1.5/1.6/1.7 Mathematical Reasoning & Methods of Proof

We will learn:

1. Rules of reasoning; how to reason correctly
2. Methods of proof; how to show whether a given (mathematical) statement is true or not

Argument: a sequence of statements with a conclusion
Valid: the conclusion follows from the truth of statements (**premises**)

Valid does NOT mean TRUE. Valid argument means that **if the premises are true, then the conclusion is true**. A valid argument may contain premises that are false:
e.g.,
"If we live on the Moon, then I am a carpenter. We live on the Moon. Therefore I am a carpenter"
This is a **valid** argument, as long as we assume "We live on the Moon" is a true statement. But the conclusion is **not necessarily true** since we know that one of the premises is false.

Valid Argument:

e.g.,

"If you have access to the network, then you can change your grade"

"You have access to the network"

∴ "You can change your grade"

$p \to q$

p

$\therefore q$

But since $p \to q$ in this argument is a false statement, the conclusion is false.

e.g.,

"If $\sqrt{2} > 3/2$ then $(\sqrt{2})^2 > (3/2)^2$."

"We know that $\sqrt{2} > 3/2$."

"Consequently $(\sqrt{2})^2 = 2 > (3/2)^2 = 9/4$."

Premises	**Reasoning**	**Conclusion**
True	Valid	Must be true
False	Valid	Even though the reasoning is valid, the conclusion can be false
True or False	Invalid	Even when the premises are true, the conclusion can be false

Rules of Inference: (Rules of reasoning)
Are used to draw conclusions from other assertions and tie the steps of a proof.
Basis of the rule of inference: **Modus ponens** or **law of detachment**

$(p \wedge (p \rightarrow q)) \rightarrow q$: Tautology

p	q	$p \rightarrow q$	$(p \wedge (p \rightarrow q)) \rightarrow q$
T	T	T	T
T	F	F	T
F	T	T	T
F	F	T	T

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

e.g.

If it is sunny today, then we'll play soccer. It is sunny today, so we'll play soccer.

e.g.

It is sunny now. Therefore, it's sunny or snowy now.

$$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$$

Addition Rule

e.g.

It is windy and raining now. Therefore, it is windy now.

$$\begin{array}{l} p \wedge q \\ \hline \therefore p \end{array}$$

Simplification Rule

Rule of Inference	Tautology	Name
p $\therefore\ p \vee q$	$p \rightarrow (p \vee q)$	Addition
$p \wedge q$ $\therefore\ p$	$(p \wedge q) \rightarrow p$	Simplification
p q $\therefore\ p \wedge q$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
P $p \rightarrow q$ $\therefore\ q$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus Ponens
$\neg q$ $p \rightarrow q$ $\therefore\ \neg p$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus Tollens
$p \rightarrow q$ $q \rightarrow r$ $\therefore\ p \rightarrow r$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Hypothetical Syllogism
$p \vee q$ $\neg p$ $\therefore\ q$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Disjunctive Syllogism

DO NOT MEMORIZE!!

What about $((p \oplus q) \wedge \neg p) \rightarrow q$??

e.g. Show that hypotheses:

"If you send me an email, then I will finish writing the program,"
"If you do not send me an email, then I will go to sleep early,"
"If I go to sleep early, then I will wake up feeling refreshed"

lead to the conclusion:
"If I do not finish writing the program, then I'll wake up feeling refreshed."

Let

- p: "you send me an email"
- q: "I'll finish writing the program"
- r: "I'll go to sleep early"
- s: "I'll wake up feeling refreshed"

Step	Reason
1. $p \rightarrow q$	hypothesis
2. $\neg p \rightarrow r$	hypothesis
3. $r \rightarrow s$	hypothesis
4. $\neg q \rightarrow \neg p$	contrapositive of step 1
5. $\neg q \rightarrow r$	hypothetical syllogism using steps 4 and 2
6. $\neg q \rightarrow s$	hypothetical syllogism using steps 5 and 3

Reached conclusion.

Rules of Inference for Quantified Statements

Universal instantiation:

$$\frac{\forall x\, P(x)}{\therefore\ P(c) \text{ if } c \in U}$$

U: universe of discourse (*domain*)

Universal generalization:

$$\frac{P(c) \text{ for an arbitrary (any) } c \in U}{\therefore\ \forall x\, P(x)}$$

Existential instantiation:

If $\exists x\, P(x)$ is true then we know some c exists s.t. $P(c)$ is true.

$$\frac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some element } c \in U}$$

Existential generalization:

If we know some c in U s.t. $P(c)$ is true then $\exists x\, P(x)$ is true

$$\frac{P(c) \text{ for some element } c \in U}{\therefore\ \exists x\, P(x)}$$

e.g.

i) "All lions are fierce"

ii) "Some lions do not drink coffee"

Does i) and ii) imply that "some fierce creatures do not drink coffee" ?

P(x): "x is a lion"

Q(x): "x is fierce"

R(x): "x drinks coffee"

Domain of P,Q,R is the set of all creatures.

i) $\forall x\ (P(x) \rightarrow Q(x))$

ii) $\exists x\ (P(x) \wedge \neg R(x))$

1. (ii) implies that there is some x_1 such that $P(x_1) \wedge \neg R(x_1)$ by Existential Instantiation.
2. Hence by (i) $Q(x_1)$ is true (using Simplification rule and Modus Ponens).
3. $\neg R(x_1)$ is also true by using again Simplification rule over step 1.
4. Then $Q(x_1) \wedge \neg R(x_1)$ by steps 2 and 3, implying that $\exists x\ (Q(x) \wedge \neg R(x))$ via Existential Generalization.

Fallacies

Types of **incorrect** reasoning:

Fallacy of affirming the conclusion:

e.g.

"If you have solved every problem in this book, then you know Discrete Math. You know Discrete Math. Therefore, you have solved every problem in this book."

$[(p \rightarrow q) \wedge q] \rightarrow p$ **NOT** a tautology

F when p is F and q is T

Fallacy of denying the hypothesis:

"If you have solved every problem in this book, then you know Discrete Math. You have not solved every problem in this book. Therefore, you don't know Discrete Math."

$[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ **NOT** a tautology

F when p is F and q is T

Begging the question fallacy: When one or more steps of a proof are based on the truth of the statement being proved (circular reasoning)

Methods of Proving Theorems

Theorem: A statement that can be shown to be true.

Proof: Arguments which show that a theorem is true.

Axiom (*postulate*): Underlying assumptions about a mathematical structure.
(Many theorems are later shown to be false by showing cases that the assumption does not hold !! **BE VERY CAREFUL WITH THE ASSUMPTIONS**)

Lemma: A simple theorem that is used in the proof of other theorems.

Corollary: A proposition that can be established directly from a theorem.

Conjecture: A statement whose truth-value is unknown (not falsified or proven yet). If a proof can be found, then it becomes a theorem.

Example: "Every even positive integer greater than 4 is the sum of two primes"
Goldbach's conjecture.

Direct proof:

Many theorems are implications:

$$p \to q$$

To prove, we need to show that whenever p is T, q is also T.
This implies that the case p true and q false never occurs.

e.g. p q
Prove that if n is odd, then n^2 is odd.
Let k be an integer such that
$n = 2k + 1 \Rightarrow n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2t + 1$ where $t = 2k^2 + 2k$ is an integer too

$$\therefore\ n^2 \text{ is odd.}$$

Indirect proof:

$$p \to q \;\equiv\; \neg q \to \neg p \ \text{(contrapositive)}$$

e.g.
Prove that if $3n + 2$ is odd, then n is odd.
Let n be even. Then $\exists k \in Z$ s.t. $n = 2k \Rightarrow 3n + 2 = 6k + 2 = 2(3k + 1) = 2t$ where $3k+1 = t \in Z$

$$\therefore\ 3n + 2 \text{ is even too.}$$

<u>DO NOT MEMORIZE NAMES OF PROOF TYPES</u>

Proof by contradiction:

Suppose that we want to prove that p is true. We start with the assumption that p is false and we proceed. If we end up with a contradiction, then we conclude that the assumption that "p is false" ($\neg$p) is false, that is, p is true.

e.g. Prove that $\sqrt{2}$ is irrational.

Suppose that it is not true, that is,

Suppose $\sqrt{2} = a/b$, **where integers *a* and *b* have no common factors** (every rational number can be represented this way).

$\Rightarrow 2 = a^2/\,b^2 \quad \Rightarrow 2b^2 = a^2$

$\Rightarrow a^2$ is even $\Rightarrow a$ is even $\quad \Rightarrow a = 2c$

$\therefore\ 2b^2 = 4c^2 \quad \Rightarrow b^2 = 2c^2$

$\Rightarrow b^2$ is even $\Rightarrow$ b is even $\Rightarrow b = 2d$

$\therefore\ 2 \mid a \ \wedge\ 2 \mid b \ \Rightarrow$ *a* and *b* have common factors $\Rightarrow$ **contradiction!**

$\therefore\ \sqrt{2}$ is irrational.

WHAT ABOUT $\sqrt{3}$ **??** (http://www.grc.nasa.gov/WWW/k-12/Numbers/Math/Mathematical_Thinking/irrationality_of_3.htm)

Proof by cases:

$p \rightarrow q$ s.t. $p \equiv (p_1 \vee p_2 \vee \ldots \vee p_n)$

The logical equivalence:

$[\,(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q\,] \equiv [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$

can be used as a rule of inference.

e.g.

Prove that if n is an integer not divisible by 3, then $n^2 \equiv 1 \pmod 3$.

q: $n^2 \equiv 1 \pmod 3$

p: n is not divisible by 3

p_1: $n \equiv 1 \pmod 3$, p_2 : $n \equiv 2 \pmod 3$ $\Rightarrow$ $p \equiv p_1 \vee p_2$

If p_1 is T: $\exists k \in Z$ where

$n = 3k + 1 \Rightarrow n^2 = 9k^2 + 6k + 1 = 3\,(3k^2 + 2k) + 1$ where $(3k^2 + 2k) \in Z$

$\Rightarrow n^2 \equiv 1 \pmod 3$

If p_2 is T: $\exists k \in Z$ where

$n = 3k + 2 \Rightarrow n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$ where $(3k^2 + 4k + 1) \in Z$

$\Rightarrow n^2 \equiv 1 \pmod 3$

$\therefore$ $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q)$ is T $\Rightarrow$ $(p_1 \vee p_2) \rightarrow q$ $\Rightarrow$ $p \rightarrow q$ is T *e.g.* Prove that the integer n is odd **if and only if** n^2 is odd.

p: n is odd, q: n^2 is odd $\Rightarrow$ Prove $p \leftrightarrow q$

$p \rightarrow q$: we showed it (page 10).
$q \rightarrow p$: use indirect proof s.t. $\neg p \rightarrow \neg q$

$\exists k \in Z$ where $n = 2k$ $\Rightarrow n^2 = 4k^2 = 2(2k^2) = 2t$ where $t = (2k^2)$, so n^2 is even since $t \in Z$.

e.g., Prove these statements about integer n ($n \in Z$) are equivalent:
p_1: n is even
p_2: n-1 is odd
p_3: n^2 is even

We need to show $p_1 \leftrightarrow p_2 \leftrightarrow p_3$ by showing $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, $p_3 \rightarrow p_1$

e.g.,
Theorem: “If x is a real number, then x^2 is a positive real number”

Proof:
p_1: x is positive
p_2: x is negative
q: x^2 is positive
We need to show $(p_1 \vee p_2) \rightarrow q$
by showing
$p_1 \rightarrow q$
and
$p_2 \rightarrow q$

Both are trivial. We are done with the proof.

e.g.,
Theorem: "If x is a real number, then x^2 is a positive real number"

Proof:
p_1: x is positive
p_2: x is negative
q: x^2 is positive
We need to show $(p_1 \vee p_2) \rightarrow q$
by showing
$p_1 \rightarrow q$
and
$p_2 \rightarrow q$

Both are trivial. We are done with the proof.

p_3: x is 0
$p \equiv p_1 \vee p_2 \vee p_3$
$p_3 \rightarrow q$ is F
Thus $p \rightarrow q$ is F

Theorems and Quantifiers:

Constructive Existence proof:

Prove $\exists x\ P(x)$: Find an a s.t. $P(a)$ is true

Non-constructive existence proof:

$\exists x\ P(x)$? : Prove or disprove the existence of an a s.t. $P(a)$ is true, without explicitly finding it.

e.g., Show that there exists irrational numbers x and y such that x^y is rational.
Consider $x = \sqrt{2}$ and $y = \sqrt{2}$. Both are irrational.

$x^y = \sqrt{2}^{\sqrt{2}}$
Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. DONE.
Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Then let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Thus $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ which is rational. DONE.

Non-constructive becase we didn't find an example x and y exactly (we do not know which case is true, but one of them must be).

Counter-example:

$\forall x$ P(x) ?

Find a for which P(a) is also false; which means $\forall x$ P(x) is false.

e.g.
Show that ‘all primes are odd’ is false.
x =2 even and prime $\therefore$ “not all primes are odd” ($\neg\forall x$ P(x))
“all primes other than 2 are odd” PROOF ??

Uniqueness proof:

$\exists x$ (P(x) $\wedge$ $\forall y$ ($y \neq x \rightarrow \neg$P($y$)))

e.g., “If a and b are real numbers and $a\neq 0$, then there exists a unique real number r such that $ar+b=0$”

Part 1 – Existence: Let $r=-b/a$. Then $ar+b = a(-b/a)+b = -b+b = 0$. DONE.

Part 2 – Uniqueness: Ley y be such that $ay+b=0$ but $y\neq r$. We know $ar+b = 0 = ay+b$. Subtracting b from both sides we get $ar=ay$. We know $a\neq 0$ hence dividing both sides by a we get $r=y$, contradicting our assumption that $y\neq r$. Therefore no such y can exist.

SUGGESTIONS (**Strongly recommended** if you want to **learn** and get a high grade!)

MAKE SURE YOU TRY SOLVING FIRST BEFORE LOOKING AT THE SOLUTION!!

Chapter 1.6:
In-text examples: 2, 4, 6, 7
Fun: Another step in Example 15 is wrong. Email comp106ta@ku if you find it.
Do ALL the exercises at the end of the chapter. Especially 19, 25, 30, 34, 38, 39, 40.
Fun: Interestingly, in exercise 38, using 4 squares is enough. **Every non-negative integer can be represented as a sum of 4 squares.** This is very useful in cryptography. Email me if interested.

Chapter 1.7:
In-text examples: 2, 3, 4, 6, 12 (a little advanced), 15
Fun: In-text example 5: Actually, you can even prove that in order, the last digit is always repeating this sequence: "0, 1, 4, 9, 6, 5, 6, 9, 4, 1". Note that the proof should have started with 0.
Fun: In-text example 14: Instead show that given two non-negative real numbers x and y with no restrictions, (x+y)/2 ≥ $\sqrt{xy}$
Do ALL the exercises at the end of the chapter.

MORE SUGGESTIONS (still strongly recommended)

End of whole Chapter 1:

Review “Key Terms and Results”

Do review question 7.

Supplementary exercises: 10, 11, 15, 16, 17, 18, 22, 24, 32, 33, 34.