $k \neq 0$ then we define n/k to be m.

In general, whenever we use such an expression we are assuming it is defined for the expression to make sense. Thinking of these expressions as natural numbers for a moment, we can say that $n-k$ to be defined it is sufficient for k to be less than n. But for n/k to be defined k must be a divisor of n. In order to avoid this problem we avoid using division and subtraction wherever possible in combinatorial proofs, except when we need to refer to arbitrary sequences like $1, 2, \ldots, n-2, n-1, n$.

Problems

Basic Combinatorial Identities

The following combinatorial identities can all be proved using a combinatorial proof using only the definitions given in Section 12.2. If we were defining combinatorics in an algebraic setting (as you might find in a course on discrete mathematics or combinatorics), these identities are often taken to be the definition of the symbols defined in Section 12.2. From the perspective of combinatorial proofs, these identities are all theorems that we prove by counting the same collection in two different ways.

In the following identities, all variables are combinatorial expressions. Use a purely combinatorial proof to prove the theorems in this section.

12.1. (*zero power*) $n^0 = 1$

12.2. (*alternate definition of multiplication*) $k \cdot n = \underbrace{n + n + \cdots + n}_{k \text{ summands}} = \underbrace{k + k + \cdots + k}_{n \text{ summands}} = n \cdot k$

12.3. (*alternate definition of factorial*) $n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$

12.4. (*alternate definition of power*) $n^k = \underbrace{n \cdot n \cdots n}_{k \text{ factors}}$

12.5. (*alternate definition of permutation*) $(n)_k = n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)!$

12.6. (*alternate definition of permutation*) $(n)_k \cdot (n-k)! = n!$

12.7. (*alternate definition of choose*) $\binom{n}{k} \cdot k! \cdot (n-k)! = n!$

12.8. (*alternate definition of choose with repeats*) $\left(\!\binom{n}{k}\!\right) = \binom{n-1+k}{k}$

Other combinatorial identities

Some of the usual properties of these expressions that can be derived from these by induction and/or algebra often have interesting combinatorial proofs as well.

12.9. (*our favorite theorem redux*) $1 + 1 = 2$

12.10. (*counting over computing*) $\binom{6}{2} \cdot \binom{4}{3} = \binom{6}{3} \cdot \binom{3}{2}$

12.11. (*more counting over computing*) $\left(\!\binom{8}{3}\!\right) = \left(\!\binom{4}{7}\!\right)$

12.12. (*our favorite theorem redux*) $(2 \cdot m) \cdot (2 \cdot n) = (m \cdot n) \cdot 4$

12.13. (*binomial complement*) $\binom{m+n}{m} = \binom{m+n}{n}$

12.14. (*multichoose complement*) $\left(\!\binom{n+1}{k}\!\right) = \left(\!\binom{k+1}{n}\!\right)$

12.15. (*choose vs permute*) $(n)_k = \binom{n}{k} \cdot k!$

12.16. (*ordered choice*) $\binom{n}{k} \cdot \binom{n-k}{j} = \binom{n}{j} \cdot \binom{n-j}{k}$

12.17. (*more ways to choose*) $\binom{2n+2}{k} = \binom{2n}{k} + 2 \cdot \binom{2n}{k-1} + \binom{2n}{k-2}$

12.18. (*Pascal's multichoose*) $\left(\!\binom{n+1}{k}\!\right) = \left(\!\binom{n}{k}\!\right) + \left(\!\binom{k}{n}\!\right)$

12.19. (*Hockey Stick Redux*) $\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \cdots + \binom{n-1}{k} + \binom{n}{k} = \binom{n+1}{k+1}$

12.20. (*multichoose Hockey Stick*) $\left(\!\binom{n}{0}\!\right) + \left(\!\binom{n}{1}\!\right) + \left(\!\binom{n}{2}\!\right) + \cdot + \left(\!\binom{n}{k-1}\!\right) + \left(\!\binom{n}{k}\!\right) = \left(\!\binom{n+1}{k}\!\right)$

12.21. (*another multichoose Hockey Stick*) $\left(\!\binom{1}{k}\!\right) + \left(\!\binom{2}{k}\!\right) + \cdot + \left(\!\binom{n-1}{k}\!\right) + \left(\!\binom{n}{k}\!\right) = \left(\!\binom{n}{k+1}\!\right)$

12.22. (*another ordered choice*) $(k+1) \cdot \binom{n+1}{k+1} = (n+1) \cdot \binom{n}{k}$

12.23. (*factorial recursion*) $n! = n \cdot (n-1)!$

12.24. (*power recursion*) $n^k = n \cdot n^{k-1}$

12.25. (*permutations recursion*) $(n+1)_{k+1} = (n+1) \cdot (n)_k$

12.26. (*combination recursion*) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

12.27. (*another permutations recursion*) $(n+1)_{k+1} = (n)_{k+1} + (k+1) \cdot (n)_k$

12.28. (*another Gauss' formula*) $1 + 2 + 3 + \cdots + n = \binom{n+1}{2}$

12.29. (*sum of squares*) $3 \cdot (1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 + n^2) = (2n+1) \cdot \binom{n+1}{2}$

12.30. (*sum of cubes*) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \binom{n+1}{2}^2$

12.31. (*Vandermonde's identity*) $\binom{m}{0} \cdot \binom{n}{k} + \binom{m}{1} \cdot \binom{n}{k-1} + \ldots + \binom{m}{k-1} \cdot \binom{n}{1} + \binom{m}{0} \cdot \binom{n}{k} = \binom{m+n}{k}$

12.32. (*binomial theorem*) $\binom{n}{0} \cdot x^n \cdot y^0 + \binom{n}{1} \cdot x^{n-1} \cdot y^1 + \binom{n}{2} \cdot x^{n-2} \cdot y^2 + \cdots + \binom{n}{n} \cdot x^0 \cdot y^n = (x+y)^n$

12.33. (*sum of row of Pascal's triangle*) $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$

12.34. (*linear sum of row of Pascal's triangle*) $0 \cdot \binom{n}{0} + 1 \cdot \binom{n}{1} + 2 \cdot \binom{n}{2} + 3 \cdot \binom{n}{3} + \cdots + n \cdot \binom{n}{n} = n \cdot 2^{n-1}$

12.35. (*sum of squares of row of Pascal's triangle*) $\binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n-1}^2 + \binom{n}{n}^2 = \binom{2n}{n}$

12.36. (*linear sum of squares of row of Pascal's triangle*)

$$0 \cdot \binom{n}{0}^2 + 1 \cdot \binom{n}{1}^2 + 2 \cdot \binom{n}{2}^2 + 3 \cdot \binom{n}{3}^2 + \cdots + n \cdot \binom{n}{n}^2 = n \cdot \binom{2n-1}{n-1}$$

Combinatorial identities and problem solving

We can apply the method of combinatorial proof to solve counting problems by defining new combinatorial expressions, and then proving identities involving them by counting in two ways.

12.37. (*Frog hopping a staircase*) Froggy Frog is at the bottom of a staircase with n stairs and wants to get to the top. He can only jump 1 or 2 stairs at a time and never backtracks. Let W_n be the number of ways Froggy can jump from the bottom of the stairs to the top.

(a) Prove that $W_{n+2} = W_{n+1} + W_n$.

(b) How many ways can Froggy climb a staircase with 20 stairs?