Math 299 Lecture Notes

© 2010 - Ken Monks

by Ken Monks
Math 299 - Introduction to Mathematical Proof
Department of Mathematics
University of Scranton

This is **not** a complete set of lecture notes for Math 299, Introduction to Mathematical Proof. Additional material will be covered in class and discussed in the textbook. This is intended to be a quick reference for the definitions and rules used in the course.

Logic

Variables, Expressions, and Statements

Term	Definition
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.

Propositional Logic

The Five Logical Operators

Definition: Let P,Q be statements. Then the five expressions "$\neg P$", "$P \text{ and } Q$", "$P \text{ or } Q$", "$P \Rightarrow Q$", 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	$\neg P$	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

Rules of Inference and Proof

Definition: A *rule of inference* is a rule which takes zero or more statements (or other items) as input and returns one or more statements as output (conclusions).

Notation. A rule of inference can be expressed in *recipe notation* as

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

Definition: A *formal logic system* consists of a set of statements and a set of rules of inference.

Definition: A *proof* in a formal logic system consists of a finite sequence of statements (and other inputs to the rules of inference) such that each statement follows from the previous statements in the sequence by one or more of the rules of inference.

Natural Deduction

Notation. The symbol $\leftarrow$ is an abbreviation for "end assumption".

Rules of Inference for Propositional Logic	
and $+$ Show: W Show: V Conclude: W and V	and $-$ Show: W and V Conclude: W Conclude: V
$\Rightarrow +$ *Assume* W Show: V $\leftarrow$ Conclude: $W \Rightarrow V$	$\Rightarrow -$ (modus ponens) Show: W Show: $W \Rightarrow V$ Conclude: V
$\Leftrightarrow +$ Show: $W \Rightarrow V$ Show: $V \Rightarrow W$ Conclude: $W \Leftrightarrow V$	$\Leftrightarrow -$ Show: $W \Leftrightarrow V$ Conclude: $W \Rightarrow V$ Conclude: $V \Rightarrow W$

Rules of Inference for Propositional Logic	
or $+$ Show: W Conclude: W or V Conclude: V or W	or $-$ (proof by cases) Show: W or V Show: $W \Rightarrow U$ Show: $V \Rightarrow U$ Conclude: U
$\neg+$ (proof by contradiction) *Assume* W Show: $\rightarrow\leftarrow$ $\leftarrow$ Conclude: $\neg W$	$\neg-$ (proof by contradiction) *Assume* $\neg W$ Show: $\rightarrow\leftarrow$ $\leftarrow$ Conclude: W
$\rightarrow\leftarrow +$ Show: W Show: $\neg W$ Conclude: $\rightarrow\leftarrow$	

Remarks:

- 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 "$\leftarrow$" 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*-$\leftarrow$ 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 $\leftarrow$, 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*-$\leftarrow$ block to keep track of what statements are valid under which assumptions.

Predicate Logic

Quantifiers

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

Definition: 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: 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*

$\forall+$	$\forall-$
Let s be arbitrary Show: $W(s)$ Conclude: $\forall x, W(x)$	Show: $\forall x, W(x)$ Conclude: $W(t)$
$\exists+$	$\exists-$
Show: $W(t)$ Conclude: $\exists x, W(x)$	Show: $\exists x, W(x)$ Conclude: $W(c)$ *for some c*

**Restrictions:*

- In $\forall+$, s cannot appear as a free variable in any assumption or premise, and $W(s)$ cannot contain any constants which were produced by the $\exists-$ rule.
- In $\forall-$ and $\exists+$, no free variable in t may become bound when t is substituted for x in $W(x)$.
- In $\exists+$, 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 $\exists-$, c must be a new constant in the proof.

Definition: 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*

$\exists!+$	$\exists!$
Show: $W(s)$ *Let y be arbitrary.* *Assume* $W(y)$ Show: $y = s$ $\leftarrow$ Conclude: $\exists! x, W(x)$	Show: $\exists! x, W(x)$ Conclude: $\exists x, W(x) \text{ and } \forall y, W(y) \Rightarrow y = x$

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.

Remark. 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.)
$\neg$
and,or
$\Rightarrow$
$\Leftrightarrow$
$\forall, \exists, \exists!$

Sets, Functions, Numbers

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

Rules of Inference for Basic Set Theory

Relative Complement+ Show: $x \in B$ Show: $x \notin A$ Conclude: $x \in B - A$	Relative Complement− Show: $x \in B - A$ Conclude: $x \in B$ Conclude: $x \notin A$
Complement+ Show: $x \notin A$ Conclude: $x \in \overline{A}$	Complement− Show: $x \in \overline{A}$ Conclude: $x \notin A$
Indexed Intersection+ *Let* $k \in I$ Show: $x \in A_k$ Conclude: $x \in \bigcap\limits_{i \in I} A_i$	Indexed Intersection− Show: $x \in \bigcap\limits_{i \in I} A_i$ Show: $k \in I$ Conclude: $x \in A_k$
Indexed Union+ Show: $k \in I$ Show: $x \in A_k$ Conclude: $x \in \bigcup\limits_{i \in I} A_i$	Indexed Union− Show: $x \in \bigcup\limits_{i \in I} A_i$ Conclude: $x \in A_k$ *for some* $k \in I$

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 Proof Shortcuts Handout for details.
- Usually we just use $x \notin A$ and $\neg x \in A$ interchangeably in our proofs without invoking the "Not an element of" rules.

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

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−

Rules of Inference for Cartesian Products

Show: $x = u$	Show: $(x, y) = (u, v)$
Show: $y = v$	Conclude: $x = u$
Conclude: $(x, y) = (u, v)$	Conclude: $y = v$

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

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.

Functions

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 $f(x)$:	$f(x) = y \Leftrightarrow f : A \to B$ and $(x, y) \in f$
Domain:	$\text{Domain}(f) = A \Leftrightarrow f : A \to B$
Codomain:	$\text{Codomain}(f) = B \Leftrightarrow f : A \to B$
Image (of a set):	$f(S) = \{y : \exists x, x \in S$ and $y = f(x)\}$
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 $\Leftrightarrow f : A \to B$ and $(\forall y, y \in B \Rightarrow \exists x, y = f(x))$
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 $S \subseteq B \Rightarrow f^{-1}(S) = \{x \in A : f(x) \in S\}$

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

Rules of Inference for Functions	
Injective+ Show: $f : A \to B$ *Let* $x, y \in A$ *Assume* $f(x) = f(y)$ Show: $x = y$ $\leftarrow$ Conclude: f *is injective*	Injective− Show: f *is injective* Show: $f(x) = f(y)$ Conclude: $x = y$
Surjective+ Show: $f : A \to B$ *Let* $y \in B$ Show: $y = f(x)$ for some $x \in A$ Conclude: f is *surjective*	Surjective− Show: $f : A \to B$ *is surjective* Show: $y \in B$ Conclude: $y = f(x)$ *for some* $x \in A$
Bijective+ Show: f *is injective* Show: f *is surjective* Conclude: f *is bijective*	Bijective− Show: f *is bijective* Conclude: f *is injective* Conclude: f *is surjective*
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: $g = f^{-1}$	Inverse function− Show: $f : A \to B$ Show: f^{-1} exists Conclude: $f^{-1} : B \to A$ Conclude: $f^{-1}(f(x)) = x$ Conclude: $f\left(f^{-1}(y)\right) = y$
Inverse image+ Show: $f(x) \in T$ Conclude: $x \in f^{inv}(T)$	Inverse image− Show: $x \in f^{inv}(T)$ 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.*

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	$\mathbb{O}_n=\{0,1,2,\ldots,n\}$

Relations

Def of $\neq$	$x \neq t \Leftrightarrow \neg (x = t)$
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:	$R\,(x, y) \Leftrightarrow (x, y) \in R$
Relation on a set:	R is a relation on $A \Leftrightarrow R \subseteq A \times A$
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$\Leftrightarrow \forall x \in A, \forall y \in A, \forall z \in A, xRy \text{ and } yRz \Rightarrow xRz$
Nonreflexive relation:	$R \subseteq A \times A$ is nonreflexive$\Leftrightarrow \forall x \in A, \neg xRx$
Antisymmetric relation:	$R \subseteq A \times A$ is antisymmetric $\Leftrightarrow \forall x \in A, \forall y \in A, xRy \text{ and } yRx \Rightarrow x = y$
Total relation:	$R \subseteq A \times A$ is total$\Leftrightarrow \forall x \in A, \forall y \in A, xRy \text{ or } yRx$
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 $A \Leftrightarrow (\forall S \in P, S \neq \varnothing \text{ and } S \subseteq A)$ and $A = \bigcup_{S \in P} S$ and $\forall S \in P, \forall T \in P, S = T \text{ or } S \cap T = \varnothing$

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$+$ Show: $\neg x = y$ Conclude: $x \neq y$	Not an element of$-$ Show: $x \neq y$ Conclude: $\neg x = y$
Relation$+$ Show: $R \subseteq A \times B$ Conclude: *R is a relation from A to B*	Relation$-$ Show: *R is a relation from A to B* Conclude: $R \subseteq A \times B$

Rules of Inference for Relations

Relation on a set+ Show: $R \subseteq A \times A$ Conclude: R *is a relation on* A	Relation on a set− Show: R *is a relation on* A Conclude: $R \subseteq A \times A$
Reflexive relation+ *Let* $x \in A$ Show: xRx Conclude: R *is reflexive*	Reflexive relation− Show: R *is reflexive* Conclude: xRx
Symmetric+ *Let* $x, y \in A$ *Assume* xRy Show: yRx ← Conclude: R *is symmetric*	Symmetric− Show: R *is symmetric* Show: xRy Conclude: yRx
Transitive+ *Let* $x, y, z \in A$ *Assume* xRy and yRz Show: xRz ← Conclude: R *is transitive*	Transitive− Show: R *is transitive* Show: xRy Show: yRz Conclude: xRz
Nonreflexive+ *Let* $x \in A$ Show: $\neg xRx$ Conclude: R *is nonreflexive*	Nonreflexive− Show: R *is nonreflexive* Conclude: $\neg xRx$
Antisymmetric+ *Let* $x, y \in A$ *Assume* xRy Show: $\neg yRx$ ← Conclude: R *is antisymmetric*	Antisymmetric− Show: R *is antisymmetric* Show: xRy Conclude: $\neg yRx$
Total relation+ *Let* $x, y \in A$ Show: xRy or yRx Conclude: R *is total*	Total relation− Show: R *is total* Conclude: xRy or yRx
Partial order+ Show: R *is reflexive* Show: R *is antisymmetric* Show: R *is transitive* Conclude: R *is a partial order*	Partial order− Show: R *is a partial order* Conclude: R *is reflexive* Conclude: R *is antisymmetric* Conclude: R *is transitive*

Rules of Inference for Relations

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

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

Remark. 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 $y \in S$.

Number Theory and Induction

Arithmetic and Algebra

While it is possible to give an axiomatic description 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.

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. Well 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".

Induction

One of the defining axioms of the natural numbers is mathematical induction. In the following, let $P(n)$ be a statement about a natural number variable n.

Types of Induction

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

Remark: 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 Proof by Induction

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

Rules of Inference for Proof by Induction

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

Remark: It can be shown that any theorem you can prove with Strong Induction can be proved using ordinary Induction and vice-versa. Also note that in strong induction the assumption should really be $\forall j, a \leq j \leq k \Rightarrow P(j)$, i.e. it only holds for values of j that are greater than or equal to a.

Quotient, Remainder, Divisibility, and Mod

Here are some useful theorems and definitions about integers. In the following all single letter variables have type *integer.*

Division Algorithm:	$\forall a, \forall b \neq 0, \exists! q, \exists! r, a = qb + r$ and $0 \leq r < \lvert b \rvert$
Quotient :	$\forall a, \forall b \neq 0, \forall q, \forall r, a = qb + r$ and $0 \leq r < \lvert b \rvert \Leftrightarrow q = (a \operatorname{quo} b)$
Remainder:	$\forall a, \forall b \neq 0, \forall q, \forall r, a = qb + r$ and $0 \leq r < \lvert b \rvert \Leftrightarrow r = (a \bmod b)$
Divides:	$a \mid b \Leftrightarrow \exists q, b = aq$
Divisor (or factor):	a is a divisor (or factor) of $b \Leftrightarrow a \mid b$
Prime:	p is prime $\Leftrightarrow p > 1$ and $\forall a > 0, a \mid p \Rightarrow a = 1$ or $a = p$
Composite:	n is composite $\Leftrightarrow$ n>0and$\exists a, \exists b, n = ab$ and $1 < a, b < n$
Congruent mod m:	$a \underset{m}{\equiv} mb \Leftrightarrow m \mid (a - b)$
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 and some $0 \leq r < \lvert b \rvert$	Show: $b \neq 0$ Show: $a = qb + r$ Show: $0 \leq r < \lvert b \rvert$ 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 $0 \leq r < \lvert b \rvert$	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: $a \mid b$	Show: $a \mid b$ 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 $a = p$
    ←
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: $a \underset{m}{\equiv} mb$	Show: $a \underset{m}{\equiv} mb$ Conclude: $m \mid a - b$

Rules of Inference for Divisibility

gcd+ Show: $d > 0$ Show: $d \mid a$ Show: $d \mid b$ *Let* $c > 0$ *Assume* $c \mid a$ and $c \mid b$ Show: $c \leq d$ $\leftarrow$ Conclude: $d = gcd\,(a, b)$	gcd− 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: $c \mid d$ $\leftarrow$ 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: $d \leq c$ $\leftarrow$ Conclude: $d = \mathrm{lcm}\,(a, b)$	lcm− Show: $d = \mathrm{lcm}\,(a, b)$ 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: $d \mid c$ $\leftarrow$ Conclude: $d = \mathrm{lcm}\,(a, b)$	lcm−(alt) Show: $d = \mathrm{lcm}\,(a, b)$ 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 integer, so you can't use these recipes on expressions that don't have the correct type.

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