MATH 145 Algebra (Advanced)

Lecture Notes

Zhongwei Zhao

List of Lectures

Lecture 1, Sept. 9

Course Orientation and Organization **About the Professor** Stephen New
MC 5419
Ext 35554
Email: snew@uwaterloo.ca
Website: www.math.uwaterloo.ca/ snew
Office Hour: MTWF 11:30-12:30 **Recommended Textbook**

- An Introduction to Mathematical Thinking by Will J. Gilbert, Scott A. Vanstone
- Lecture Notes: Integers, Polynomials and Finite Fields by K. Davidson

Some Paradoxes There are lots of paradoxes in English, such as "This statement is false".

There are also some paradoxes in Mathematical world.

Russell's Paradox Let X be the set of all sets. Let $S = \{A \in X | A \notin A\}$. Is $S \in S$?

Some Question To avoid such paradoxes, some question was raised.

1. What is an allowable mathematical object?
2. What is an allowable mathematical statement?
3. What is an allowable mathematical proof?

Mathematical Object Essentially all mathematical objects are (mathematical) sets. In math, a set is a certain specific kind of collection whose elements are sets. Not all collection of sets are called sets. For a collection to be a set, it must be constructable using specific rules. These rules are called the ZFC axioms of set theory (or the Zermelo–Fraenkel axioms along with the Axiom of Choice)

These axioms include (imply) the following:

- Empty Set: there exist a set, denoted by $\emptyset$, with no elements.
- Equality: two sets are equal when they have the same elements. $A = B$ when for every set x, $x \in A \iff x \in B$
- Pair Axiom: if A and B are sets then so is $\{A, B\}$
- Union Axiom: if S is a set of sets then $\cup_S = \{x | x \in A \text{ for some } A \in S\}$. If A and B are sets, then so is $\{A, B\}$ hence so is $A \cup B = \cup_{\{A,B\}}$

Lecture 2, Sept. 12

Mathematics Contest Big Contests

- Small C
- Big E/Special K
- Putnam
- Bernoulli Trials

Students Run

- Integration Bee
- over 6000

Others

- Recreational Problem Sessions

ZFC Axioms

- Empty Set: there exist a set, denoted by $\emptyset$, with no elements.
- Equality: two sets are equal when they have the same elements. $A = B$ when for every set x, $x \in A \iff x \in B$
- Pair Axiom: if A and B are sets then so is $\{A, B\}$. In particular, taking $A = B$ shows that $\{A\}$ is a set.
- Union Axiom: if S is a set of sets then $\cup_S = \bigcup_{A \in S} A = \{x \mid x \in A \text{ for some } A \in S\}$. If A and B are sets, then so is $\{A, B\}$ hence so is $A \cup B = \cup_{\{A,B\}}$
- Power Set Axiom: if A is a set, then so is its Power Set $P(A)$. $P(A) = \{X \mid X \subseteq A\}$. In particular, $\emptyset \subseteq X$, $X \subseteq X$
- Axiom of Infinity: if we define

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} = \{\emptyset\} \\ 2 &= \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\ 3 &= \{0, 1, 2\} = \{\emptyset, \{\emptyset, \{\emptyset\}\}\} \\ &\vdots \\ n + 1 &= n \cup \{n\} \end{aligned}$$

  Then $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is a set (called the set of natural numbers)

Lecture 3, Sept. 13

Women in Math Tue Sept. 13
4:30-6:00
DC 1301

ZFC Axioms

- Empty Set: there exist a set, denoted by $\emptyset$, with no elements.
- Equality: two sets are equal when they have the same elements. $A = B$ when for every set x, $x \in A \iff x \in B$
- Pair Axiom: if A and B are sets then so is $\{A, B\}$. In particular, taking $A = B$ shows that $\{A\}$ is a set.
- Union Axiom: if S is a set of sets then $\cup_S = \bigcup_{A \in S} A = \{x \mid x \in A \text{ for some } A \in S\}$. If A and B are sets, then so is $\{A, B\}$ hence so is $A \cup B = \cup_{\{A,B\}}$
- Power Set Axiom: if A is a set, then so is its Power Set $P(A)$. $P(A) = \{X \mid X \subseteq A\}$. In particular, $\emptyset \subseteq X$, $X \subseteq X$
- Axiom of Infinity: if we define

  $$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} = \{\emptyset\} \\ 2 &= \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\ 3 &= \{0, 1, 2\} = \{\emptyset, \{\emptyset, \{\emptyset\}\}\} \\ &\vdots \\ n + 1 &= n \cup \{n\} \end{aligned}$$

  Then $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is a set (called the set of natural numbers)
- Specification Axioms: if A is a set, and $F(x)$ is a mathematical statement about an unknown set x, then $\{x \in A \mid F(x) \text{ is true }\}$ is a set.

  Examples:

  $$\{x \in \mathbb{N} \mid x \text{ is even }\} = \{0, 2, 4, 6, \dots\}$$

  $$A \cap B = \{x \in A \cup B \mid x \in A \text{ and } x \in B\}$$
- Replacement Axioms: if A is a set and $F(x, y)$ is a mathematical statement about unknown sets x and y with the property that for every $x \in A$ there is a unique set y such that the statement is true, and if we denote this unique set y by $y = F(x)$, then $\{F(x) \mid x \in A\}$ is a set.
- Axiom of Choice: if S is a set of non-empty sets then there exists a function $F \colon S \to U_S$ which is called a choice function for S such that

  $$F(A) \in A \quad \forall A \in S$$

Things that are sets

3.1 Example.

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

$$A \cap B = \{x \in A \cup B \mid x \in A \text{ and } x \in B\}$$

$$A \backslash B = \{x \in A \mid x \notin B\}$$

$$A \times B = \{(x, y) \mid x \in A, x \in B\}$$

$$A^2 = A \times A$$

One way to define ordered pairs

$$(x, y) = \{\{x\}, \{x, y\}\}$$

$$x \in A, y \in B \therefore x, y \in A \cup B$$

$$\{x\}, \{x, y\} \in P(A \cup B)$$

$$(x, y) = \{\{x\}, \{x, y\}\} \subseteq P(A \cup B)$$

$$(x, y) \in P(P(A \cup B))$$

$$\therefore A \times B = \{(x, y) \in P(P(A \cup B)) \mid x \in A \text{ and } y \in B\}$$

function When A and B are sets, a function from A yo B is a subset $F \subseteq A \times B$ with the property that for every $x \in A$ there exists a unique $y \in B$ such that $(x, y) \in F$

When F is a function from A to B we write

$$F : A \to B$$

and for $x \in A$ and $y \in B$ we write $y = F(x)$ to indicate that $(x, y) \in F \subseteq A \times B$

Sequence A sequence $a_0, a_1, a_2, \ldots$ of natural numbers is a function $a : \mathbb{N} \to \mathbb{N}$ and we write $a(k)$ as a_k

Less than the relation $<$ on $\mathbb{Z}$ is a subset $<\subseteq \mathbb{Z}^2$ and we write $x < y$ when $(x, y) \in <$

We can use the ZFC Axioms to define and construct

- $\mathbb{Z}$: the set of integers
- $\mathbb{Q}$: the set of rationals
- $\mathbb{R}$: the set of real numbers
- $+, \times$: operations
- $<, >$: relations

Lecture 4, Sept. 14

Class

4.1 Definition. A class is a collection of sets of the form

$$\{x \mid F(x) \text{ is true }\}$$

Where $F(x)$ is a mathematical statement about an unknown set x.

4.2 Example. The collection of all sets is the class $\{x \mid x = x\}$

4.3 Example. If A is a set then $A = \{x \mid x \in A\}$ which is also a class

Mathematical Statement

4.4 Definition. In the languages of Propositional logic we use symbols from the symbol set

$$\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, (,)\}$$

together with propositional variable symbols such as $P, Q, R, \ldots$

The variable symbols are intended to represent mathematical statements which are either true or false.

In propositional logic, a formula is a non-empty, finite string of symbols (from the above set of symbols) which can be obtained by applying the following rules.

1. Every propositional variable is a formula.
2. If F is a formula, then so is the string $\neg F$.
3. If F and G are formulas then so is each of the following strings
   - $(F \vee G)$
   - $(F \wedge G)$
   - $(F \rightarrow G)$
   - $(F \leftrightarrow G)$

A derivation for a formula F is a list of formulas

$$F_1, F_2, F_3, \ldots$$

with $F = F_k$ for some index k and for each index l, either F_l is a propositional variable, or F_l is equal to $F_l = \neg F_i$ for some $i < l$, or $F_l = (F_i * F_j)$ for some $i, j < l$ and for some symbol $* \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$

4.5 Example.

$$(\neg(\neg P \rightarrow Q) \leftrightarrow (R \vee \neg S))$$

is a formula and one possible derivation, with justification on each line, is as follows

1. P

2. Q
3. R
4. S
5. $\neg P$
6. $(\neg P \rightarrow Q)$
7. $\neg S$
8. $R \vee \neg S$
9. $\neg(\neg P \rightarrow Q)$
10. $(\neg(\neg P \rightarrow Q) \leftrightarrow (R \vee \neg S))$

4.6 Definition. An **assignment** of truth-values to the propositional variables is a function $\alpha \colon \{P, Q, R \dots\} \rightarrow \{0, 1\}$

For a propositional variable X when $\alpha(X) = 1$ we say $X$is true under α and when $\alpha(X) = 0$ we say X is false under α

Given an assignment $\alpha \colon \{\text{propositional variables}\} \rightarrow 0, 1$ we extend α to a function $\alpha \colon \{\text{formulas}\} \rightarrow 0, 1$ by defining $\alpha(F)$ for all formulas F recursively as follows:

When $F = X$ where X is a propositional variable symbol, the value of $\alpha(X)$is already known

When $F = \neg G$ where G is a formula, define $\alpha(F)$ according to the following table

G	$\neg G$
1	0
0	1

When $F = (G * H)$ where G and H are formulas and where $* \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$

we define $\alpha(F)$ according to the following table

G	H	$G \wedge H$	$G \vee H$	$G \rightarrow H$	$G \leftrightarrow H$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Lecture 5, Sept. 16

Mathematical Statement Given a formula F and an assignment α, (that is give the values of $\alpha(P), \alpha(Q), \alpha(R), \dots$), we can calculate $\alpha(F)$ by making a derivation $F_1, F_2, F_3, \dots, F_l$ for F then calculate the values $\alpha(F_1), \alpha(F_2), \dots$ one at a time.

5.1 Example. Let F be the formula $F = (\neg(P \leftrightarrow R) \vee (Q \rightarrow \neg R))$ and let α be an assignment then with $\alpha(P) = 0$, $\alpha(Q) = 1$ and $\alpha(R) = 0$. Find $\alpha(F)$.

We make a derivation $F_1, F_2, F_3, \dots, F_l$ for F and calculate the values $\alpha(F_k)$

P	Q	R	$P \leftrightarrow R$	$\neg(P \leftrightarrow R)$	$\neg R$	$Q \rightarrow \neg R$	F
0	1	0	1	0	1	1	0

Truth Table

5.2 Definition. For variable symbols $P_1, P_2, \dots, P_n$, an assignment on $(P_1, P_2, \dots, P_n)$ is a function

$$\alpha\colon \{P_1, P_2, \dots, P_n\} \rightarrow \{0, 1\}$$

For a formula F which only involves the variable symbols in $\{P_1, P_2, \dots, P_n\}$, a truth table for F on $(P_1, P_2, \dots, P_n)$ is a table whose top header row is a derivation $F_1, F_2, F_3, \dots, F_l$ for F with $F_i = P_i$ for $1 \leq i \leq n$, and under the header row there are 2^n rows which correspond to the 2^n assignments on $(P_1, P_2, \dots, P_n)$. For each assignment $\alpha\colon \{P_1, P_2, \dots, P_n\} \rightarrow \{0, 1\}$ there is a row of the form $\alpha(F_1), \alpha(F_2), \dots, \alpha(F_n)$ and the rows are listed in order such that in the first n columns, the rows $\alpha(F_1), \alpha(F_2), \dots, \alpha(F_n)$ (that is $\alpha(P_1), \alpha(P_2), \dots, \alpha(P_n)$) list the 2^n binary numbers from $111\dots1$ at the top, in order, down to $000\dots0$ at the bottom.

5.3 Example. Make a truth table for the formula

$$F = P \leftrightarrow (Q \wedge \neg(R \rightarrow P))$$

P	Q	R	$R \rightarrow$P	$\neg(R \rightarrow P)$	$Q \wedge \neg(R \rightarrow P)$	F
1	1	1	1	0	0	0
1	1	0	1	0	0	0
1	0	1	1	0	0	0
1	0	0	1	0	0	0
0	1	1	0	1	1	0
0	1	0	1	0	0	1
0	0	1	0	1	0	1
0	0	0	1	0	0	1

Tautology Let F and G be formula and let S be a set of formulas

5.4 Definition. We say that F is a tautology, and we write $\models F$, when $\alpha(F) = 1$ for every assignment α

We say that F is a contradiction when $\alpha(F) = 0$ for every assignment α, or equivalently when $\models \neg F$

We say that F is equivalent to G, and we write $F \equiv G$ when $\alpha(F) = \alpha(G)$ for every assignment α

We say that argument "S therefore G" is valid, or that "S induces G" or that "G is a consequence of S", when for every assignment α for which $\alpha(F) = 1$ for every $F \in S$ we have $\alpha(G) = 1$.

When $S = \{F_1, F_2, \ldots, F_n\}$ we have $S \models G$ is equivalent to $\{((F_1 \wedge F_2) \wedge \cdots \wedge F_n)\} \models G$ which is equivalent to $\models (((F_1 \wedge F_2) \wedge \cdots \wedge F_n) \to G)$

Lecture 6, Sept. 19

Tautology

Let F and G be formula and let S be a set of formulas

Notation. We say that F is a tautology, and we write $\models F$, when $\alpha(F) = 1$ for every assignment α

We say that F is a contradiction when $\alpha(F) = 0$ for every assignment α, or equivalently when $\models \neg F$

We say that F is equivalent to G, and we write $F \equiv G$ when $\alpha(F) = \alpha(G)$ for every assignment α

We say that argument "S therefore G" is valid, or that "S induces G" or that "G is a consequence of S", when for every assignment α for which $\alpha(F) = 1$ for every $F \in S$ we have $\alpha(G) = 1$.

When $S = \{F_1, F_2, \ldots, F_n\}$ we have $S \models G$ is equivalent to $\{((F_1 \wedge F_2) \wedge \cdots \wedge F_n)\} \models G$ which is equivalent to $\models (((F_1 \wedge F_2) \wedge \cdots \wedge F_n) \to G)$

When we consider an argument "S therefore G", the formula in S are called the premises for the hypothesis or the assumption and the formula G is called the conclusion of the argument.

Here are some examples of tautology.

1. $\models F \vee \neg F$
2. $\models P \to P$
3. $\models P \leftrightarrow P$
4. $\models \neg(P \wedge \neg P)$
5. $\models \neg P \to (P \to Q)$
6. $\models Q \to (P \to Q)$

Here are some truth equivalences

1. $P \equiv P$
2. $P \equiv \neg\neg P$
3. $P \vee Q \equiv Q \vee P$
4. $P \wedge Q \equiv Q \wedge P$
5. $P \leftrightarrow Q \equiv Q \leftrightarrow P$
6. $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$
7. $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$
8. $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
9. $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

Here are some valid argument

1. $\{P\} \models P$
2. $\{P \wedge Q\} \models P$
3. $\{P \wedge Q\} \models Q$
4. $P \models \{P \wedge Q\}$
5. $Q \models \{P \wedge Q\}$
6. $\{\neg P\} \models P \to Q$
7. $\{Q\} \models P \to Q$
8. $\{P, Q\} \models P \leftrightarrow Q$
9. $\{\neg P, \neg Q\} \models P \leftrightarrow Q$
10. $\{P, P \to Q\} \models Q$

6.1 Example. Determine whether

$$\models (P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$$

Solution. We make a truth table for

$$F = (P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$$

P	Q	R	$(P \to (Q \to R))$	$((P \to Q) \to (P \to R))$
1	1	1	1	1
1	1	0	0	0
1	0	1	1	1
1	0	0	1	1
0	1	1	1	1
0	1	0	1	1
0	0	1	1	1
0	0	0	1	1

Here are some relationships between tautologies, equivalences and validity.

$$\begin{aligned} F \equiv G &\Leftrightarrow \models (F \leftrightarrow G) \\ &\Leftrightarrow \models ((F \to G) \wedge (G \to F)) \\ &\Leftrightarrow \{F\} \models G \text{ and } \{G\} \models F \end{aligned}$$

When $S = \{F_1, F_2, \ldots, F_n\}$,

$$\begin{aligned} S \models G &\Leftrightarrow \{F_1, F_2, \ldots, F_n\} \models G \\ &\Leftrightarrow (((F_1 \wedge F_2) \wedge \cdots \wedge F_n) \models G \\ &\Leftrightarrow \models (((F_1 \wedge F_2) \wedge \cdots \wedge F_n) \rightarrow G \end{aligned}$$

Also

$$\models F \Leftrightarrow \emptyset \models F$$

$\models F$ means for all assignment α, $\alpha(F) = 1$

$\emptyset \models F$ means for all assignment α, if (for every $G \in \emptyset, \alpha(G) = 1$) then $\alpha(F) = 1$

Notation. For a set A and a statement or formula F

$$\forall x \in A \;\; F \text{ means } \forall x(x \in A \rightarrow F)$$

and

$$\exists x \in A \;\; F \text{ means } \forall x(x \in A \wedge F)$$

So (for every $G \in \emptyset, \alpha(G) = 1$) is always true. This proves that $\models F \Leftrightarrow \emptyset \models F$.

6.2 Example. Determine whether

$$(P \vee Q) \rightarrow R \equiv (P \rightarrow R) \wedge (Q \rightarrow R)$$

Solution.

P	Q	R	$(P \vee Q) \rightarrow R$	$(P \rightarrow R) \wedge (Q \rightarrow R)$
1	1	1	1	1
1	1	0	0	0
1	0	1	1	1
1	0	0	0	0
0	1	1	1	1
0	1	0	0	0
0	0	1	1	1
0	0	0	1	1

6.3 Example. Determine whether

$$\{P \rightarrow (Q \vee \neg R), Q \rightarrow \neg P\} \models R \rightarrow \neg P$$

Solution.

P	Q	R	$\neg R$	$Q \vee \neg R$	$\neg P$	$P \rightarrow (Q \vee \neg R)$	$Q \rightarrow \neg P$	$R \rightarrow \neg P$
1	1	1	0	1	0	1	0	0
1	1	0	1	1	0	1	0	1
1	0	1	0	0	0	0	1	0
1	0	0	1	1	0	1	1	1
0	1	1	0	1	1	1	1	1
0	1	0	1	1	1	1	1	1
0	0	1	0	0	1	1	1	1
0	0	0	1	1	1	1	1	1

Lecture 7, Sept. 20

7.1 Example. Let F and G be formulas

Determine whether

$$\{F \to G, F \vee G\} \models F \wedge G$$

Solution. We make a truth table

F	G	$F \to G$	$F \vee G$	$F \wedge G$
1	1	1	1	1
1	0	0	1	0
0	1	1	1	0
0	0	1	0	0

Remark. It appears from row 3 that the argument is not valid.

But in fact, the argument may or may not be valid, depending on the formulas F and G.

For example, if F is a tautology and G is any formula, the argument is valid.

Or if $F = G$ then the argument is valid.

First-Order Language

Symbol Set

7.2 Definition. A First-Order Language is determined by its symbol set. The symbol set includes symbols from the common symbol set

$$\{\neg, \wedge, \vee, \to, \leftrightarrow, =, \forall, \exists, (,), , \}$$

along with some variable symbols such as

$$x, y, z, u, v, w, \ldots$$

The symbol $=$ is read as "equals". The symbols $\forall$, $\exists$ are called quantifier symbols. The symbol $\forall$ is read as "for all" or "for every", and the symbol $\exists$ is read in "for some" or "there exists".

The symbol set can also include some additional symbols which can include

1. constant symbols
$$a, b, c, \emptyset, 0, i, e, \pi, \ldots$$
2. function symbols
$$f, g, h, \cup, \cap, +, \times, \ldots$$
3. relation symbols
$$P, Q, R, \in, \subset, \subseteq, <, >, =, \ldots$$

The variable and constant symbols are intended to represent elements in a certain set or class u called the universal set or the universal class. The universal set or class is often understood from the context.

Function

7.3 Definition. A unary function f from a set u is a function $f\colon u \to U$ (for every $x \in u$ there is a unique element $y = f(x) \in U$)

A binary function g on u is a function $g\colon u^2 \to U$ where $u^2 = u \times u$ (for every $x, y \in u$ there is a unique element $z = g(x, y) \in U$)

Some binary function symbols are used with infix notation, which means that we write $g(x, y)$ as xgy or as (xgy)

7.4 Example. $+$ is a binary function on $\mathbb{N}$ written with infix notation. So we write $+(x, y)$ as $x + y$ or as $(x + y)$.

Relation

7.5 Definition. A unary relation P on a set u is a subset $P \subseteq U$. For $x \in u$, we write $P(x)$ to indicate that $x \in P$

A binary relation R on u is a subset of U^2. We write $R(x, y)$ to indicate that $(x, y) \in R$

Sometimes a binary relation symbol R is used with indix notation which means that we write $R(x, y)$ as xRy.

7.6 Example. $<$ is a binary relation on $\mathbb{N}$, which means that $<\subseteq \mathbb{N}^2$ and it is used with infix notation, So we write $<(x, y)$ as $x < y$

Also, the symbol $=$ is a binary relation symbol written with infix notation.

Remark. $(P \wedge Q)$ can be written with infix notation as $\wedge PQ$, which is also called polish notation.

Term

7.7 Definition. In a first-order language, a term is a non-empty finite string of symbols from the symbol set which can be obtained by applying the following rules.

1. Every variable symbol is a term and every constant symbol is a term.
2. if f is a unary function symbol and t is a term, then the string $f(t)$ is a term
3. if g is a binary function symbol and s and t are terms, the the string $g(s, t)$ (or the string sgt) is a term.

7.8 Example. The following strings are terms.

- u
- $u \cap v$
- $u \cap (v \cap \emptyset)$
- x
- $x + 1$
- $g(x, f(y + 1))$

Each term represents an element in the universal set or class u

Formula

7.9 Definition. A formula is a non-empty finite string of symbols which can be obtained using the following rules.

1. if P is a unary relation symbol and t is a term then the string $P(t)$ is a formula. (in standard mathematical language we would write $P(t)$ as $t \in P$)
2. if R is a binary relation symbol and s and t are terms then the string $R(s, t)$ is a formula (or sRt)
3. if F is a formula, then so is the string $\neg F$
4. if F and G are formulas then so is each of the strings $F \wedge G$, $F \vee G$, $F \rightarrow G$, $F \leftrightarrow G$
5. if F is a formula and x is a variable symbol, then the string $\forall x F$ and $\exists x F$ are both formulas

Examples: Each of the following strings is formula

- $u \subseteq R$
- $\forall u \;\; \emptyset \in u$
- $f(x) < x + 1$
- $x = g(y, z + 1)$

A formula is a formal way of expressing a mathematical statement about element in u, and about functions and relations on u.

Remark. In standard mathematical language, we continually to add new notations which we allow ourselves to use.

7.10 Example. $\dfrac{x+1}{y}$ could be written as $(x + 1)/y$

$\displaystyle\sum_{k=1}^{n} \frac{1}{k}$ could be written as .... (a very long formula)

Lecture 8, Sept. 21

Recap

Symbol Set

Term

Formula

First-Order Language

8.1 Definition. In the language of first-order number theory, we allow us to use the following additional symbols:

$$\{0, 1, +, \times, <\}$$

Unless otherwise stated, we do not allow ourselves to use any other additional symbols.

8.2 Example. Express each of the following statement as formulas in the language of first-order number theory.

a) x is a factor of y

b) x is a prime number

c) x is a power of 3

Solution. We take he universal set to be $\mathbb{Z}$.

a) $\exists z \in \mathbb{Z} \;\; y = x \times z$

b) $1 < x \wedge \forall y(\exists z \;\; x = y \times z \rightarrow ((y = 1 \vee y = x) \vee (y + 1 = 0 \vee y + x = 0)))$
$1 < x \wedge \forall y((1 < y \wedge \exists z \;\; x = z \times y) \rightarrow y = x)$

c) $(0 < x) \wedge$ the only prime factor of x is 3
$\iff (0 < x) \wedge \forall y \in \mathbb{Z}((\text{y is prime} \wedge \text{y is a factor of x}) \rightarrow y = 3)$
$\iff (0 < x) \wedge \forall y \in \mathbb{Z}((1 < y \wedge \exists z \;\; x = y \times z) \rightarrow \exists z \;\; y = ((z + z) + z))$

$$\begin{aligned} x = -y &\iff x + y = 0 \\ x = y - z &\iff x + z = y \end{aligned}$$

Remark. The two minus signs in the two equations above are different.

8.3 Example. Express the following statements about a function $f : \mathbb{R} \rightarrow \mathbb{R}$ as formulas in first-order number theory after adding the function symbol f to the symbol set.

a) f is surjective (or onto)

b) f is bijective (or invertible)

c) $\lim_{x \rightarrow u} f(x) = v$

Solution. a) $\forall y \in \mathbb{R} \;\; \exists x \in \mathbb{R} \;\; y = f(x)$

b) $\forall y \in \mathbb{R} \;\; \exists! x \in \mathbb{R} \;\; y = f(x)$
$\iff \forall y \in \mathbb{R} \;\; (\exists x \in \mathbb{R}(y = f(x) \land \forall z(y = f(z) \to z = x)))$

c) $\forall \epsilon > 0 \;\; \exists \delta > 0 \;\; \forall x \in \mathbb{R}(0 < |x - v| < \delta \to |f(x) - v| < \epsilon)$
$\iff \forall \epsilon(0 < \epsilon \to \exists \delta(0 < \delta \land \forall x((\neg x = u \land (u < x + \delta \land x < u + \delta)) \to (v < f(x) + \epsilon \land f(x) < v + \epsilon))))$

Lecture 9, Sept. 23

9.1 Definition. In the language of **first-order set theory**, we only use the one additional symbol

$$\in$$

(the membership or "is an element of" symbol), which is a binary relation symbol used with infix notation.

All mathematical statement can be expressed in **this language**

When we use this language, we normally take the universal class to be the class of all sets.

Example: Express each of the following statements about sets as formulas in **first-order set theory**

1. $u = v \backslash (x \cap y)$
2. $u \subseteq P(v \cup w)$
3. $u = 2$

Solution. 1. For sets u, v, x, y

$$\begin{aligned} u = v\backslash(x \cap y) &\iff \forall t(t \in u \leftrightarrow t \in v\backslash(x \cap y)) \\ &\iff \forall t(t \in u \leftrightarrow (t \in v \land \neg t \in (x \cap y))) \\ &\iff \forall t(t \in u \leftrightarrow (t \in v \land \neg(t \in x \land t \in y))) \end{aligned}$$

2.

$$\begin{aligned} u \subseteq P(v \cup w) &\iff \forall x\ (x \in u \rightarrow x \in P(v \cup w)) \\ &\iff \forall x\ (x \in u \rightarrow \forall y\ (y \in x \rightarrow y \in (v \cup w))) \\ &\iff \forall x\ (x \in u \rightarrow \forall y\ (y \in x \rightarrow (y \in v \lor y \in w))) \end{aligned}$$

3.

$$\begin{aligned} u = 2 &\iff u = \{\emptyset, \{\emptyset\}\} \\ &\iff \forall x\ (x \in u \leftrightarrow x \in \{\emptyset, \{\emptyset\}\}) \\ &\iff \forall x\ (x \in u \leftrightarrow (x = \emptyset \lor x = \{\emptyset\})) \\ &\iff \forall x\ (x \in u \leftrightarrow (\forall y\ \neg y \in x \lor \forall y\ y \in x \leftrightarrow y = \emptyset)) \\ &\iff \forall x\ (x \in u \leftrightarrow (\forall y\ \neg y \in x \lor \forall y\ y \in x \leftrightarrow (\forall z \neg z \in y))) \end{aligned}$$

The ZFC axioms can all be expressed as formulas in first order set theory.

1. Equality Axiom:
$$\forall u \forall v\ (u = v \leftrightarrow \forall x\ (x \in u \leftrightarrow x \in u))$$
2. Empty Set Axiom:
$$\exists u \forall x\ \neg x \in u$$

3. Pair Axiom:
$$\forall u \, \forall v \, \exists w \, \forall x \; (x \in w \leftrightarrow (x = u \vee x = v))$$

4. Union Axiom:
$$\forall u \, \exists w \, \forall x \; (x \in w \leftrightarrow \exists v \; (v \in u \cup x \in v))$$

Proof. When we do mathematical proofs, one of the things we allow ourselves to do is make use of some equivalences.

When F, G, H are formulas, s, t are terms, and x, y are variables, the following are equivalences which we call **basic equivalence**

1. $F \equiv F$
2. $\neg\neg F \equiv F$
3. $F \wedge F \equiv F$
4. $F \vee F \equiv F$
5. $F \wedge G \equiv G \wedge G$
6. $F \vee G \equiv G \vee F$
7. $(F \wedge G) \vee H \equiv F \wedge (G \vee H)$
8. $(F \vee G) \wedge H \equiv F \vee (G \wedge H)$
9. $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$
10. $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$
11. $\neg(F \wedge G) \equiv \neg F \vee \neg G$
12. $\neg(F \vee G) \equiv \neg F \wedge \neg G$
13. $F \rightarrow G \equiv \neg G \rightarrow \neg F$
14. $F \rightarrow G \equiv \neg F \vee G$
15. $\neg(F \rightarrow G) \equiv F \wedge \neg G$
16. $F \leftrightarrow G \equiv (F \rightarrow G) \wedge (G \rightarrow F)$
17. $F \leftrightarrow G \equiv (\neg F \vee G) \wedge (\neg G \vee F)$
18. $F \leftrightarrow G \equiv (F \wedge G) \vee (\neg F \wedge G)$
19. $F \wedge (G \vee \neq G) \equiv F$
20. $F \vee (G \vee \neq G) \equiv (G \vee \neq G)$
21. $F \wedge (G \wedge \neg G) \equiv G \wedge \neg G$
22. $F \vee (G \wedge \neg G) \equiv F$

□

Note. We can use basic equivalences one at a time, to derive other equivalences.

9.2 Example. Derive the equivalence:

$$(F \vee G) \rightarrow H \equiv (F \rightarrow H) \wedge (G \rightarrow H)$$

Solution.

$$\begin{aligned}
(F \vee G) \rightarrow H &\equiv \neg(F \vee G) \vee H \text{ (by the equivalence)}\\
&\equiv (\neg F \wedge \neg G) \vee H \text{ (by the de Morgan's)}\\
&\equiv H \vee (\neg F \wedge \neg G) \text{ (by the Commutativity)}\\
&\equiv (H \vee \neg F) \wedge (H \vee \neg G) \text{ (by the Distributivity)}\\
&\equiv (\neg F \vee H) \wedge (\neg G \vee H) \text{ (by the Commutativity)}\\
&\equiv (F \rightarrow H) \wedge (G \rightarrow H) \text{ (by the equivalence)}
\end{aligned}$$

9.3 Definition. Here are some more basic equivalences.

1. $s = t \equiv t = s$
2. $\forall x \forall y\ F \equiv \forall y \forall x\ F$
3. $\exists x \exists y\ F \equiv \exists y \exists x\ F$
4. $\neg \forall x\ F \equiv \exists x\ \neg F$
5. $\neg \exists x\ F \equiv \forall x\ \neg F$
6. $\forall x\ (F \wedge G) \equiv \forall x\ F \wedge \forall x\ G$
7. $\exists x\ (F \vee G) \equiv \exists x\ F \vee \exists x\ G$

Lecture 10, Sept. 26

10.1 Example.

$$\begin{aligned}\exists x\ (F \to G) &\equiv \exists X\ (\neg F \vee G)\\ &\equiv \exists x\ \neg F \vee \exists x\ G\\ &\equiv \neg \forall x\ F \vee \exists x\ G\\ &\equiv \forall x\ F \to \exists x\ G\end{aligned}$$

10.2 Definition. In a formula f, every occurrence of a variable symbol x (Except when the occurrence of x immediately follows a quantifier $\forall, \exists$) is either **free** or **bound**.

In the formulas $\forall x\ F$ and $\exists x\ F$, every free occurrence of x in F becomes **bound** by the initial quantifier, and every bound occurrence of x in F remains bound (by the same quantifier which binds it in F).

10.3 Example.

$$\forall y\ (x \times y = y \times x)$$

Both occurrence of x are free, and both occurrence of y are bound by the initial quantifier.

$$\forall x\ (\forall y\ (x \times y = y \times x) \to x \times a = a \times x)$$

10.4 Definition. An **interpretation** in a first-order language consists of the following: a choice of the universal set u, and a choice of meaning for each constant, function and relation symbol.

A formula is a meaningless string of symbols until we choose an interpretation. Once we choose an interpretation, a formula becomes a meaningful mathematical statement about its free variables.

The truth or falsehood of a formula may still depend on the value in u which are assigned to the free variable symbols in F.

An assignment (of values in u to the variable symbols) is a function $\alpha : \{\text{variable symbols}\} \to u$

10.5 Example. Consider the formula

$$\forall y\ (x \times y = y \times x)$$

when $u = \mathbb{R}$ (and $\times$ is multiplication) the formula becomes true (for any value assigned to x).

when $u = \mathbb{R}^3$ annd $\times$ is cross-product, the formula is true iff $x = 0$

when u is the set of all $n \times n$ matrices with entries in $\mathbb{R}$, and $\times$ denotes matrix multiplication, the formula is can be read as "the matrix x commutes with every matrix", and it is true iff $x = cI$ for some $c \in \mathbb{R}$

Notation. For a formula F, a variable symbol x and a term t, we write $[F]_{x \mapsto t}$ to denote the formula which is constructed from F by replacing x by t.

In an interpretation, the formula $[F]_{x \mapsto t}$ has the same meaning about t that f has about x.

Roughly speaking, $[F]_{x \mapsto t}$ is obtained from F by replacing each free occurrence of the symbol x by the term t. (but if a variable symbol in t would become bound by this replacement, we rename the variable first.)

10.6 Example. In $u = \mathbb{Z}$, $x \mid y$ means $\exists z\ y = x \times z$

$|\exists z\ y = x \times z|_{y \mapsto u} = \exists z\ u = x \times z$ means $x \mid u$

$|\exists z\ y = x \times z|_{y \mapsto x} = \exists z\ x = x \times z$ means $x \mid x$

$|\exists z\ y = x \times z|_{y \mapsto z} \neq \exists z\ z = x \times z$

$|\exists z\ y = x \times z|_{y \mapsto z} = |\exists u\ y = x \times u|_{y \mapsto z} = \exists u\ z = x \times u$

Here are some more basic equivalences:

E32 $\forall x\ F \equiv F$ if x is not free in F

E34 $\forall x\ F \equiv \forall y\ [F]_{x \mapsto y}$ if y is not free in F

Lecture 11, Sept. 27

11.1 Definition. Interpretation is a choice of a non-empty set u, and constant, functions and relations for each constant, function and relation symbol.

An **Assignment** in u,

$$\alpha\colon \{\text{variale symbols}\} \to u$$

We write $\alpha(F) = 1$ when F is true in u under α.

We write $\alpha(F) = 0$ when F is false in u under α.

We say F is true in u when $\alpha(F) = 1$ for **every** assignment $\alpha \in u$

11.2 Example. the formula $x \times y = y \times x$ is true in $\mathbb{Z}$ but not true in $n \times n$ matrices.

11.3 Definition. For formulas F and G and a set of formulas S, we say that F is a **tautology** and we write $\models F$, when for every interpretation u and every assignment $\alpha \in u$, $\alpha(F) = 1$

11.4 Definition. We say that F and G are **equivalent**, and we write $F \equiv G$, when for every interpretation u, for every assignment $\alpha \in u$, $\alpha(F) = \alpha(G)$, we say that the argument "F there fore G" is valid, or that "S induces G", or that "G is a consequences of S", when for every interpretation u and for every assignment $\alpha \in u$, if $\alpha(F) = 1$ for every $F \in S$ then $\alpha(G) = 1$

11.5 Definition. Given a formula G and a set of formulas S, such that $S \models G$, a **derivation** for the valid argument $S \models G$ is a list of valid arguments

$$S_1 \models G_1, S_2 \models G_2, S_3 \models G_3, \ldots$$

where for some index k we have $S_k = S$ and $G_k = G$, such that each valid argument in the list is obtained from previous valid arguments in the list by applying one of the basic validity rules.

1 Basic Validity Rules

Each basic validity rule is a formal and precise way of describing standard method of mathematical proof.

Rules V1, V2 and V3 are used in derivations because we make a careful distinction between **premises** and **conclusions**. In standard mathematical proofs we do not make a careful distinction.

Premise V1. If $F \in S$ then $S \models F$. In words, if we assume F, we can conclude F.

V2. If $S \models F$ and $S \subseteq \mathcal{T}$ then $\mathcal{T} \models F$. In words, if we can prove F without assuming G, then we can still prove F if we assume G.

Chain Rule V3. If $S \models F$ and $S \cup \{F\} \models G$ then $S \models G$. In words, if we can prove F, and by assuming F we can prove G, then we can prove G directly without assuming F.

Proof by Cases V4. If $S \cup \{F\} \models G$ and $S \cup \{\neg F\} \models G$ then $S \models G$. In words, in either case G is true.

Contradiction V5. If $S \cup \{\neg F\} \models G$ and $S \cup \{\neg F\} \models \neg G$ then $S \models F$. In words, to prove F by contradiction, we suppose, for a contradiction, that F is false, we choose a formula G, then we prove that G is true and we prove that G is false.

V6. If $S \cup \{F\} \models G$ and $S \cup \{F\} \models \neg G$ then $S \models \neg F$

V7. If $S \models F$ and $S \models \neg F$ then $S \models G$

Conjunction V8. $S \models F \wedge G \iff (S \models F$ and $S \models G)$

V9. If $S \cup \{F, G\} \models H$ then $S \cup \{F \wedge G\} \models H$

V10. ...

V11. ...

V12. ...

Disjunction V13. $S \models F \vee G \iff S \cup \{\neg F\} \models\iff S \cup \{\neg G\} \models F$

V14. ...

Lecture 12, Sept.28

V13. How to prove an or statement

V14. $S \cup F \vDash H$ and $S \cup G \vDash H \iff S \cup (F \vee G) \vDash H$

V15. In words, from F we can conclude $F \vee G$

V16.

V17. In words, from $F \vee G$ and $\neg F$ we can conclude G

V18.

...

V25. In words, to prove $F \iff G$ we suppose F then prove G, and we suppose G and prove F

V26. $(F \iff G) \equiv (F \wedge G) \vee (\neg F \wedge \neg G)$

...

V33. $S \vDash t = t$. In words, we can always conclude that $t = t$ is true under any assumptions.

V34. From $s = t$ we can conclude $t = s$

V35. From $r = s$ and $s = t$ we can conclude $r = t$

V36. If $S \vDash s = t$ then $(S \vDash [F]_{x \mapsto t} \iff S \vDash [F]_{x \mapsto s})$. In words, if $\vDash s = t$, we can always replace any occurrence of the term s by the term t.

V37. If $S \vDash [F]_{x \mapsto y}$ and y is not free in $S \cup \{\forall x\ F\}$ then $S \vDash \forall x\ F$

If have not made any assumptions about x (earlier in out proof) then to prove $\forall x\ F$ we write "let x be arbitrary" then we prove F.

If we have not made any assumptions about y, then to prove $\forall x\ F$, we write "let y be arbitrary" then prove $[F]_{x \mapsto y}$

(This is related to the equivalence

$$\forall x\ F \equiv \forall y\ [F]_{x \mapsto y}$$

)

V38. If $S \vDash \forall x\ F$, then $S \vDash [F]_{x \mapsto t}$

V39.

V40. If $S \cup \{[F]_{x \mapsto t}\} \vDash G$ then $S \vDash \exists X\ F$. In words, to prove $\exists x\ F$ we choose any term t, and prove $[F]_{x \mapsto t}$.

V41. If y is not free in $S \cup \{\exists x\ F, G\}$ and if $S \cup [F]_{x \mapsto y} \vDash G$ then $S \cup \exists x\ F \vDash G$. In words, to prove that $\exists x\ F$ implies G, choose a variable y which we have not made assumptions about and which does not occur in G, we write "choose y so that $[F]_{x \mapsto y}$ is true", then prove G.

Note. In standard mathematical language,

$$\forall x \ \in A \ F$$

means

$$\forall x \ (x \in a \to F)$$

To prove $\forall x \ (x \in a \to F)$ we write "let x be arbitrary", then prove $x \in a \to F$ which we do by writing "suppose $x \in A$" then prove F.

Usually, instead of writing "let x be arbitrary" and "suppose $x \in A$ " we write "let $x \in A$ be arbitrary" or simply "let $x \in A$".

So to prove $\forall x \in A \ F$ we write "let $x \in A$" then prove F. Alternatively, write "let $y \in A$" then prove $[F]_{x \mapsto y}$.

12.1 Example. Prove that

$$\{F \to (G \wedge H), (F \wedge G) \vee H\} \models H$$

For all assignment $\alpha \colon \{P, Q, R, \dots\} \to \{0, 1\}$, if $\alpha(F \to (G \wedge H)) = 1$ and $\alpha((F \wedge G) \vee H) = 1$ then $\alpha(H) = 1$

Proof. Let α be an arbitrary assignment. Suppose that $F \to (G \wedge H)$ is true (under α), and $(F \wedge G) \vee H$ is true (under α).

Suppose, for a contradiction, that H is false.

$$\begin{aligned}
&(F \wedge G) \vee H, \neg H \quad \therefore F \wedge G \\
&(F \wedge G) \quad \therefore F \\
&F \to (G \wedge H), F \quad \therefore G \wedge H \\
&G \wedge H \quad \therefore H \\
&\neg H, H \quad \textit{gives the contradiction} \\
&\therefore H
\end{aligned}$$

□

Lecture 13, Sept. 30

13.1 Example.

$$\{F \to (G \wedge H), (F \wedge G) \vee H\} \vDash H$$

Proof. Proof by contradiction. Suppose H is false

$$(F \wedge G) \vee H, \neg H \quad \therefore F \wedge G$$
$$(F \wedge G) \quad \therefore F$$
$$F \to (G \wedge H), F \quad \therefore G \wedge H$$
$$G \wedge H \quad \therefore H$$
$$\neg H, H \quad \textit{gives the contradiction}$$
$$\therefore H$$

□

Here is a derivation for the valid argument

$S = \{F \to (G \wedge H), (F \wedge G) \vee H, \neg H\} \vDash F \to (G \wedge H)$	*by V1*
$S \vDash (F \wedge G) \vee H$	*by V1*
$S \vDash \neg H$	*V1*
$S \vDash F \wedge G$	*V18 on line 2,3*
$S \vDash F$	*V11 on line 4*
$S \vDash G \wedge H$	*V23 on line 1,5*
$S \vDash H$	*by V12 on 6*
$\{F \to (G \wedge H), (F \wedge G) \vee H\} \vDash H$	*V5 on line 3,7*

Here is another proof

Proof. Let α be an arbitrary assignment

Suppose that $F \to (G \wedge H)$ is true (under α)

Suppose that $(F \wedge G) \vee H$ is true

Note that wither $F \wedge G$ is true or H is true

Case 1. Suppose $F \wedge G$ is true. [V14]

Since $F \wedge G \therefore F$ [V11]

Since $F \to (G \wedge H)$ and $F \therefore F$ [V23]

Since $G \wedge H \therefore H$ [V12]

Case 2. Support that H is true. [V14]

Then H is true. [V1]

In either case, we have proven H [V14]

□

Here is a corresponding derivation of valid argument

1. $S = \{F \to (G \wedge H), (F \wedge G)\} \vDash F \to (G \wedge H)$
2. $S \vDash F \wedge G$
3. $S \vDash F$
4. $S \vDash G \wedge H$
5. $S \vDash H$
6. $\{F \to (G \wedge H), H\} \vDash H$
7. $\{F \to (G \wedge H), (F \wedge G) \vee H\} \vDash H$

13.2 Example. Show that

$$\{(F \vee \neg G) \to H, F \leftrightarrow (G \wedge \neg H)\} \vDash \neg(H \to F)$$

Solution: We need to show that

for every assignment α

if $(F \vee \neg G) \to H$ is true under α

and $F \leftrightarrow (G \wedge \neg H)$ is true

then $H \to F$ is false

Proof. Let α be arbitrary assignment

Suppose $(F \vee \neg G) \to H$ is true

Suppose $F \leftrightarrow (G \wedge \neg H)$ is true.

[We need to show that $H \to F$ is false. Notice that $\neg(H \to F) \equiv H \wedge \neg F$. So we need to show that H is true and F is false.]

Suppose, for a contradiction, that H is false.

Since $(F \vee \neg G) \to H$ and $\neg H$ $\quad \therefore \neg(F \vee \neg G)$

Since $\neg(F \vee \neg G)$ $\quad \therefore \neg F \wedge G$

Since $F \leftrightarrow (G \wedge \neg H)$ and $\neg F$ $\quad \therefore \neg(G \wedge \neg H)$

Since G and $\neg H$ $\quad \therefore G \wedge \neg H$

Since $G \wedge \neg H$ and $\neg(G \wedge \neg H)$ we have a contradiction

So H is true.

Since H is true, then $\neg\neg H$

Since $\neg\neg H$ we have $\neg G \vee \neg\neg H$

Since $\neg G \vee \neg\neg H$ we have $\neg(G \wedge \neg H)$

Since $F \leftrightarrow (G \wedge \neg H)$ and $\neg(G \wedge \neg H)$, we have $\neg F$

Since H and $\neg F$, we have $H \wedge \neg F$

Since $H \wedge \neg F$ we have $\neg(H \rightarrow F)$

□

$$\{(F \vee \neg G) \rightarrow H, F \leftrightarrow (G \wedge \neg H)\} \vDash \neg(H \rightarrow F)$$

Here is a derivation

Proof.

1. $S = \{(F \vee \neg G) \rightarrow H, F \leftrightarrow (G \wedge \neg H), \neg H\} \vDash \neg(H \rightarrow F)$ v1
2. $S \vDash F \leftrightarrow (G \wedge \neg H)$ v1
3. $S \vDash \neg H$ v1
4. $S \vDash \neg(F \vee \neg G)$ v24
5. $S \vDash \neg F \wedge \neg\neg G$ v45,E8
6. $S \vDash \neg F \wedge G$ v11 on 5
7. $S \vDash \neg F$ v31 on 2,6
8. $S \vDash \neg\neg G$ 12 on 5
9. $S \vDash G$ v45,e2 on 8
10. $S \vDash G \wedge \neg H$ v10 on 9,3
11. $T = \{(F \wedge \neg G) \rightarrow H, F \leftrightarrow (F \wedge \neg H)\} \vDash H$ v5 on 10,7
12. $T \vDash \neg\neg H$
13. $T \vDash \neg G \vee \neg\neg H$
14. $T \vDash \neg(G \wedge \neg H)$
15. $T \vDash F \leftrightarrow (G \wedge \neg H)$
16. $T \vDash \neg F$
17. $T \vDash H \wedge \neg F$
18. $T \vDash \neg(H \rightarrow F)$

□

Lecture 14, Oct. 5

14.1 Example.

$$\models \forall x\ (\exists y\ \neg xRy \vee \exists y\ yRx)$$

Solution.

$$\begin{aligned} &\forall x\ (\exists y\ \neg xRy \vee \exists y\ yRx) \\ [E28]\ &\equiv \forall x\ (\neg \forall y\ xRy \vee \exists y\ yRx) \\ [E20]\ &\equiv \forall x\ (\forall y\ xRy \to \exists y\ yRx) \end{aligned}$$

Proof. Let u be an arbitrary non-empty set. Let R be an arbitrary binary relation on u (that is $R \subseteq u^2$)

Let $x \in u$ be arbitrary.

Suppose that $\forall y\ xRy$.

Then in particular we have xRx. [V38]

Since xRx it follows that $\exists y\ yRx$. [V40]

We have proven that $\forall y\ xRy \to \exists y\ yRx$. [V19]

Since x was arbitrary, we have proven that $\forall x\ (\forall y\ xRy \to \exists y\ yRx)$. [V37]

Since u and R are arbitrary, we have proven that $\models \forall x\ (\forall y\ xRy \to \exists y\ yRx)$. [V37, V19]

Since equivalence, we have proven that $\models \forall x\ (\exists y\ \neg xRy \vee \exists y\ yRx)$.

□

	1	$\{\forall y\ xRy\} \models \forall y\ xRy$	V1
	2	$\{\forall y\ xRy\} \models xRx$	V38 on 1
	3	$\{\forall y\ xRy\} \models \exists y\ yRx$	V40 on 2
Here is a derivation	4	$\models (\exists y\ xRy \to \exists y\ yRx)$	V19 on 3
	5	$\models (\neg \forall y\ xRy \vee \exists y\ yRx)$	V45, E20
	6	$\models (\exists y\ \neg xRy \vee \exists y\ yRx)$	V45, E28
	7	$\forall x\ (\exists y\ \neg xRy \vee \exists y\ yRx)$	V37 on 6

14.2 Example. For $a, b, c \in \mathbb{Z}$, show that if $a \mid b$ and $b \mid c$ then $a \mid c$

(We say a divides b, or a is a factor of b, of b is a multiple of a, and we write $a \mid b$, when $\exists x\ b = a \cdot x$)

Here is a proof in standard mathematical language.

Proof. Let $a, b, c \in \mathbb{Z}$ be arbitrary.

Suppose that $a \mid b$ and $b \mid c$.

Since $a \mid b$, choose $u \in \mathbb{Z}$ so that $b = a \cdot u$

Since $a \mid b$, choose $v \in \mathbb{Z}$ so that $c = b \cdot v$

Since $b = a \cdot u$ and $c = b \cdot v$

We have $c = (a \cdot u) \cdot v = a \cdot (u \cdot v)$

Thus $a \mid c$ (we have $\exists x \; c = a \cdot x$ choose $x = u \cdot v$)

□

Here is a step-by-step proof to show that

$$\{\exists x \; b = a \times x, \exists x \; c = b \times x, \forall x \, \forall y \, \forall z \; ((x \times y) \times z) = (x \times (y \times z))\} \vDash \exists x \; c = a \times x$$

V37, v19. Let U be a non-empty set,

[V37, v19] Let × be a binary function on U.

[V9] Suppose $\exists x \; b = a \times x$,

[V9] Suppose $\exists x \; c = b \times x$,

[V9] Suppose $\forall x \, \forall y \, \forall z \; ((x \times y) \times z) = (x \times (y \times z))$

[V41] Since $\exists x \; b = a \times x$, we can choose $u \in U$ so that $b = a \times u$

[V41] Since $\exists x \; c = b \times x$, we can choose $v \in U$ so that $c = b \times v$

[V36]Since $b = a \times u$ and $c = b \times v$, we have $c = (a \times u) \times v$

[V38] Since $\forall x \, \forall y \, \forall z \; ((x \times y) \times z) = (x \times (y \times z))$ we have $\forall y \, \forall z \; ((a \times y) \times z) = (a \times (y \times z))$

[V38] Since $\forall y \, \forall z \; ((a \times y) \times z) = (a \times (y \times z))$ we have $\forall z \; ((a \times u) \times z) = (a \times (u \times z))$

[V38] Since $\forall z \; ((a \times u) \times z) = (a \times (u \times z))$ we have $((a \times u) \times v) = (a \times (u \times v))$.

[V35] Since $c = (a \times u) \times v$ and $((a \times u) \times v) = (a \times (u \times v))$, we have $c = a \times (u \times v)$

[V40] Since $c = a \times (u \times v)$ we have proven that $\exists x \; c = a \times x$

□

Lecture 15, Oct. 5

15.1 Definition. An **ordered n-tuple** with entries in a set A, is a function $a\colon \{1,2,3,\dots\} \to A$ where we write $a(k)$ as a_k.

We write $a = (a_1, a_2, \dots)$ to indicate that $a = \{1,2,3,\dots\} \to A$ is given by $a(k) = a_k$ for $k \in \{1,2,3,\dots,n\}$

The set of all such n-tuples is denoted by A^n

$$A^n = \{(a_1, a_2, \dots) \mid \text{ } each\ a_{\mathbb{Z}} \in A\}$$

15.2 Definition. A **sequence** with **entries** or **terms** in a set A is a function

$$a\colon \{1,2,3,\dots\} \to A$$

Where we write $a(k) = a_k$ or sometimes a function

$$a\colon \{m, m+1, m+2, \dots\} \to A$$

where $m \in \mathbb{Z}$.

We write $a = (a_k)_{k \geq m} = (a_m, a_{m+1}, \dots)$

or we write $a = \{a_k\}_{k \geq m} = \{a_m, a_{m+1}, \dots\}$

to indicate that $a = \{m, m+1, \dots\} \to A$ is given by $a(k) = a_k$

Remark. For sets A and B we define A^B to be the set of all functions

$$f: B \to A$$

Also the integer n is defined to be

$$n = \{0, 1, 2, \dots, n-1\}$$

So Actually

$$A^n = A^{\{0,1,2,\dots,n-1\}} = \{a\colon \{0,1,\dots,n-1\} \to A\}$$

and we write elements in A^n as $(a_0, a_1, \dots a_{n-1})$

And the set of sequences with entries in A is the set $A^{\mathbb{N}} = \{a\colon \{0,1,2,\dots\} \to A\}$

15.3 Definition. We say that a sequence is defined in **closed-form** when we are given a formula for a_k in terms of k.

We say that a sequence is defined **recursively** when we are given a formula for a_n in terms of k and in terms of previous terms a_i in the sequence.

15.4 Example. Fibonacci Sequence

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

15.5 Example. When we write

$$S_n = \sum_{k=1}^{n} \frac{1}{k^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots$$

we mean that $S_1 = 1$ and $S_n = S_{n-1} + \dfrac{1}{n^2}$

15.6 Example. When we write

$$P_n = \prod_{k=1}^{n} \frac{2k-1}{2k}$$

We mean that $P_1 = \dfrac{1}{2}$ and $P_n = P_{n-1} \cdot \dfrac{2n-1}{2n}$

15.7 Example. When we write $n!$, we mean that $0! = 1$ and $n! = (n-1)! \cdot n$ for $n \geq 1$

15.8 Example. In Set Theory, we define addition on $\mathbb{N}$, recursively as follows

$$0 = \emptyset, 1 = \{0\}, x + 1 = x \cup \{x\}$$

For $n \in \mathbb{N}$, $n + 0 = n$, $n + (m+1) = (n+m) + 1 = (n+m) \cup \{(n+m)\}$

15.9 Theorem. Mathematical Induction *Let $F(n)$ be a mathematical statement about an integer n. Let $m \in \mathbb{Z}$*

Suppose $F(m)$ is true. (that is $[F]_{n \mapsto m}$)

Suppose that for all $k \geq m$, if $F(k)$ is true then $F(k+1)$ is true.

Then $F(n)$ is true for all $n \geq m$.

15.10 Example. Define a_n recursively by $a_1 = 1$ and $a_{n+1} = \dfrac{n}{n+1} \cdot a_n + 1$. Find a closed-form formula for a_n

Solution. We have $a_1 = 1$, $a_2 = \dfrac{3}{2}$, $a_3 = \dfrac{4}{2}, \dots$

It appears that $a_n = \dfrac{n+1}{2}$

When $n = 1$, $\cdots$

Suppose $a_k = \dfrac{k+1}{2}$

When $n = k+1$ we have

$$\begin{aligned} a_n = a_{k+1} &= \frac{k}{k+1} \cdot a_k + 1 \\ &= \frac{k}{k+1} \cdot \frac{k+1}{2} + 1 \\ &= \frac{k+2}{2} \\ &= \frac{(k+1)+1}{2} \\ &= \frac{n+1}{2} \end{aligned}$$

By induction, $a_n = \dfrac{n+1}{2}$ forall $n \geq 1$

15.11 Exercise.

1. $$\sum_{k=1}^{n} k^3$$

2. $$\prod_{k=1}^{n} (1 - \frac{1}{k^2})$$

Lecture 16, Oct. 5

16.1 Theorem. *Let $F(n)$ be a statement about an integer n. Let $m \in \mathbb{Z}$*

Suppose $F(m)$ is true

Suppose that for all $k \geq m$, if $F(k)$ is true then $F(k+1)$ is true

Then $F(n)$ is true for all $n \geq m$

Proof Method Let $F(n)$ be a statement about an integer and let $m \in \mathbb{Z}$

To prove $F(n)$ is true for all $n \geq m$, we can do the following.

1. Prove that $F(n)$ is true
2. Let $k \geq m$ be arbitrary and suppose, inductively, that $F(k)$ is true
3. Prove $F(k+1)$ is true

Alternatively, suppose $F(k-1)$ prove $F(k)$

A slightly different proof method To prove that $F(n)$ is true for all $n \geq m$ we can do the following:

1. Prove that $F(m)$ is true and that $F(m+1)$ is true
2. Let $k \geq m+2$ be arbitrary and suppose that $F(k-1)$ and $F(k-2)$ are true
3. Prove that $F(k)$ is true

Another Proof Method we can prove that $F(n)$ is true for all $n \geq m$ as follows.

1. Let $n \geq m$ be arbitrary and suppose that $F(k)$ is true for all k with $m \leq k < n$
2. prove that $F(n)$ is true.

16.2 Theorem. Strong Mathematical Induction *Let $F(n)$ be a statement about an integer n and let $m \in \mathbb{Z}$*

Suppose that for all $n \geq m$, if $F(k)$ for all $k \in \mathbb{Z}$ with $m \leq k < n$, then $F(n)$ is true.

Then $F(n)$ is true for all $n \geq m$.

Proof. Let $G(n)$ be a statement "F(n) is true for all $k \in \mathbb{Z}$ with $m \leq k < n$"

Note that $G(m)$ is true vacuously. (since there is no value of $k \in \mathbb{Z}$ with $m \leq k < n$)

Let $n \geq m$ be arbitrary.

Suppose $G(n)$ is true, that is "$F(n)$ is true for all $k \in \mathbb{Z}$ with $m \leq k < n$"

Since $F(n)$ is true for all $k \in \mathbb{Z}$ with $m \leq k < n$, then $F(n)$ is true for all $k \in \mathbb{Z}$ with $m \leq k < n+1$. In other words, $G(n+1)$ is true.

Now let $n \geq m$ be arbitrary. Since $G(k)$ is true for all $k \geq m$, in particular $G(n+1)$. In other words, $F(k)$ is true for all k with $m \leq k < n+1$. In particular $F(n)$ is true

Since $n \geq m$ was arbitraty, $F(n)$ is true for all $n \geq m$. □

16.3 Example. Let $(x_n)_{n\geq 0}$ be the sequence which is defined recursively by $x_0 = 2$, $x_1 = 2$ and $x_n = 2x_{n-1}+3x_{n-2}$ for all $x \geq 2$

Find a closed formula for x_n

Solution. Observe that $x_n = 3^n + (-1)^n$

When $n = 0$, $x_0 = 2$ and $3^0 + (-1)^0 = 2$, so $x_n = 3^n + (-1)^n$ is true when $n = 0$

When $n = 1$, $x_1 = 2$ and $3^1 + (-1)^1 = 2$, so $x_n = 3^n + (-1)^n$ is true when $n = 1$

Let $n \geq 2$ be arbitrary.

Suppose that $x_{n-1} = 3^{n-1} + (-1)^{n-1}$ and $x_{n-2} = 3^{n-2} + (-1)^{n-2}$

$$\begin{aligned} x_n &= 2x_{n-1} + 3x_{n-2} \\ &= 2(3^{n-1} + (-1)^{n-1}) + 3(3^{n-2} + (-1)^{n-2}) \\ &= 9^{n-2} + (3-2)(-1)^{n-2} \\ &= 3^n + (-1)^n \end{aligned}$$

By induction, $x_n = 3^n + (-1)^n$ for all $n \geq 0$

Binomial Theorem

16.4 Definition. For $n, k \in \mathbb{N}$ with $0 \leq k \leq n$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!}$$

Lecture 17, Oct. 7

Binomial Theorem

17.1 Definition. For $n, k \in \mathbb{N}$ with $0 \leq k \leq n$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!}$$

The number of ways to choose k of n objects,

1. If we choose the k objects with replacement (or with repetition), and if order matters, is n^k
2. If we choose the k objects without replacement, and if order matters, is $\dfrac{n!}{(n-k)!}$. (In particular the number of ways to arrange n objects is $n!$)
3. If we choose the k objects without replacement, and if order does not matters (so we form a k-element set), is $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$

Note. For $n, k \in \mathbb{N}$ with $0 \leq k \leq n$, $\binom{n}{0} = 1$, $\binom{n}{n} = 1$, $\binom{n}{k} = \binom{n}{n-k}$, $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$

Proof.

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} \\
&= \frac{n!(k+1)}{(k+1)!(n-k)!} + \frac{n!(n-k)!}{(k+1)!(n-k)!} \\
&= \frac{n!(k+1+n-k)}{(k+1)!(n-k)!} \\
&= \frac{(n+1)!}{(k+1)!(n+1-k-1)!} \\
&= \binom{n+1}{k+1}
\end{aligned}$$

□

Pascal Triangle

17.2 Example.

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

17.3 Theorem. Binomial Theorem *For $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$ we have the following formula*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Proof. When $n = 0$,

$$(a+b)^0 = 1$$

$$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \binom{0}{0} a^0 b^0 = 1$$

When $n = 1$,

$$(a+b)^1 = a + b$$

$$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b$$

Let $n \geq 1$ be arbitrary.

Suppose, inductively, that

$$(a+b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + \binom{n}{n} b^n$$

Then

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)(\binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n-1} a^1 b^{n-1} + \binom{n}{n} b^n) \\
&= \binom{n}{0} a^{n+1} + \binom{n}{1} a^n b + \cdots + \binom{n}{n-1} a^2 b^{n-1} + \binom{n}{n} ab^n \\
&\qquad + \binom{n}{0} a^n b + \binom{n}{1} a^{n-1} b^2 + \cdots + \binom{n}{n-1} a^1 b^n + \binom{n}{n} b^{n+1} \\
&= \binom{n+1}{0} a^{n+1} + \binom{n+1}{1} a^n b + \cdots + \binom{n+1}{n} ab^n + \binom{n+1}{n+1} b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n-k}
\end{aligned}$$

By induction, it follows that $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ for all $n \geq 0$ □

17.4 Example.

$$(x+2)^6 = x^6 + 12x^5 + 60x^4 + 160x^3 + 240x^2 + 192x + 64$$

17.5 Example. Find the coefficient of x^8 in the expansion of

$$(5x^3 - \frac{2}{x^2})^{11}$$

Solution.

$$\begin{aligned}
(5x^3 - \frac{2}{x^2})^{11} &= \sum_{k=0}^{11} \binom{11}{k} (5x^3)^{11-k} (-\frac{2}{x^2})^{11} \\
&= \sum_{k=0}^{11} (-1)^k \binom{11}{k} 5^{11-k} 2^k x^{3(11-k)-2k}
\end{aligned}$$

To get $3(11-k)-2k=8$ that is $k=5$

So that the coefficient of x^8 is $(-1)^5\binom{11}{5}5^{11-5}2^5=-231000000$

17.6 Example. Find

$$\sum_{k=0}^{n}\binom{2n}{2k}\frac{1}{2^k}$$

Solution.

$$(1+\frac{1}{2})^{2n}=\binom{2n}{0}+\binom{2n}{1}\frac{1}{2}+\dots$$

$$(1-\frac{1}{2})^{2n}=\binom{2n}{0}-\binom{2n}{1}\frac{1}{2}+\dots$$

And replace 2 by $\sqrt{2}$