Intro to Proof Lecture Notes - Revised Draft

Dr. Monks - University of Scranton

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.

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

The Proof Spectrum

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

In order 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.

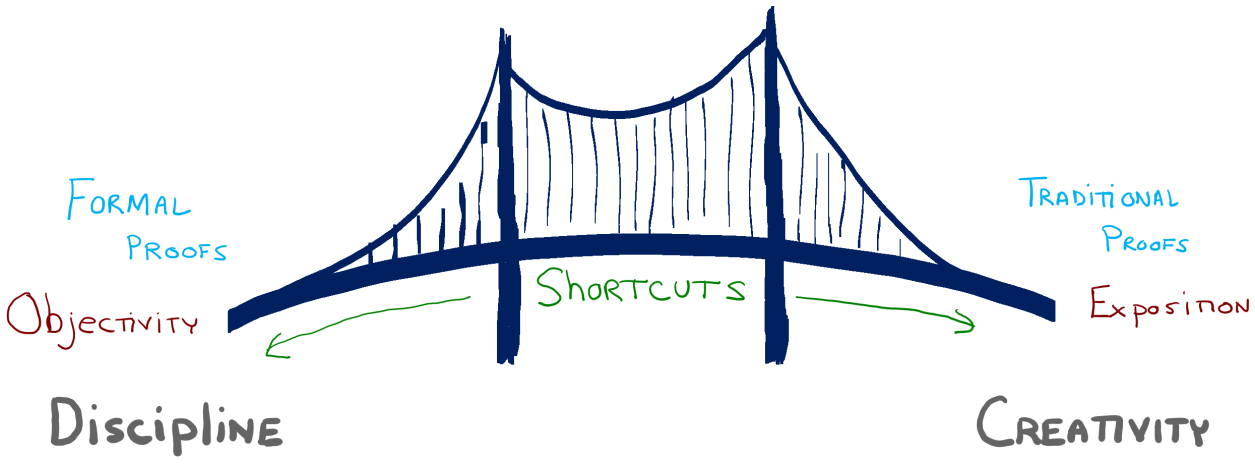


Figure 1: The Proof Spectrum

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

Formal Proof Systems

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

1. A set of expressions $\mathcal{S}$, called the *statements*.
2. A set of rules $\mathcal{R}$, called the *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

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

2. for each $1 \leq i \leq k$, if P_i is a statement, then P_i is provable from a (possibly empty) subcollection of $Q_1, \ldots, Q_n$.

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*.

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.

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

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

It is also commonplace to refer to such an expression as a theorem. To prove such a theorem is to give a proof of Q in the same formal system where additionally the premises are 'Given' as axioms.

Toys Proofs and Lurch

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

`proveitmath.org/toyproofs`

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. Warning: it can be both addictive and hard!

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. 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!

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 of 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.

Finally, *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`

2 The Language of Mathematics

We write our proofs in the language of mathematics. The building blocks of this language are described by the following terms.

2.1 Variables, Expressions, and Statements

Term	**Description**
set	A *set* is a collection of items.
element	The items in a set are called its *elements* (or members).
expression	An *expression* is an arrangement of symbols which represents an element of a set
type	The set of elements that an expression can represent is called the *type* of the expression.
value	The element of the domain that the expression represents is called a *value* of that expression.
variable	A *variable* is an expression consisting of a single symbol
constant	A *constant* is an expression whose domain contains a single element.
statement	A *statement* (or *Boolean expression*) is an expression whose domain is $\{\text{true}, \text{false}\}$.
truth value	The value of a statement is called its *truth value*.
solve	To *solve* a statement is to determine the set of all elements for which the statement is true.
solution set	The set of all solutions of a statement is called the *solution set*.
equation	An *equation* is a statement of the form $A = B$ where A and B are expressions.
inequality	An *inequality* is a statement of the form $A \star B$ where A and B are expressions and $\star$ is one of $\leq$, $\geq$, $>$, $<$, or $\neq$.

Remarks:

- An element is either in a set or it is not in a set, it cannot be in a set more than once.
- It is not necessary that we know specifically which element of the domain an expression represents, only that it represents some unspecified element in that set.
- We do not have to know if a statement is true or false, just that it is either true or false.
- If a statement contains n variables, $x_1, \ldots x_n$, then to solve the statement is to find the set of all n-tuples $(a_1, \ldots, a_n)$ such that each a_i is an element of the domain of x_i and the statement becomes true when $x_1, \ldots, x_n$ are replaced by $a_1, \ldots, a_n$ respectively. In this situation, each such n-tuple is called a *solution* of the statement.
- In formal mathematics, 'true' means 'provable'.

2.2 Recipe Notation for Rules of Inference

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

Show: P_1
$\vdots$
Show: P_k
Conclude: Q_1
$\vdots$
Conclude: Q_n

Additionally if a premise is of the form $P \vdash Q$, we call P an *assumption*. We denote this in recipe notation by as an indented 'assume-block' as illustrated below.

Example 6. Suppose we have the following rule of inference.

$$(\varphi \vdash \psi), (\psi \vdash \varphi) \vdash (\varphi \Leftrightarrow \psi)$$

Then we would express this in recipe notation as

Assume φ
Show ψ
$\leftarrow$
Assume ψ
Show φ
$\leftarrow$
Conclude $\varphi \Leftrightarrow \psi$

In this, everything between an *Assume* and the following $\leftarrow$ (the 'end assumption' symbol) is a *subproof* that shows 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 do not need to be justified by a rule of inference.

3 Propositional Logic

3.1 The Language of Propositional Logic

Definition 7. Let P, Q be statements. Then the five expressions "$\neg P$", "P and Q", "P or Q", "$P \Rightarrow Q$", and "$P \Leftrightarrow Q$" are also statements whose truth values are completely determined by the truth values of P and Q as shown in the following table:

P	Q	not P	P and Q	P or Q	$P \Rightarrow Q$	$P \Leftrightarrow Q$
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

Definition 8. The language $\mathcal{L}$, of Propositional Logic consists 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 elements of $\mathcal{L}$.

3.2 Natural Deduction

Rules of Inference for Propositional Logic

and +	and −
Show: W Show: V Conclude: W and V	Show: W and V Conclude: W Conclude: V
$\Rightarrow$ +	$\Rightarrow$ − (modus ponens)
Assume W Show: V ← Conclude: $W \Rightarrow V$	Show: W Show: $W \Rightarrow V$ Conclude: V
$\Leftrightarrow$ +	$\Leftrightarrow$ −
Show: $W \Rightarrow V$ Show: $V \Rightarrow W$ Conclude: $W \Leftrightarrow V$	Show: $W \Leftrightarrow V$ Conclude: $W \Rightarrow V$ Conclude: $V \Rightarrow W$
or +	or − (proof by cases)
Show: W Conclude: W or V Conclude: V or W	Show: W or V Show: $W \Rightarrow U$ Show: $V \Rightarrow U$ Conclude: U
not + (proof by contradiction)	not − (proof by contradiction)
Assume W Show: →← ← Conclude: not W	*Assume* not W Show: →← ← Conclude: W

Rules of Inference for Propositional Logic

→← +	
Show: W Show: not W Conclude: →←	

Remarks:

- The symbol ← is an abbreviation for "end assumption".
- The symbol →← is called "contradiction" and represents the logical constant FALSE.
- The italicized word *Assume* is actually entered as part of the proof itself, not just instructions in the recipe like the words '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 reason however, to insert such statements unless you intend to use one of the rules of inference that requires them as inputs.
- 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.

4 Predicate Logic

4.1 Quantifiers

Definition 9. The symbols ∀ and ∃ are *quantifiers*. The symbol ∀ is called "for all", "for every", or "for each". The symbol ∃ is called "for some" or "there exists".

Definition 10. If x is a variable, t an expression, and $W(x)$ a statement then $W(t)$ is the statement obtained by replacing every free occurance of x in $W(x)$ with t.

Definition 11. If W is a statement and x is any variable then $\forall x, W$ and $\exists x, W$ are both statements. The rules of inference for these quantifiers are given in the following table.

Rules of Inference for Quantifiers*

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

**Restrictions:*

- 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. One consequence of this is that the declaration of s in the ∀+ rule must come before proving $W(s)$.
- In ∀− and ∃+, no free variable in t may become bound when t is substituted for x in $W(x)$.
- 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.
- In ∃−, c must be a new constant in the proof. Also $W(c)$ must immediately follow the constant declaration for c in the proof.

Definition 12. Let $W(x)$ be a statement and $W(y)$ the statement obtained by replacing every free occurrence of x in $W(x)$ with 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*

∃!+	∃!−
Show: $\exists x, W(x)$ and $\forall y, W(y) \Rightarrow y = x$ Conclude: $\exists! x, W(x)$	Show: $\exists! x, W(x)$ Conclude: $\exists x, W(x)$ and $\forall y, W(y) \Rightarrow y = x$

4.1.1 Equality

Definition: The equality symbol, =, is defined by the two rules of inference given as follows.

Rules of Inference for Equality

Reflexivity of =	Substitution*
Conclude: $x = x$	Show: $x = y$ Show: W Conclude: W with the *nth* free occurrence of x replaced by y.

**Restriction:* No free variable in y may become bound when y is substituted for x in W.

Note. 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.

Precedence: Quantifiers have a lower precedence than $\Leftrightarrow$. Thus they quantify the largest statement to their right possible unless specifically limited by parentheses. In order to eliminate parentheses we give the operators the following precedence (from highest to lowest):

Precedence of Logical Operators
other math operators ($+, =, \cdot, \cup, -$, etc.)
not
and , or
$\Rightarrow$
$\Leftrightarrow$
$\forall, \exists, \exists!$

Example 13. 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 "$\forall x, L(x, \text{Bob})$".

1. Alice loves everyone.
2. Someone loves Alice.
3. Bob loves Alice, but she does not love him.
4. Everyone loves someone.
5. There is only one person who loves everyone.
6. Someone loves everyone.
7. There is a person who is loved by only one person.
8. Some people do not love themselves.
9. Some people only love themselves.
10. Nobody loves everybody.
11. If everyone loves themselves, then everyone loves someone.
12. 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 Proof Shortcuts

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 document we 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.

5.1 Use Theorems as Rules of Inference

Once we have proved a theorem we can use it to make new Rules 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 14. $P \Rightarrow P$

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

`12.` $P \Rightarrow P$ `by Theorem 14.`

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.

5.2 Expand Theorems to Derive Rules of Inference

A more advanced way to avoid tedious repetitive steps of logic is to derive rules of inference from a theorem. 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
Conclude: $P \Rightarrow Q$

we obtain a new rule

some famous implication
Show P Conclude: Q

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*
Show: P Conclude: Q	Show: Q Conclude: P

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.

If the ROI has:	Replace that with:
Show: P and Q	Show: P Show: Q
Show: $P \Rightarrow Q$	*Assume* P Show: Q $\leftarrow$

If the ROI has:	Replace that with:
Show: $P \Leftrightarrow Q$	*Assume* P Show: Q $\leftarrow$ *Assume* Q Show: P $\leftarrow$
Show: $\forall x, P(x)$	*Let* s *be arbitrary.* Show: $P(s)$ $\leftarrow$
Conclude: $P \Rightarrow Q$	Show: P Conclude: Q
Conclude: $P \Leftrightarrow Q$	Show: P Conclude: Q Show: Q Conclude: P
Conclude P and Q	Conclude P Conclude Q
Conclude $\forall x, P(x)$	Conclude $P(z)$
Conclude $\exists x, P(x)$	*For some constant* c*,* Conclude $P(c)$ **these lines must be consecutive in the proof*

Similarly if we have a Show P in our ROI for which P is the conclusion of a previously expanded ROI, 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.

5.3 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 $\neg\neg\neg(y = x)$.

5.4 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 semi-formal proof). Since most of these are equivalences, they are frequently useful when combined with the previous shortcut.

Theorems of Logic	
excluded middle	P or not 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 $Q(x))$
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	$(P \Rightarrow Q) \Leftrightarrow$ (not P or Q)
alternate or-	$(P$ or $Q)$ and not $P \Rightarrow Q$ $(P$ or $Q)$ and not $Q \Rightarrow P$
not implies	not $(P \Rightarrow Q) \Leftrightarrow (P$ and not $Q)$
contrapositive	$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

Theorems of Logic (cont.)	
DeMorgan's Law	$\neg(P \text{ and } Q) \Leftrightarrow (\neg P \text{ or } \neg Q)$ $\neg(P \text{ or } Q) \Leftrightarrow (\neg P \text{ and } \neg Q)$ $(\neg\forall x, P(x)) \Leftrightarrow \exists x, \neg P(x)$ $(\neg\exists x, P(x)) \Leftrightarrow \forall x, \neg P(x)$
contradiction	$\rightarrow\leftarrow \Rightarrow Q$
alternate substitution	$x = y$ and $W \Rightarrow W$ with the nth free occurrence of y replaced by x.
alternate $\exists!$	$(\exists! x, W(x)) \Leftrightarrow \exists c, \forall z, W(z) \Leftrightarrow z = c$

5.5 Identify Certain Statements

In some cases even using Shortcut 5.3 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) ⇒ 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
P or Q	Q or P
$P \Leftrightarrow Q$	$Q \Leftrightarrow P$
$x = y$	$y = x$
$\neg\neg P$	P

5.6 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 '∧ and +' or '∧ and −' rules by allowing P and Q to be used as a premise whenever P or Q are required, e.g.,

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

Similar shortcuts can be used to avoid '∧ and +', e.g.,

	⋮	
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
	⋮	

Notice that in this case we can specify three premises even though the '⇒ +' 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 '∧ and −' rule.

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

Example 15. Suppose we have a theorem in this form (for some appropriate P and Q).

Theorem 16. $P \Leftrightarrow Q$

Then we will frequently abbreviate the proof like this.

Proof

(⇒)		
1.	Assume P	-
⋮	⋮	⋮
11.	Q	for some reason
12.	←	-
(⇐)		

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.

5.7 Sometimes skip the last line of the proof

Frequently when we write a proof is immediately follows the statement of the theorem being proved. Since the last line of the proof should be the statement of the theorem itself, it can frequently be omitted because the reader can refer to the theorem statement itself as long as the reason for the final statement would be obvious. (If not, then the reason should be stated even if it is in the form "Thus, the desired result follows by such-and-such a reason."

Some authors also omit any premises given in a theorem that is stated in the form $P_1, \ldots, P_n \vdash Q$ for a similar reason. While this is common practice in mathematics, we don't recommend it as it makes it more difficult to cite the premises when necessary, and can frequently make the proof more difficult for the reader to follow.

5.8 Eliminate extra parentheses for associative binary operators

A special case of Shortcut 5.5 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

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

5.9 Omit Most References to Premises and Line Labels

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 $a \to b$ reader.

5.10 Use the abbreviations for quantifying over a type

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 ∃− ; 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 "$\exists x_0, \exists x_1, \ldots \exists x_n, P(x_0, \ldots, x_n)$".

5.11 Use the shorthand notation $\{E(x_0, \ldots, x_n) : P(x_0, \ldots, x_n)\}$

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 17. 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
	⋮	⋮

5.12 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

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

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 18. 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 Sets, Functions, Numbers

6.1 Basic Definitions from Set theory

The symbol $\in$ is formally undefined, but it means "is an element of". The expression $x \in A$ is a statement that is true if and only if A is a set and x is an element of A. The constant $\varnothing$ is set called the empty set. Many of the definitions below are informal definitions that are sufficient for our purposes.

Basic set notation and operations

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 $\notin$:	$x \notin A \Leftrightarrow \neg (x \in A)$
Empty set:	$A = \varnothing \Leftrightarrow \forall x, x \notin A$
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:	$x \in \overline{A} \Leftrightarrow x \notin A$
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 $P(x)$

Remark: Each such definition can be used as a line in a proof directly, with any of the free variables replaced by any expression of the same type. As such, each represents a rule of inference with no inputs and only the entire definition as a conclusion. However, in practice, it is usually quite useful to use rules of inference that are derived from these definitions. Some of the more useful ones are listed in the following table.

Rules of Inference for Basic Set Theory

Finite set notation+	Finite set notation−
Conclude: $x_k \in \{x_1, \ldots, x_n\}$ (where x_k is one of $x_1, \ldots, x_n$)	Show: $x \in \{x_1, \ldots, x_n\}$ Conclude: $x = x_1$ or $x = x_2$ or $\cdots$ or $x = x_n$
Set builder+	**Set builder−**
Show: $P(x)$ Conclude: $x \in \{y : P(y)\}$	Show: $x \in \{\, y : P(y) \,\}$ Conclude: $P(x)$
Subset+	**Subset−**
Let $x \in A$ Show: $x \in B$ $\leftarrow$ Conclude: $A \subseteq B$	Show: $A \subseteq B$ Show: $x \in A$ Conclude: $x \in B$
Set equality+	**Set equality−**
Let $x \in A$ Show: $x \in B$ $\leftarrow$ *Let* $y \in B$ Show: $y \in A$ $\leftarrow$ Conclude: $A = B$	(see Substitution Rule)
Not an element of+	**Not an element of−**
Show: not $x \in A$ Conclude: $x \notin A$	Show: $x \notin A$ Conclude: not $x \in A$
Empty Set+	**Empty Set−**
Let x be arbitrary Show: $x \notin A$ $\leftarrow$ Conclude: $A = \varnothing$	Conclude: $x \notin \varnothing$
Power Set+	**Power Set−**
Show: $B \subseteq A$ Conclude: $B \in \mathcal{P}(A)$	Show: $B \in \mathcal{P}(A)$ Conclude: $B \subseteq A$
Intersection+	**Intersection−**
Show: $x \in A$ Show: $x \in B$ Conclude: $x \in A \cap B$	Show: $x \in A \cap B$ Conclude: $x \in A$ Conclude: $x \in B$

Rules of Inference for Basic Set Theory

Union+	Union−
Show: $x \in A$ Conclude: $x \in A \cup B$ Conclude: $x \in B \cup A$	Show: $x \in A \cup B$ Conclude: $x \in A$ or $x \in B$
Relative Complement+	**Relative Complement−**
Show: $x \in B$ Show: $x \notin A$ Conclude: $x \in B - A$	Show: $x \in B - A$ Conclude: $x \in B$ Conclude: $x \notin A$
Complement+	**Complement−**
Show: $x \notin A$ Conclude: $x \in \overline{A}$	Show: $x \in \overline{A}$ Conclude: $x \notin A$
Indexed Intersection+	**Indexed Intersection−**
Let $k \in I$ Show: $x \in A_k$ $\leftarrow$ Conclude: $x \in \bigcap_{i \in I} A_i$	Show: $x \in \bigcap_{i \in I} A_i$ Show: $k \in I$ Conclude: $x \in A_k$
Indexed Union+	**Indexed Union−**
Show: $\exists k \in I, x \in A_k$ Conclude: $x \in \bigcup_{i \in I} A_i$	Show: $x \in \bigcup_{i \in I} A_i$ *For some* $k \in I$, Conclude: $x \in A_k$

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. See the Section 5 above for details.
- Usually we just use $x \notin A$ and not $x \in A$ interchangeably in our proofs without invoking the "Not an element of" rules.

6.1.1 Cartesian products

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:	$A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$
Cartesian Product:	$A_1 \times \cdots \times A_n = \{(x_1, \ldots, x_n) : x_1 \in A_1 \text{ and } \cdots \text{ and } x_n \in A_n\}$
Power of a Set	$A^n = A \times A \times \cdots \times A$ where there are n "A's" in the Cartesian product

Remark: Each such definition can be used as a line in a proof directly, with any of the free variables replaced by any expression of the same type. As such, each represents a rule of inference with no inputs and only the entire definition as a conclusion. However, in practice, it is usually quite useful to use rules of inference that are derived from these definitions. Some of the more useful ones are listed in the following table.

Rules of Inference for Cartesian Products

Ordered pair+	Ordered pair−
Show: $x = u$ Show: $y = v$ Conclude: $(x, y) = (u, v)$	Show: $(x, y) = (u, v)$ Conclude: $x = u$ Conclude: $y = v$
Ordered n-tuple+	**Ordered n-tuple−**
Let $k \in \{1, 2, \ldots, n\}$ Show: $x_k = y_k$ ← Conclude: $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$	Show: $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ Show: $k \in \{1, 2, \ldots, n\}$ Conclude: $x_k = y_k$
Cartesian Product+	**Cartesian Product−**
Show: $x \in A$ Show: $y \in B$ Conclude: $(x, y) \in A \times B$	Show: $z \in A \times B$ *For some* $x \in A$ *and some* $y \in B$, Conclude: $z = (x, y)$
Cartesian Product+(n sets)	**Cartesian Product−(n sets)**
Let $k \in \{1, 2, \ldots, n\}$ Show: $x_k \in A_k$ ← Conclude: $(x_1, \ldots, x_n) \in A_1 \times A_2 \times \cdots \times A_n$	Show: $z \in A_1 \times A_2 \times \cdots \times A_n$ *For some* $x_1 \in A_1$,$x_2 \in A_2$,...,$x_n \in A_n$, Conclude: $z = (x_1, \ldots, x_n)$
Power of a set+	**Power of a Set−**
Let $k \in \{1, 2, \ldots, n\}$ Show: $x_k \in A$ ← Conclude: $(x_1, \ldots, x_n) \in A^n$	Show: $z \in A^n$ *For some* $x_1, \ldots, x_n \in A_n$, Conclude: $z = (x_1, \ldots, x_n)$

Remark: 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.

6.2 Functions

In the following definitions, A,B,C,S are sets and f, g, h are functions (except in the definition of function, where f is only assumed to be a set),

Def of function:	$f : A \to B \Leftrightarrow f \subseteq A \times B$ and $(\forall x, \exists! y, (x, y) \in f)$
Alt. function notation	$X \xrightarrow{f} Y \Leftrightarrow f : X \to Y$
Def of $f(x)$:	$f(x) = y \Leftrightarrow (x, y) \in f$
Domain & Codomain:	$\text{Domain}(f) = A$ and $\text{Codomain}(f) = B \Leftrightarrow f : A \to B$
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 $f \circ f^{-1} = id_B$ and $f^{-1} \circ f = id_A$
Inverse Image:	$f : A \to B$ and $S \subseteq B \Rightarrow f^{\text{inv}}(S) = \{x \in A : f(x) \in S\}$

Remark: Each such definition can be used as a line in a proof directly, with any of the free variables replaced by any expression of the same type. As such, each represents a rule of inference with no inputs and only the entire definition as a conclusion. However, in practice, it is usually quite useful to use rules of inference that are derived from these definitions. Some of the more useful ones are listed in the following table.

Rules of Inference for Functions

Function +	Function−
Show: $f \subseteq A \times B$	Show: $f : A \to B$
Let $x \in A$	Show $x \in A$
Show: $\exists! y \in B, (x, y) \in f$	Conclude: $f \subseteq A \times B$
Conclude: $f : A \to B$	Conclude: $\exists! y \in B, (x, y) \in f$

Rules of Inference for Functions

Function application+	Function application−
Show: $f : A \to B$ Show: $(x, y) \in f$ Conclude: $f(x) = y$	Show: $f : A \to B$ Show: $y = f(x)$ Conclude: $(x, y) \in f$
Domain and Codomain+	**Domain and Codomain−**
Show: $f : A \to B$ Conclude: Domain $(f) = A$ Conclude: Codomain $(f) = B$	Show: Domain $(f) = A$ Show: Codomain $(f) = B$ Conclude: $f : A \to B$
Function equality+	**Function equality−**
Show: $f : A \to B$ Show: $g : A \to B$ *Let* $x \in A$ Show: $f(x) = g(x)$ Conclude: $f = g$	(see Substitution Rule)
Image+	**Image−**
Show: $\exists x \in S, y = f(x)$ Conclude: $y \in f(S)$	Show: $y \in f(S)$ *For some* $x \in S$ Conclude: $y = f(x)$
Range+	**Range−**
Show: $y = f(x)$ Conclude: $y \in \text{Range}(f)$	Show: $f : A \to B$ Show: $y \in \text{Range}(f)$ *For some* $x \in A$ Conclude: $y = f(x)$
Identity map+	**Identity map−**
Show: $f : A \to A$ *Let* $x \in A$ Show: $f(x) = x$ Conclude: $f = \text{id}_A$	Conclude: $\text{id}_A(x) = x$
Composition+	**Composition−**
Show: $f : A \to B$ Show: $g : B \to C$ Conclude: $(g \circ f) : A \to C$ Conclude: $(g \circ f)(x) = g(f(x))$	Show: $h = (g \circ f)$ Conclude: $h(x) = g(f(x))$ Conclude: Domain $(h) =$ Domain (f) Conclude: Codomain $(h) =$ Codomain (g)

Rules of Inference for Functions

Injective+	Injective−

Show: $f : A \to B$
Let $x, y \in A$
  Assume $f(x) = f(y)$
  Show: $x = y$
  $\leftarrow$
Conclude: f *is injective*
	Show: f *is injective*
	Show: $f(x) = f(y)$
	Conclude: $x = y$

Surjective+	**Surjective−**
Show: $f : A \to B$ *Let* $y \in B$ Show: $x \in A$ Show: $y = f(x)$ Conclude: f is *surjective*	Show: $f : A \to B$ *is surjective* Show: $y \in B$ *For some* $x \in A$ Conclude: $y = f(x)$
Bijective+	**Bijective−**
Show: f *is injective* Show: f *is surjective* Conclude: f *is bijective*	Show: f *is bijective* Conclude: f *is injective* Conclude: f *is surjective*
Inverse function+	**Inverse function−**
Show: $f : A \to B$ Show: $g : B \to A$ Show: $g \circ f = \mathrm{id}_A$ Show: $f \circ g = \mathrm{id}_B$ Conclude: $g = f^{-1}$	Show: $f : A \to B$ Show: f *is bijective* Conclude: $f^{-1} : B \to A$ Conclude: $f^{-1}(f(x)) = x$ Conclude: $f\left(f^{-1}(y)\right) = y$
Inverse image+	**Inverse image−**
Show: $f(x) \in T$ Conclude: $x \in f^{\mathrm{inv}}(T)$	Show: $x \in f^{\mathrm{inv}}(T)$ Conclude: $f(x) \in T$

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

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

6.3 Famous Sets of Numbers

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	$\mathbb{Q} = \left\{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}, b > 0, \text{ and } \gcd(a, b) = 1\right\}$
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	$A^+ = A \cap \mathbb{R}^+$
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 $a, b \in \mathbb{Z}$ you can say that $a \cdot b \in \mathbb{Z}$ 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.

6.4 Algebra

These are properties that addition and multiplication operations may have.

additive identity	$x + 0 = x$ and $0 + x = x$
multiplicative identity	$1 \cdot x = x$ and $x \cdot 1 = x$
commutativity of $+$	$x + y = y + x$
commutativity of $\cdot$	$x \cdot y = y \cdot x$
associativity of $+$	$(x + y) + z = x + (y + z)$
associativity of $\cdot$	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
distributive laws	$x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$
additive inverse	$x + (-x) = 0$ and $(-x) + x = 0$
multiplicative inverse	x is invertible $\Rightarrow x \cdot \left(\frac{1}{x}\right) = 1$ and $\left(\frac{1}{x}\right) \cdot x = 1$
subtraction	$x - y = x + (-y)$
division	y is invertible $\Rightarrow \frac{x}{y} = x \cdot \left(\frac{1}{y}\right)$
definition of squaring	$x^2 = x \cdot x$

6.5 Inequalities

The following define some properties an order relation $<$ can have on a particular set. In particular, these hold for real numbers x, y. Note that we can compare the order of numerical constants using the reason *by arithmetic*. For example, we can say that $-2 < 3/5$ by arithmetic.

trichotomy	$(x = 0$ or $x < 0$ or $0 < x)$ and $x = 0 \Rightarrow$ not $x < 0$ and not $0 < x$ and $0 < x \Rightarrow$ not $x = 0$ and not $x < 0$ and $x < 0 \Rightarrow$ not $x = 0$ and not $0 < x$
transitivity	$x < y$ and $y < z \Rightarrow x < z$
translation	$x < y \Rightarrow x + z < y + z$
scaling	$0 < z$ and $x < y \Rightarrow x \cdot z < y \cdot z$
definition of $>$	$x > y \Leftrightarrow y < x$
definition of $\leq$	$x \leq y \Leftrightarrow x < y$ or $x = y$
definition of $\geq$	$x \geq y \Leftrightarrow x > y$ or $x = y$
positive	x is positive $\Leftrightarrow 0 < x$
negative	x is negative $\Leftrightarrow x < 0$
nonnegative	x is nonnegative $\Leftrightarrow 0 \leq x$

6.6 Relations

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 $yRz \Rightarrow xRz$
Nonreflexive relation:	$R \subseteq A \times A$ is nonreflexive$\Leftrightarrow \forall x \in A,$ not 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 nonreflexive, 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 $A \Leftrightarrow (\forall S \in P, S \neq \varnothing$ and $S \subseteq A)$ and $A = \bigcup_{S \in P} S$ and $\forall S \in P, \forall T \in P, S = T$ or $S \cap T = \varnothing$

Remark: Each such definition can be used as a line in a proof directly, with any of the free variables replaced by any expression of the same type. As such, each represents a rule of inference with no inputs and only the entire definition as a conclusion. However, in practice, it is usually quite useful to use rules of inference that are derived from these definitions. Some of the more useful ones are listed in the following table.

Rules of Inference for Relations

Not equal+	Not an element of−
Show: not $x = y$ Conclude: $x \neq y$	Show: $x \neq y$ Conclude: not $x = y$

Rules of Inference for Relations

Relation+	Relation−
Show: $R \subseteq A \times B$ Conclude: *R is a relation from A to B*	Show: *R is a relation from A to B* Conclude: $R \subseteq A \times B$
Relation on a set+	**Relation on a set−**
Show: $R \subseteq A \times A$ Conclude: *R is a relation on A*	Show: *R is a relation on A* Conclude: $R \subseteq A \times A$
Reflexive+	**Reflexive−**
Let $x \in A$ Show: xRx Conclude: *R is reflexive*	Show: *R is reflexive* Conclude: xRx
Symmetric+	**Symmetric−**
Let $x, y \in A$ *Assume* xRy Show: yRx ← Conclude: *R is symmetric*	Show: *R is symmetric* Show: xRy Conclude: yRx
Transitive+	**Transitive−**
Let $x, y, z \in A$ *Assume* xRy and yRz Show: xRz ← Conclude: *R is transitive*	Show: *R is transitive* Show: xRy Show: yRz Conclude: xRz
Nonreflexive+	**Nonreflexive−**
Let $x \in A$ Show: not xRx Conclude: *R is nonreflexive*	Show: *R is nonreflexive* Conclude: not xRx
Antisymmetric+	**Antisymmetric−**
Let $x, y \in A$ *Assume* xRy and yRx Show: $x = y$ ← Conclude: *R is antisymmetric*	Show: *R is antisymmetric* Show: xRy Show: $x \neq y$ Conclude: not yRx OR Show: *R is antisymmetric* Show: xRy Conclude: $x = y$ or not yRx

Rules of Inference for Relations

Total relation+	Total relation−
Let $x, y \in A$ Show: xRy or yRx Conclude: *R is total*	Show: *R is total* Conclude: xRy or yRx
Partial order+	**Partial order−**
Show: *R is reflexive* Show: *R is antisymmetric* Show: *R is transitive* Conclude: *R is a partial order*	Show: *R is a partial order* Conclude: *R is reflexive* Conclude: *R is antisymmetric* Conclude: *R is transitive*
Strict partial order+	**Strict partial order−**
Show: *R is nonreflexive* Show: *R is antisymmetric* Show: *R is transitive* Conclude: *R is a strict partial order*	Show: *R is a strict partial order* Conclude: *R is nonreflexive* Conclude: *R is antisymmetric* Conclude: *R is transitive*
Total order+	**Total order−**
Show: *R is antisymmetric* Show: *R is transitive* Show: *R is total* Conclude: *R is a total order*	Show: *R is a total order* Conclude: *R is antisymmetric* Conclude: *R is transitive* Conclude: *R is total*
Equivalence relation+	**Equivalence relation−**
Show: *R is reflexive* Show: *R is symmetric* Show: *R is transitive* Conclude: *R is an equivalence relation*	Show: *R is an equivalence relation* Conclude: *R is reflexive* Conclude: *R is symmetric* Conclude: *R is transitive*
Equivalence class+	**Equivalence class−**
Show: xRa Conclude: $x \in [a]_R$	Show: $x \in [a]_R$ Conclude: xRa
Partition+	**Partition−**
Let $S, T \in P$ Show: $S \neq \emptyset$ Show: $S \subseteq A$ *Let* $x \in A$ Show: $\exists U \in P, x \in U$ *Assume* $x \in S$ and $x \in T$ Show: $S = T$ $\leftarrow$ Conclude: *P is a partition of A*	Show: *P is a partition of A* Show: $S, T \in P$ Conclude: $S \neq \emptyset$ Conclude: $S \subseteq A$ Conclude: $S \cap T = \emptyset$ or $S = T$ OR Show: *P is a partition of A* Show: $x \in A$ Conclude: $x \in S$ *for some* $S \in P$

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

$$\forall a, b \in A, [a] = [b] \text{ or } [a] \cap [b] = \varnothing.$$

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 $\forall x, y \in A, xRy \Leftrightarrow \exists S \in P, x \in S$ and $y \in S$.

7 Number Theory and Induction

7.1 The Peano Postulates

It is possible to define addition, multiplication, and $<$ for the Natural Numbers from scratch without referring to the rule '*by arithmetic*'. One famous way of doing that is with the following axioms which were developed by Giuseppe Peano at the end of the 19th century.

Axiom Name	Definition
N0	$0 \in \mathbb{N}$
N1	$\forall n, \sigma(n) \in \mathbb{N}$
N2	$\forall n, \forall m, \sigma(n) = \sigma(m) \Rightarrow m = n$
N3	$\forall n, 0 \neq \sigma(n)$
N4	$P(0)$ and $(\forall k \in \mathbb{N}, P(k) \Rightarrow P(\sigma(k))) \Rightarrow \forall n \in \mathbb{N}, P(n)$
A0	$\forall n, n + 0 = n$
A1	$\forall n, \forall m, m + \sigma(n) = \sigma(m + n)$
M0	$\forall n, n \cdot 0 = 0$
M1	$\forall n, \forall m, m \cdot \sigma(n) = m + m \cdot n$
I	$\forall n, \forall m, m \leq n \Leftrightarrow \exists k, m + k = n$

In N4 above and in the following, let $P(n)$ be a statement about a natural number variable n. Axiom N4 is called *mathematical induction*, or simply *induction*.

7.2 Equivalent forms of Induction

There are several useful statements that are equivalent to Axiom N4 and can be used interchangeably with N4 to justify a line in a proof by induction.

Theorem 19. *Let $P(n)$ be a statement about an arbitrary natural number n, and $a \in \mathbb{N}$. The following are equivalent.*

a) ***(Induction)*** $P(0)$ and $(\forall k \in \mathbb{N}, P(k) \Rightarrow P(k+1)) \Rightarrow \forall n \in \mathbb{N}, P(n)$

b) ***(Induction from a)*** $P(a)$ and $(\forall k \geq a, P(k) \Rightarrow P(k+1)) \Rightarrow \forall n \geq a, P(n)$

c) ***(Strong Induction)*** $P(0)$ and $(\forall k \in \mathbb{N}, (\forall j \leq k, P(j)) \Rightarrow P(k+1)) \Rightarrow \forall n \in \mathbb{N}, P(n)$

d) ***(Strong Induction from a)*** $P(a)$ and $(\forall k \geq a, (\forall a \leq j \leq k, P(j)) \Rightarrow P(k+1)) \Rightarrow \forall n \geq a, P(n)$

Remark: Since statements #2-4 are equivalent to #1 and statement #1 is an axiom, all four statements can be used as a rule of inference. As usual, each such definition can be used as a line in a proof directly, with any of the free variables replaced by any expression of the same type. As such, each represents a rule of inference with no inputs and only the entire definition as a conclusion. However, in practice, it is usually quite useful to use rules of inference that are derived from these statement. Some useful ones are listed in the following table.

Rules of Inference for Proof by Induction

Induction	Induction from a
Show: $P(0)$ *Let* $k \in \mathbb{N}$ *Assume* $P(k)$ Show: $P(k+1)$ $\leftarrow$ Conclude: $\forall n \in \mathbb{N}, P(n)$	Show: $P(a)$ *Let* $k \in \mathbb{N}$ and $a \leq k$ *Assume* $P(k)$ Show: $P(k+1)$ $\leftarrow$ Conclude: $\forall n \geq a, P(n)$
Strong Induction	**Strong Induction from a**
Show: $P(0)$ *Let* $k \in \mathbb{N}$ *Assume* $\forall j \leq k, P(j)$ Show: $P(k+1)$ $\leftarrow$ Conclude: $\forall n \in \mathbb{N}, P(n)$	Show: $P(a)$ *Let* $k \in \mathbb{N}$ and $a \leq k$ *Assume* $\forall a \leq j \leq k, P(j)$ Show: $P(k+1)$ $\leftarrow$ Conclude: $\forall n \geq a, P(n)$

7.3 Arithmetic and Algebra

While it is possible to prove all of the usual properties of the natural numbers and the arithmetic operations of addition, subtraction, multiplication, division, and exponentiation, such a detailed study is more appropriate in a full course on Number Theory. The same is true for elementary algebra. Thus unless specified otherwise, we will allow the following two shortcut rules of inference.

By Arithmetic. For our purposes we will assume that the basic facts about the arithmetic of real or integer constants that we know from elementary school are valid and may be used in a proof. Thus we can make statements in our proof like "$2 + 2 = 4$" or "$-3 < 2$" and for the reason use "by arithmetic" with no inputs.

By Algebra. We will also assume the basic facts about the algebra of real numbers such as associativity, commutativity, distributivity, identity, inverse laws, and properties of signs and exponents. Thus we can use statements about real numbers or integers like "$x^2 - 1 = (x + 1)(x - 1)$" and for the reason use "by algebra".

7.4 Recursive definitions and Sequences

A function from $\mathbb{N}$ to some other set (or $\mathbb{N}^+$) is frequently referred to as an *infinite sequence*. 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 first, and then the rest are defined in terms of previously defined objects of the same kind. Here are some common examples of recursive definitions in mathematics.

One convenient way to write such definitions is to us *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 $\neg(P_1 \text{ or } P_2 \text{ or } \cdots \text{ or } P_{k-1})$. The entire equation given in (1) is an abbreviation for the statement

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

In the following table, f is a function from $\mathbb{N}$ (or $\mathbb{N}^+$) to some other set, n, a, b are natural numbers, and z is anything which can be multiplied by itself.

Some Recursive Defintions and Sequences	
Sequence notation:	$f_n = f(n)$
Natural Powers:	$z^n = \begin{cases} 1 & \text{if } n = 0 \\ z \cdot z^{n-1} & \text{otherwise} \end{cases}$
Factorial:	$n! = \begin{cases} 1 & \text{if } n = 0 \\ n \cdot (n-1)! & \text{otherwise} \end{cases}$
Summation:	$\sum_{n=a}^{b} f(n) = \begin{cases} 0 & \text{if } b < a \\ f(b) + \sum_{n=a}^{b-1} f(n) & \text{otherwise} \end{cases}$

7.5 Quotient, Remainder, Divisibility, and Mod

Here are some useful theorems and definitions about integers. In the following all single letter variables have type *natural number* unless otherwise specified.

Division Algorithm:	$\forall a, \forall b \neq 0, \exists! q, \exists! r, a = qb + r$ 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:	$\forall a, b \in \mathbb{Z}, a \mid b \Leftrightarrow \exists q \in \mathbb{Z}, b = qa$
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 $\forall a > 0, a \mid p \Rightarrow a = 1$ or $a = p$
Composite:	n is composite $\Leftrightarrow \exists a, a \mid n$ and $1 < a < n$
Congruent mod m:	$\forall a, b \in \mathbb{Z}, a \underset{m}{\equiv} b \Leftrightarrow m \mid (a - b)$
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 $\Leftrightarrow \gcd(a, b) = 1$

Remarks: It is also possible to define prime and composite for negative integers by removing the restriction that they be positive from their respective definitions.

As usual, each such definition can be used as a line in a proof directly, with any of the free variables replaced by any expression of the same type. As such, each represents a rule of inference with no inputs and only the entire definition as a conclusion. However, in practice, it is usually quite useful to use rules of inference that are derived from these definitions. Some of the more useful ones are listed in the following table.

Rules of Inference for Divisibility

Division Algorithm (existence)	Division Algorithm (uniqueness)
Show: $b \neq 0$ Conclude: $a = qb + r$ for some $q \in \mathbb{Z}$ and some $0 \leq r < b$	Show: $b \neq 0$ Show: $a = qb + r$ Show: $0 \leq r < b$ Conclude: $q = (a \operatorname{quo} b)$ Conclude: $r = (a \bmod b)$
Quotient	**Remainder**
Show: $q = (a \operatorname{quo} b)$ Conclude: $a = qb + r$ for some $0 \leq r < b$	Show: $r = (a \bmod b)$ Conclude: $a = qb + r$ for some q
Divides+	**Divides−**
Show: $b = aq$ Show: $q \in \mathbb{Z}$ Conclude: $a \mid b$	Show: $a \mid b$ Conclude: $b = aq$ for some $q \in \mathbb{Z}$
Divisor+	**Divisor−**
Show: $b = aq$ Show: $q \in \mathbb{Z}$ Conclude: a is a divisor of b	Show: a is a divisor of b Conclude: $b = aq$ for some $q \in \mathbb{Z}$
Prime+	**Prime−**
Show: $p > 1$ *Let* $a > 0$ *Assume* $a \mid p$ Show: $a = 1$ or $a = p$ $\leftarrow$ Conclude: p is prime	Show: p is prime Show: $a > 0$ Show: $a \mid p$ Conclude: $a = 1$ or $a = p$
Composite+	**Composite−**
Show:n>0 Show: $n = ab$ Show: $1 < a < n$ Conclude: n is composite	Show: n is composite Conclude:n>0 Conclude: $n = ab$ for some $1 < a, b < n$
Congruent mod m+	**Congruent mod m−**
Show: $m \mid a - b$ Conclude: $a \underset{m}{\equiv} b$	Show: $a \underset{m}{\equiv} b$ Conclude: $m \mid a - b$
gcd+	**gcd−**

Rules of Inference for Divisibility

Show: $d > 0$
Show: $d \mid a$
Show: $d \mid b$
Let $c > 0$
    Assume $c \mid a$ and $c \mid b$
    Show: $c \leq d$
    ←
Conclude: $d = \gcd(a, b)$

Show: $d = \gcd(a, b)$
Conclude: $d > 0$
Conclude: $d \mid a$
Conclude: $d \mid b$
Conclude: $\forall c > 0, c \mid a$ and $c \mid b \Rightarrow c \leq d$

gcd+(alt)

Show: $d > 0$
Show: $d \mid a$
Show: $d \mid b$
Let $c > 0$
    Assume $c \mid a$ and $c \mid b$
    Show: $c \mid d$
    ←
Conclude: $d = \gcd(a, b)$

gcd−(alt)

Show: $d = \gcd(a, b)$
Conclude: $d > 0$
Conclude: $d \mid a$
Conclude: $d \mid b$
Conclude: $\forall c > 0, c \mid a$ and $c \mid b \Rightarrow c \mid d$

lcm+

Show: $d > 0$
Show: $a \mid d$
Show: $b \mid d$
Let $c > 0$
    Assume $a \mid c$ and $b \mid c$
    Show: $d \leq c$
    ←
Conclude: $d = \text{lcm}(a, b)$

lcm−

Show: $d = \text{lcm}(a, b)$
Conclude: $d > 0$
Conclude: $a \mid d$
Conclude: $b \mid d$
Conclude: $\forall c > 0, a \mid c$ and $b \mid c \Rightarrow d \leq c$

lcm+(alt)

Show: $d > 0$
Show: $a \mid d$
Show: $b \mid d$
Let $c > 0$
    Assume $a \mid c$ and $b \mid c$
    Show: $d \mid c$
    ←
Conclude: $d = \text{lcm}(a, b)$

lcm−(alt)

Show: $d = \text{lcm}(a, b)$
Conclude: $d > 0$
Conclude: $a \mid d$
Conclude: $b \mid d$
Conclude: $\forall c > 0, a \mid c$ and $b \mid c \Rightarrow d \mid c$

Relatively prime+

Show: $\gcd(a, b) = 1$
Conclude: *a, b are relatively prime*

Relatively prime −

Show: *a, b are relatively prime*
Conclude: $\gcd(a, b) = 1$

Remarks: Keep in mind that all single letter variables in these recipes have type natural number, so you can't use these recipes on expressions that don't have the correct type.

Precedence: Arithmetic relations such as $=, \neq, <, \leq, \underset{m}{\equiv}$ have a lower precedence than arithmetic operations such as $+, -, \cdot, /, \wedge$.

8 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 5 to eliminate tedious, repetitive steps, shorten the proofs, and emphasize the aspect 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 semi-formal 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*.

8.1 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 semi-formal 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 semi-formal 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.

8.2 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're trying to say.

8.3 Notation

An important part of making mathematical writing unambiguous and easy to understand is to choose good notation for the things you're 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's not a good idea to assume that your reader knows what you mean by it.

  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 notations 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 $f(x) = mx + b$ is linear.

- *Don't use the same notation for different objects in a single proof.* Aside from being confusing to the reader, this can 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 $a = 2k$ for some integer k and $b = 2l$ for some integer l. Thus $ab = 2k \cdot 2l = 4kl$ 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.

8.4 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 $b \in \mathbb{Z}/n\mathbb{Z}$.

  Good: Let a be a quadratic residue. Then we can write $a = b^2$ for some $b \in \mathbb{Z}/n\mathbb{Z}$.

- *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 writings. However, this usually distracts from the meaning of the sentence and makes writing less understandable.

  Bad: Each solution satisfies $x^2 + y^2 = 1 \vee x + y = 0$.

  Good: Each solution satisfies either $x^2 + y^2 = 1$ or $x + y = 0$.

  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 another way of presenting this logical expression is 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 $n^2 \equiv a \pmod{p}$ has a solution $n = \overline{b}$, $n = \overline{p} - \overline{b}$ is the only other solution of the equation.

  Good: If the congruence equation $n^2 \equiv a \pmod{p}$ 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.

8.5 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 a 'stacked' 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:

$$\begin{aligned}(a+b)^3 &= (a+b)(a+b)^2\\ (a+b)^3 &= (a+b)(a^2+2ab+b^2)\\ (a+b)^3 &= x^3+3x^2+3x+1\end{aligned}$$

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 this writing guide, 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: $(x+y)(-z) = -xz-yz$

8.6 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.

- *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 semi-formal or formal proofs, we generally do not name the rules of inference for logic in traditional expository proofs, although we may refer to the overall strategy being used (induction, contradiction, etc.).

  Bad: We showed that if a prime p divides an integer power a^k, then p divides a. Suppose 5 divides b^8 and 3 divides b^6. Then 5 divides b. Also, 3 divides b. Thus, 15 divides b.

  Good: We showed that if a prime p divides an integer power a^k, then p divides a. Suppose 5 divides b^8 and 3 divides b^6. Then by applying the previous proposition twice, we see that both 5 and 3 divide b. As a result, we see that 15 also divides 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 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!

8.7 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 LaTeXtutorials 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.)

9 Combinatorial Proofs

9.1 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 20. 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 $f : \{1, 2, \ldots, n\} \to S$. 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 21. With this definition we can formally prove that $\#\{\text{☺}\} = 1$.

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.

9.2 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 discuss so far. This form of proof will be based on counting, and so we need something to count.

Definition 22. 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 23. 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 24. A *combinatorial identity* is a expression of the form

$$A = B$$

where A and B are combinatorial expressions.

9.3 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 25. 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.

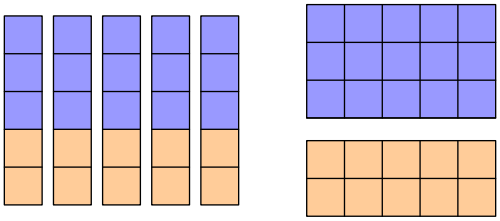
It is truly amazing the extent to which we can build up much of algebra from a combinatorial perspective, and give combinatorial proofs of many algebraic identities. Often, combinatorial interpretations are considered to be easier and more intuitive explanations of a given fact than algebraic or inductive proofs.

Example 26. 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 listed in Section 6.4. 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.

9.4 Combinatorial subtraction and division

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 27. Let k, m, and n be combinatorial expressions.

1. If $k + m = n$ then we define $n - k$ to be m.

2. If $k \cdot m = n$ 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 $1, 2, \ldots, n-2, n-1, n$.

9.5 Some Basic Combinatorial Identities

The following combinatorial identities can all be proved using a combinatorial proof using only the definitions given in Section 9.2. 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 9.2.

Theorem 28. *Let n, k be combinatorial expressions. Then*

1. $k \cdot n = \underbrace{n + n + \cdots + n}_{k \text{ summands}}$

2. $n^k = \underbrace{n \cdot n \cdots n}_{k \text{ factors}}$

3. $n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$

4. $(n)_k = n \cdot (n-1) \cdots (n-k+1)$

5. $\binom{n}{k} \cdot k! \cdot (n-k)! = n!$

6. $\left(\!\binom{n}{k}\!\right) = \binom{n-1+k}{k}$

Note that in the algebraic axiomatic setting the above formulas are usually taken to be the definition of the expression on the left hand side in Theorem 28 parts 1-4 and 6, and similarly, in an algebraic setting w define $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. From the perspective of combinatorial proofs, these formulas are all theorems that we prove by counting the same collection in two different ways.

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.

Example 29. Give combinatorial proofs of the following identities without resorting to any algebra or substitution. Assume the given expressions are defined.

1. $n! = n \cdot (n-1)!$

2. $n^k = n \cdot n^{k-1}$

3. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

We can also define new combinatorial expressions that count a certain collection, and then prove identities using that new expression with combinatorial proofs.