Transition to advanced mathematics

University of Houston - MATH 3325

Spring 2020

Textbook: Smith, Eggen, St. Andre - A Transition to Advanced Mathematics, 7th edition

Chapters covered: 1, 2.1-5, 3.1-4, 4.1-4, 5

*note: The sections in these notes do not correspond to the chapters

Contents

1 Propositional logic

Definition 1.1: proposition

A sentence that has only one truth value; it is either true (T) or false (F).

Definition 1.2: negation

Let P be a proposition. Then $\neg P$ is its *negation* and is true when P is false.

Truth table for $\neg P$

P	$\neg P$
T	F
F	T

Definition 1.3: conjunction

Let P and Q be propositions. Then $P \wedge Q$ is the *conjuction* of P and Q and is true only when both P and Q are true.

$P \wedge Q$ can be translated as "P and Q". Other words instead of "and" are: but, while, although.

Truth table for $P \wedge Q$

P	Q	$P \wedge Q$
T	T	T
F	T	F
T	F	F
F	F	F

Definition 1.4: disjunction

Let P and Q be propositions. Then $P \vee Q$ is the *disjuction* of P and Q and is true when at least on of P or Q are true.

Truth table for $P \vee Q$

P	Q	$P \vee Q$
T	T	T
F	T	T
T	F	T
F	F	F

Definition 1.5: tautology

A proposition that is true for every assignment of truth values to its components.

In other words, a tautology is when a proposition has all true values in its truth table.

Definition 1.6: contradiction

A proposition that is true for every assignment of truth values to its components.

In other words, a contradiction is when a proposition has all false values in its truth table.

Proof 1.1: propositional equivalence

Two propositional forms are equivalent if and only if they have the same truth tables.

To prove that two propositions are equivalent, write out a truth table for each.

Definition 1.7: conditional

Let P and Q be propositions. Then $P \implies Q$ is a conditional sentence that means "If P, then Q". P is called the *antecendent* and Q is called the *consequent*. The conditional sentence $P \implies Q$ is true if and only if P is false or Q is true.

Helpful note:

$$P \implies Q \text{ is equivalent to } \neg P \vee Q$$

Truth table for $P \implies Q$

P	Q	$P \implies Q$
T	T	T
F	T	T
T	F	F
F	F	T

Definition 1.8: converse

Let P and Q be propositions. The *converse* of $P \implies Q$ is $Q \implies P$.

The converse of a proposition is not always true.

Definition 1.9: contrapositive

Let P and Q be propositions. The *contrapositive* of $P \implies Q$ is $\neg Q \implies \neg P$.

The contrapositive is always equivalent to the original proposition.

Definition 1.10: biconditional

Let P and Q be propositions. Then $P \iff Q$ is a biconditional sentence that means "P if and only if Q". The biconditional sentence $P \iff Q$ is true when P and Q have the same truth values.

Truth table for $P \iff Q$

P	Q	$P \iff Q$
T	T	T
F	T	F
T	F	F
F	F	T

Theorem 1.1: Propositional equivalences

A list of propositions and equivalent forms.

$$P \qquad \neg\neg P$$

$$\neg(P \wedge Q) \qquad \neg P \vee \neg Q$$

$$\neg(P \vee Q) \qquad \neg P \wedge \neg Q$$

$$P \implies Q \qquad \neg P \vee Q$$

$$P \iff Q \qquad (P \implies Q) \wedge (Q \implies P)$$

$$\text{“exclusive or”} \qquad (P \vee Q) \wedge \neg(P \wedge Q)$$

1.1 Quantifiers

Definition 1.11: open sentence (predicate)

A sentence that contains variables. For example, $P(x)$ is an open sentence with a variable x.

An open sentence becomes a proposition when its variables are assigned values.

Definition 1.12: universe of discourse

The set of all objects that a variable in an open sentence can be.

Definition 1.13: existential quantifier

The symbol $\exists$ is the existential quantifier that means ”there exists”.

For example, $(\exists x)P(x)$ means ”There exists x such that $P(x)$”.

Definition 1.14: unique existential quantifier

The symbol $\exists!$ is the unique existential quantifier that means ”there exists only one”.

Definition 1.15: universal quantifier

The symbol $\forall$ is the universal quantifier that means ”for all”.

For example, $(\forall x)P(x)$ means ”For all x, $P(x)$”.

Theorem 1.2: Negation of quantified sentences

$\neg(\forall x)A(x)$ is equivalent to $(\exists x)\neg A(x)$

$\neg(\exists x)A(x)$ is equivalent to $(\forall x)\neg A(x)$

2 Proof techniques

Rules of writing proofs:

- At any time, you can state an axiom, assumption, or previously proved result.
- At any time, you can state an equivalent line.
- At any time, you can state a tautology.
- After proving $P \implies Q$, you can state that Q is true (modus ponens).

General tips:

- Don't start a sentence with a symbol.
- If a definition has “if” in it, it usually means “if and only if”.
- Use proper English and grammar.

Proof 2.1: direct proof

Assume P
$\vdots$
Therefore Q.
Thus $P \implies Q$.

tip: work backwards from the intended result to figure out what the next step should be.

Proof 2.2: proof by exhaustion

Examine every possible case.

If proving something with integers, use exhaustion with even and odd numbers.

If proving something about an interval, check inside and outside the interval.

Proof 2.3: proof by contraposition

Assume $\neg Q$
$\vdots$
Therefore $\neg P$.
So $\neg Q \implies \neg P$, and by contraposition, $P \implies Q$.

tip: use this when there is a negation in the claim.

Proof 2.4: proof by contradiction

Assume $\neg P$
$\vdots$
Therefore Q
$\vdots$
Therefore $\neg Q$
Since $Q \wedge \neg Q$ is a contradiction, therefore P.

Proof 2.5: proof of "if and only if"

Assume P
$\vdots$
Therefore Q
So $P \implies Q$.

Assume Q
$\vdots$
Therefore P
So $Q \implies P$.

Thus $P \iff Q$.

Proof 2.6: direct proof of "for all"

Let x be arbitrary.
$\vdots$
Therefore $P(x)$
Since x is arbitrary, then $(\forall x)P(x)$ is true.

Proof 2.7: proof by contradiction of "for all"

Suppose $\neg(\forall x)P(x)$.
Then $(\exists x)\neg P(x)$.
Let t be an object such that $\neg P(t)$.
$\vdots$
Therefore a contradiction. Since $(\exists x)\neg P(x)$ is false, $(\forall x)P(x)$ is true.

Proof 2.8: constructive proof

To prove $(\exists x)P(x)$, name an t such that $P(t)$.

Proof 2.9: proof by contradiction of "there exists"

Suppose $\neg(\exists x)P(x)$.
Then $(\forall x)\neg P(x)$.
$\vdots$
Therefore a contradiction. Since $(\forall x)\neg P(x)$ is false, $(\exists x)P(x)$ is true.

Proof 2.10: proof of unique existence

Prove $(\exists x)P(x)$.
Assume that y and z are objects in the universe such that $P(y)$ and $P(z)$ are true.
$\vdots$
Therefore $y = z$. Thus $(\exists! x)P(x)$ is true.

Proof 2.11: proof by weak induction

Let $S \subseteq \mathbb{N}$ be the set of all possible n.

1. Show that the base case is true.
2. Suppose that $P(n)$ is true for some $n \in S$.
   $\vdots$
   Thus $P(n+1)$ is true.
3. So $P(n)$ is true for all $n \in S$.

Proof 2.12: proof by strong induction

Let $S \subseteq \mathbb{N}$ be the set of all possible n.

1. Show that the base case is true.
2. Suppose that up to $P(n-1)$ is true for some $n \in S$.
   $\vdots$
   Thus $P(n)$ is true.
3. So $P(n)$ is true for all $n \in S$.

2.1 Proofs to know

The square root of 2 is an irrational number.

Proof. □

There are infinite primes.

Proof. □

3 Naïve set theory

Definition 3.1: set

A collection of objects

Definition 3.2: element

An *element* is an object in a set.

if x is element of set A, then

$$x \in A$$

if x is not an element of set A, then

$$x \notin A$$

Definition 3.3: empty set

the unique set with no elements, denoted by $\{\}$ or $\varnothing$

Definition 3.4: subset

$A \subseteq B$ if and only if every element of A is also an element of B

Definition 3.5: proper subset

$A \subset B$ if and only if every element of A is also an element of B and $A \neq B$

Definition 3.6: finite set

a set is finite if it is empty or has n elements

Definition 3.7: infinite set

a set is infinite if it is not finite

4 Combinatorics

5 Elementary number theory

Definition 5.1: division

Let $a, b \in \mathbb{Z}$. Then a divides b if and only if there exists $k \in \mathbb{Z}$ such that $b = ak$.

It is written $a \mid b$.

Definition 5.2: perfect square

A number is a *perfect square* if and only if it is equal to k^2 for some natural number k.

Definition 5.3: prime

A natural number p is *prime* if and only if $p \neq 1$ and whenever k is a natural number such that $k \mid p$, then $k = p$.

Definition 5.4: unit

The number 1.

5.1 Numbers

Definition 5.5: number systems

$\mathbb{N}$ is the set of all natural numbers

$\mathbb{Z}$ is the set of all integers

$\mathbb{Q}$ is the set of all rational numbers

$\mathbb{R}$ is the set of all real numbers

$\mathbb{C}$ is the set of all complex numbers

Theorem 5.1: Fundamental theorem of arithmetic

Every integer greater than 1 is either a prime or can be represented by a unique product of primes

Definition 5.6: even

An integer x is *even* if and only if there exists $k \in \mathbb{Z}$ such that $x = 2k$.

Definition 5.7: odd

An integer x is *odd* if and only if there exists $k \in \mathbb{Z}$ such that $x = 2k + 1$.

Definition 5.8: rational

A number x is *rational* if and only if there exists $p, q \in \mathbb{Z}$ with $q \neq 0$ such that $x = p/q$. Rational numbers have terminating or repeating decimals. All other numbers are irrational.

The Peano axioms completely describes the natural numbers.

Definition 5.9: Peano axioms

1. There is a natural number called 1.
2. Every natural number n has a unique successor $S(n)$ which is also a natural number.
3. Distinct numbers have distinct successors.
4. 1 is not the successor of any natural number.
5. If a property is possessed by 1 and also n, then $S(n)$ also has that property. So all the natural numbers have that property.

Theorem 5.2: Division algorithm

Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Then there exists $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that

$$b = aq + r$$

Definition 5.10: common divisor

Let $a, b \in \mathbb{N}$. A *common divisor* of a and b is a natural number d such that $d \mid a$ and $d \mid b$.

The *greatest common divisor* is the largest of such numbers. It is written as $\gcd(a, b)$.

Lemma 5.1: Bézout's lemma

Let $a, b \in \mathbb{N}$. Then there exist $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b)$$

Theorem 5.3

Let $a, b \in \mathbb{N}$. If d is a common divisor of a and b, then

$$d \mid \gcd(a, b)$$

Lemma 5.2: Euclid's lemma

Let p be prime and $a, b \in \mathbb{N}$. If $p \mid ab$, then

$$p \mid a \quad \text{or} \quad p \mid b$$

Definition 5.11: common multiple

Let $a, b \in \mathbb{N}$. A *common multiple* of a and b is a natural number c such that $a \mid c$ and $b \mid c$.

The *least common multiple* is the smallest of such numbers. It is written as $\operatorname{lcm}(a, b)$.

Theorem 5.4

Let $a, b \in \mathbb{N}$. If c is a common multiple of a and b, then

$$\operatorname{lcm}(a, b) \mid c$$

5.1.1 Algorithm for computing $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$

Let $a, b \in \mathbb{N}$ and $p_1 \dots p_n$ be distinct primes. Then

$$a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$$
$$b = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$$

So,

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_n^{\min(e_n, f_n)}$$

$$\operatorname{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_n^{\max(e_n, f_n)}$$

Theorem 5.5

Let $a, b \in \mathbb{N}$. Then
$$a \cdot b = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$$

5.2 Modular arithmetic

Definition 5.12

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then

$$a \equiv b \mod n \iff n \mid a - b$$

Theorem 5.6: Freshman's Dream

Let p be prime. If $x, y \in \mathbb{Z}$, then

$$(x + y)^p \equiv x^p + y^p \mod p$$

Theorem 5.7: Fermat's Little theorem (version 1)

Let p be prime. If $a \in \mathbb{Z}$, then
$$a^p \equiv a \mod p$$

Theorem 5.8: Fermat's Little theorem (version 2)

Let p be prime. If $a \in \mathbb{Z}$ such that $p \nmid a$, then

$$a^{p-1} \equiv 1 \mod p$$

6 Relations

Definition 6.1: relation

Let A and B be sets. R is a *relation* from A to B if and only if R is a subset of $A \times B$. A relation from A to A is called a relation *on* A. If $(a, b) \in R$, we write $a\,R\,b$ and "a is related to b".

Definition 6.2: identity relation

For any set A, the relation $I_A = \{(x, x) : x \in A\}$ is called the identity relation on A.

Definition 6.3: inverse relation

If R is a relation from A to B, then the inverse of R is the relation

$$R^{-1} = \{(y, x) : (x, y) \in R\}.$$

Definition 6.4: composition of relations

Let R be a relation from A to B, and let S be a relation from B to C. The composite of R and S is

$$S \circ R = \{(a, c) : there exists b \in B such that (a, b) \in R and (b, c) \in S\}.$$

$$Dom(S \circ R) \subseteq Dom(R)$$

Definition 6.5: equivalence relation

A relation R on a set A is an equivalence relation on A if and only if R is reflexive on A, symmetric, and transitive.

Proof 6.1: proving equivalence

Let A be a set and R be a relation on A. R is reflexive on A if and only if forall $x \in A$,$x\,R\,x$.

R is symmetric if and only if for all $x, y \in A$,if $x\,R\,y$, then $y\,R\,x$.

R is transitive if and only if for all $x, y, z \in A$,if $x\,R\,y$ and $y\,R\,z$, then $x\,R\,z$.

Thus R is an equivalence relation.

Definition 6.6: antisymmetry

A relation R on a set A is antisymmetric if and only if for all $x, y \in A$, if $x\,R\,y$ and $y\,R\,x$, then $x = y$.

Definition 6.7: partial order

A relation R on a set A is a partial order (or partial ordering) for A if R is reflexive on A, antisymmetric, and transitive. A set A with partial order R is called a partially ordered set, or poset.

Definition 6.8: immediate predecessor

Let R be a partial ordering on a set A and let $a, b \in A$ with $a \neq b$. Then a is an immediate predecessor of b if and only if $a\,R\,b$ and there does not exist $c \in A$ such that $a \neq c$, $a \neq$, $a\,R\,c$ and$c\,R\,b$.

Definition 6.9: total order

A partial ordering R on A is called a linear order (or total order) on A if for any two elements x and y of A, either $x\,R\,y$ or $y\,R\,x$.

7 Functions

8 Cardinality