MATH1061
Discrete Mathematics I

Michael Kasumagic, s4430266

Semester 2, 2024

Contents

Chapter 1

Week 1

1.1 Lecture 1

This course will run a little differently. Prior to every lecture, we must work through a set of pre-lecture problems. The goal of timetabled lectures is to discuss and learn from solving problems.

What is in this course?

Logic and set theory, methods of proof

Modern mathematics uses the language of set theory and the notation of logic.

$$((P \wedge \sim Q) \vee (P \wedge Q)) \wedge Q \equiv P \wedge Q$$

We will learn to read and analyse this. Historical, there was a big shift in recent history, there was a big effort to define and axiom-itise everything, such that math itself is defined rigorously. Symbolic logic is the basis for many areas of computer science. It helps us formulate mathematical ideas and proofs effectively and cobbrectly!

Definition 1.1.1: Gödel's Incompleteness Theorem (1931)

There exists true statements which we can not prove!

Number Theory

Example 1.1.1 $(1 + \cdots + 100)$

A young Gauss had to add up all the numbers from 1 to 100 in primary school. What did he do?

$$\begin{array}{ccccccccccccc} & & 1 & + & 2 & + & \cdots & + & 98 & + & 99 & + & 100 \\ 100 & + & 99 & + & 98 & + & \cdots & + & 2 & + & 1 & & \\ \hline 100 & + & 100 & + & 100 & + & \cdots & + & 100 & + & 100 & + & 100 \end{array}$$

So...

$$1 + \cdots + 100 = \frac{101 \cdot 100}{2} = 5050$$

This generalises to $\forall n \in \mathbb{N}$. Two leaps of faith are needed though!

- The dots: We introduce the notation to deal with them.
- The equality of two equations invoving dots. We will use induction to deal with this!

Graph Theory

Example 1.1.2 (The Königsberg Bridge Problem)

Find a route through the city which crosses each of seven bridges exactly once, and returns you to your start location.

This is provably impossible! But how can we rigorously prove this? Euler solve this problem in 1935 and in doing so invented graph theory. We'll learn how eventually... :p

Counting and Probability

Both fundamental and beautifully applicable. We introduce the pigeonhole principle as a introduction to "counting."

Example 1.1.3 (The pigeonhole principle)

If you have n pigeons sitting in k pigeonholes, if $n > k$, then at least of the pigeonholes contains at least 2 pigeons.

Question 1

If you have socks of three different colours in your drawer, what is the minimum number of socks you need to pull out to guarantee a matching pair?

Solution: #socks $\equiv$ #pigeons and #colours $\equiv$ #holes. If #socks $>$ #colors, a double must occur. Therefore, we need a minimum of 4 socks to guarantee a match.

Question 2: True or False?

In every group of five people, there are two people who have the same number of friends within the group.

Solution: True! #people $\equiv$ #pigeons and #friends $\equiv$ #holes. There are 5 possible values for the amount of friends one could have, $\{0, 1, 2, 3, 4\}$, but you can never have an individual with 0 friends, and 4 friends in the same group. So there are 5 people, and 4 possible #friend values (think "holes.") Therefore, by pigeonhole principle, the statement is true!

Question 3: True or False?

A plane is coloured blue and red. Is it possible to find exactly two points the same colour exactly one unit apart?

Note:-

We will answer this on Wednesday!

Recursion

Example 1.1.4 (The Tower of Hanoi)

Given: a tower of 8 discs in decreasing size on one of three pegs.
Problem: transfer the entire towert to one of the other pegs.
Rule 1: Move only one disc at a time.
Rule 2: Never move a larger disc onto a smaller disk.

1. Is there a solution?
2. What's the minimal number of moves necessary and sufficient for the task?

A key idea is to generalise! What if there are n discs? Let T_n be the minimal number of moves, then trivially $T_0 = 0$, $T_1 = 1$, $T_2 = 3$, so what is $T_3 =$?. Is there a pattern? The winning strategy is

1. Move the $n-1$ smallest discs from peg A to B.
2. Move the big disc from A to C.
3. Move $n-!$ smallest discs from B to C

By induction we show that

$$T_n = 2T_{n-1} + 1.$$

So $T_3 = 7$, $T_4 = 15$, $T_5 = 31$, $T_6 = 63$. Remarkably, this is one less then the sqaure numbers! We will prove this fact by induction later in the course.

1.2 Lecture 2

Definition 1.2.1: Statement or Proposition

A sentence that is either true or false but not both.

Example 1.2.1

Statements:

- The number 6 is a number.
- $\pi > 3$
- Euler was born in 1707.

Not statements:

- How are you? (This is a question.)
- Stop! (This is a command.)
- She likes math. ("She" is not well defined.)
- $x^2 = 2x - 1$ (x is not well defined.)

Definition 1.2.2: Negation

Let p be a statement. The negation is of p is denoted $\sim p$ or $\neg p$ and is read "not p." It is defined as in the following truth table:

p	$\sim p$
T	F
F	T

Definition 1.2.3: Conjuction

Let p and q be statements. The conjuction of p and q is denoted $p \wedge q$ and is read "p and q." It is defined as in the following truth table:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Definition 1.2.4: Disjunction

Let p and q be statements. The disjunction of p and q is denoted $p \vee q$ and is read "p or q." It is defined as in the following truth table:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Definition 1.2.5: Logical Equivalence

Two statements, p and q are said to be logically equivalent if have identical truth values for every possible combination of truth values for their statement variables. This is denoted $p \equiv q$.

Example 1.2.2

$$\sim(\sim p) \equiv p.$$

p	$\sim p$	$\sim(\sim p)$
T	F	T
F	T	F

Consider $P = \sim(p \wedge q)$, $Q = \sim p \wedge \sim q$ and $R = \sim p \vee \sim q$.

p	q	$\sim p$	$\sim q$	P	Q	R
T	T	F	F	F	F	F
T	F	F	T	T	F	T
F	T	T	F	T	F	T
F	F	T	T	T	T	T

$\therefore P \equiv R \not\equiv Q$.

Definition 1.2.6: Contradictions and Tautologies

A contradiction has truth values of false for every possible combination of its statement's truth values, and is denoted c or $\perp$. A tautology has truth values of true for every possible combination of its statement's truth values, and is denoted t or $\top$.

Example 1.2.3

p	$\sim p$	$p \wedge \sim p$
T	F	F
F	T	F

$\therefore p \wedge \sim p \equiv \top$

p	$\sim p$	$p \vee \sim p$
T	F	T
F	T	T

$\therefore p \vee \sim p \equiv \perp$

Important Laws of Logical Equivalence!

De Morgan's Law

$$\sim(p \wedge q) \equiv \sim p \vee \sim q$$
$$\sim(p \vee q) \equiv \sim p \wedge \sim q$$

Commutativity

$$p \wedge q \equiv q \wedge p$$
$$p \vee q \equiv q \vee p$$

Associativity

$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$$
$$p \vee (q \vee r) \equiv (p \vee q) \vee r$$

Distributivity

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

Double Negative

$$\sim(\sim p) \equiv p$$

Idempotent

$$p \wedge p \equiv p$$
$$p \vee p \equiv p$$

Absorbtion

$$p \vee (p \wedge q) \equiv p$$
$$p \wedge (p \vee q) \equiv p$$

Identity Laws

$$p \wedge \top \equiv p$$
$$p \vee \bot \equiv p$$

Domination

$$p \vee \top \equiv \top$$
$$p \wedge \bot \equiv \bot$$

Negation Laws

$$p \vee \sim p \equiv \top$$
$$p \wedge \sim p \equiv \bot$$

Negations

$$\sim\top \equiv \bot$$
$$\sim\bot \equiv \top$$

Example 1.2.4

Prove that $((p \wedge \sim q) \vee (p \wedge q)) \wedge q \equiv p \wedge q$.

$$\begin{aligned} ((p \wedge \sim q) \vee (p \wedge q)) \wedge q &\equiv (p \wedge (\sim q \vee q)) \wedge q && \text{(Distributivity)} \\ &\equiv (p \wedge \top) \wedge q && \text{(Negation Law)} \\ &\equiv p \wedge q && \text{(Identity)} \end{aligned}$$

□

1.3 Lecture 3

Definition 1.3.1: Conditional Statement

Let p and q be statement variables. The conditional form p to q is denoted $p \to q$, and read as "if p, then q," or "p implies q." It is defined by the following truth table

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

p is called the hypothesis.
q is called the conclusion.

Example 1.3.1

Suppose I make you the following promise:

"If you do your homework then you get a chocolate."

(a) You do not do your homework and you get a chocolate.

(b) You do your homework and you get a chocolate.

(c) You do your homework and you do not get a chocolate.

(d) You do not do your homework and you do not get a chocolate.

I only lied in scenario (c), which corresponds with $(p, q) = (F, T)$.

Note:-

$$p \to q \equiv \sim p \vee q$$

p	q	$\sim p$	$\sim p \vee q$	$p \to q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	F

Definition 1.3.2: Contrapositive

The contrapositive of $p \to q$ is $\sim q \to \sim p$.

p	q	$\sim p$	$\sim q$	$p \to q$	$\sim q \to \sim p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

$$p \to q \equiv \sim q \to \sim p$$

Example 1.3.2

The contrapositive of

"If you do your homework then you get a chocolate."

Is the equivalent

"If you did not get a chocolate then you did not finish your homework."

Negation of the Conditional Statement

The negation of $p \to q$ is given by $p \wedge \sim q$ and can be proved logcically.

$$\begin{aligned} p \to p &\equiv \sim p \vee q \\ \sim(p \to p) &\equiv \sim(\sim p \vee q) \\ &\equiv \sim(\sim p) \wedge \sim q \\ &\equiv p \wedge \sim q \end{aligned}$$

Example 1.3.3

The negation of

"If today is Monday, then tomorrow is my birthday"

Is

"Today is Monday but tomorrow is not my birthday."

Definition 1.3.3: Biconditional Statement

Let p and q be statement variables. The biconditional statement of p and q, denoted $p \leftrightarrow q$, and read "p if and only if q" is defined by the following truth table

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
T	T	T

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$

Chapter 2

Week 2

2.1 Lecture 4

Definition 2.1.1: Argument

Given a collection of statements, $p_1, p_2, \ldots, p_n$ (called premises), and another statement q (called the conclusion), an arugment is the assertion that the conjuction of the premises implies the conclusion. This is often represented

$$\begin{array}{ll} p_1 & \ldots \\ p_2 & \ldots \\ \vdots & \\ p_n & \ldots \\ \hline \therefore\ q & \end{array}$$

An argument is **valid** if whenever all the premises are true, the conclusion is true. Mathematically,

$$\bigwedge_{i=1}^{n} (p_i) \to q \equiv \top$$

An argument is **invalid** if there exists a configuration, such that all the premises are true, but the conclusion is false.

$$\bigwedge_{i=1}^{n} (p_i) \to q \not\equiv \top$$

Example 2.1.1

$$\begin{array}{ll} p_1 & \text{If it is raining, then there are clouds.} \\ p_2 & \text{It is raining.} \\ \hline \therefore & \text{There are clouds.} \end{array}$$

Which is an argument of form:

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

This is a valid argument! As long as p_1 and p_2 are true, q is necessarily true.

$$\begin{array}{ll} p_1 & \text{If it is raining then there are clouds.} \\ p_2 & \text{There are clouds.} \\ \hline \therefore & \text{It is raining.} \end{array}$$

Which is an argument of form:
$$\begin{array}{l} p \to q \\ q \\ \hline \therefore \ p \end{array}$$

This is an invalid argument! Because the conclusion doesn't follow from the premises. For example, if p_1 and p_2 were true, q still may be false.

Rules of Inference

These are common argument forms.

Modus Ponens

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

p	q	Premise 1: $p \to q$	Premise 2: p	Conclusion: q
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	F	T

Pay special attention to row 1. This is the only row in which every premise is true. When every primise is true, the conclusion is always true. Therefore this is a valid argument form. Every argument form can be proven with a truth table in this manner.

Modus Tellens

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

Generalisation

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

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

Specalisation

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

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

Conjuction

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

Elimination

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

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

Transitivity

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

Proof by Division into Cases

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

Contradiction

$$\begin{array}{l} \sim p \to \bot \\ \hline \therefore \ p \end{array}$$

Example 2.1.2 (Valid or invalid)

Is the following argument valid?

$$\begin{array}{ll} 1. & p \to \sim r \\ 2. & r \vee \sim q \\ 3. & \underline{q} \\ \therefore & \sim p \end{array}$$

We might be tempted to use a truth table, but it'll have an unreaonsable, $\left(2^3\right)$, amount of rows! We can use our rules of inference to figure this out.

1.	$p \to \sim r$	
2.	$r \vee \sim q$	
3.	q	
4.	$\sim q \vee r$	(2. by Commutativity)
5.	$p \to r$	(4. by Logical Equivalence)
6.	r	(3. and 5. by Modus Ponens)
7.	$\underline{\sim(\sim r)}$	(6. by Double Negative)
$\therefore$	$\sim p$	(1. and 7. by Modus Tellens)

Therefore the argument is valid!

Searching for Invalidity

Another method for checking validity may be to look for truth values which make the premises true, but the conclusion false. If we can find such an example, we can prove that the arugment is invalid. If it is impossible to do this, then the argument is valid.

Example 2.1.3

Consider the argument

$$\begin{array}{ll} & p \to q \\ & \underline{q} \\ \therefore & p \end{array}$$

Since p is the conclusion, take it to be false.
Since q is a premise, take it to be true.
The premise $p \to q$ is therefore False $\to$ True $\equiv$ True.
Therfore all our premises are true.
But wait! Our conclusion was set to false!
Therefore, there and is called the existential quantifier.

Let $Q(x)$ be a preda configuration of truth values, namely $(p, q) = (\text{False}, \text{True})$, such that all the premises are true, but the conclusion is false.
Therefore, the argument is invalid.

Example 2.1.4

Consider the argument

$$\begin{array}{ll} & p \to \sim r \\ & r \vee \sim q \\ & \underline{q} \\ \therefore & \sim p \end{array}$$

Let's suppose the argument is invalid.
Then, our conclusion $\sim p$, is false.
Then p is true.
Since q is a premise, take it to be true.
Consider the premise $p \to \sim r$. Since p is true, $\sim r$ must also be true, such that the premise is true.

Then, r is false.
Consider the premise $r \vee \sim q$. Substituting, we see False $\vee$ False $\equiv$ False.
Therefore, it is impossible for us to configure (p, q, r) such that all the premises are true, and the conclusion is false.
Therefore the argument is not invalid.
Therefore the argument is valid.

2.2 Lecture 5

Definition 2.2.1: Predicate

A predicate is a sentence which contains finitely many variables, and which becomes a statement if the varaibles are given specific values.

The **domain** of each variable in a predicate is the set of all possible values that may be assigned to it. Predicates are commonly denoted with an upper case letter followed by a list of finitely many varaibles within brackets, $P(x)$, $Q(x)$, $R(x)$.

Example 2.2.1

Given some variables $x, y, a, b, c \in \mathbb{Z}$, here are some example predicates:

- x is even.
- $x \leq y$.
- a divides b and b divides c.

The following are not predicates:

- Divide by 2.
- Is x an integer?

Definition 2.2.2: Truth Set

The truth set of a predicate is the set of all values in the variables' domains, such that when a value from those domains are assigned to those variables, the predicate is evaluated as true.

Example 2.2.2

Let $P(x)$ be the predicate $x|5$, and $\operatorname{dom} x = \mathbb{N}$.

The truth set of $P(x)$ is $\{-5, -1, 1, 5\}$, because these are all the numbers in the domain which divide 5.

Common Domains

- The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- The positive integers: $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$
- The nonnegative integers: $\mathbb{Z}^{\geq 0} = \{0, 1, 2, 3, \ldots\}$
- The natural numbers: $\mathbb{N} = \{1, 2, 3, \ldots\}$
- The rational numbers: $\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z} \wedge b \neq 0 \right\}$
- The real numbers: The entire number line.

Note:-

The real numbers have a rigorous definition, but it is outside the scope of this introducctory course.

The Universal Quantifier

The symbol $\forall$ denotes "for all" and is called the universal quantifier.

Let $Q(x)$ be a predicate and $\operatorname{dom} x = D$.
The statement

$$\forall x \in D, Q(x)$$

is true if and only if $Q(x)$ is true for every single element in D.
It is false if and only if $Q(x)$ is false for at least one element in D.

Example 2.2.3

Let $Q(x)$ be the predicate $x \leq x^2$, and $\operatorname{dom} x = \mathbb{Z}$. The statement $\forall x \in \mathbb{Z}, Q(x)$ can be expressed in the following equivalent ways:

- $\forall x \in \mathbb{Z}, x \leq x^2$
- For all $x \in \mathbb{Z}, x \leq x^2$
- Every integer is less then or equal to its sqaure.

Are the following statements true or false?

$$\forall x \in \mathbb{Z}, x \in \mathbb{R}$$

True. $\because \mathbb{Z} \subseteq \mathbb{R}$.

$$\forall y \in \mathbb{Q}, y^2 \geq 1$$

False. Counterexample, let $y = \frac{1}{2}$. Then $\left(\frac{1}{2}\right)^2 = \frac{1}{4} < 1$. Take any $y < 1$. It's square is less then 1.

The Existential Quantifier

The symbol $\exists$ denotes "there exists" and is called the existential quantifier.

Let $Q(x)$ be a predicate and $\operatorname{dom} x = D$.
The statement

$$\exists x \in D : Q(x)$$

is true if and only if $Q(x)$ is true for at least a single element in D.
It is false if and only if $Q(x)$ is false for every single element in D.

Example 2.2.4

Let $Q(x)$ be the predicate $x^2 = 4$, and $\operatorname{dom} x = \mathbb{Z}$. The statement $\exists x \in D : Q(x)$ can be expressed in the following equivalent ways:

- $\exists x \in \mathbb{Z}$ such that $x^2 = 4$
- There exists an integer x such that $x^2 = 4$
- There is some integer whose square is 4.

Are the following true or false?

$$\exists x \in \mathbb{R} : x^2 = 1 \wedge x < 0$$

Note that $P(x)$ is the conjuction of two other predicates.

This is true. Take $x = -1 \in \mathbb{R}$.
Then $-1^2 = 1$ and $-1 < 0$.

$$\exists x \in \{2, 4, 6\} : x^2 = 9.$$

False. We can prove this by exhaustion.
$2^2 = 4 \neq 9 \quad 4^2 = 16 \neq 9 \quad 6^2 = 36 \neq 9$.
Therefore, there is no x in the domain such that the predicate is satisfied.

Universal Conditional Statements

One of the most important statement forms in mathematics:

$$\forall x \in D, P(x) \to Q(x)$$

Example 2.2.5

The universal conditional statement

$$\forall x \in \mathbb{R}, x > 3 \to x^2 > 9$$

Can be equivalently expressed

- For every real number, x, if $x > 3$, then $x^2 > 9$.
- Whenever a real number is greater then 3, its square is greater then 9.
- The squares of real numbers greater then 3, are greater then 9.

2.3 Lecture 6

Negations of Quantified Statements

Negating the Universal Quantifier

Consider the universally quantified statement

$$\forall x \in D, Q(x).$$

The negation of this statement is logically equivalent to

$$\exists x \in D : \sim Q(x).$$

$\forall$ negates to $\exists$, and the predicate $Q(x)$ negates to $\sim Q(x)$.

Example 2.3.1

Consider the statement

$$\forall x \in \mathbb{Z}, x \text{ is prime.}$$

The negation of this statement is

$$\exists x \in \mathbb{Z} : x \text{ is not prime.}$$

Naturally, and to maintain logical equivalence, the original statement, in this case, evaluates to False, while its negation evaluates to True.

Now, Consider the statement

$$\text{All integers are odd or even.}$$

This can be written mathematically as

$$\forall x \in \mathbb{Z}, x \equiv 0 \pmod 2 \vee x \equiv 1 \pmod 2.$$

And it's negation is

$$\exists x \in \mathbb{Z} : x \not\equiv 0 \pmod 2 \wedge x \not\equiv 1 \pmod 2.$$

Which when brought back into the English language, is read

There is an integer which is not even and not odd.

Clearly, the original statement evaluates to True, and its negation to False.

Negating the Existential Quantifier

Now let's consider the existentially quantified statement

$$\exists x \in D : P(x).$$

The negation of this statement Is

$$\forall x \in D : \sim P(x).$$

$\exists$ negates to $\forall$, and the predicate $P(x)$ negates to $\sim P(x)$.

Example 2.3.2

Consider the statement

There is a pink elephant.

Its negation is

Every elephant is not pink.

Consider the statement

$$\exists x \in \mathbb{Q} : x \in \mathbb{Z}$$

Its negation is

$$\forall x \in \mathbb{Q}, x \notin \mathbb{Z}$$

Again, we can tell that the original statement is true, and its negation is false.

A couple more examples... Let's consider the statement

Some rabbit has white fur.

Note that this is existentially quantified, so its negation will be universally quantified,

No rabbit has white fur.

Finally, consider the statement

Every UQ student is happy.

This time, note that this statement is universally quantified, so its negation will be existentially quantified,

There is a UQ student who is not happy.

We're getting the hang of this!

Negating the Universal Conditional Quantifier

Finally, we consider the statement

$$\forall x \in D, P(x) \to Q(x).$$

Using laws of logical equivalence, and what we've just learned, we can easily conclude that the negation of this statement is

$$\exists x \in D : \sim(P(x) \to Q(x)) \equiv \exists x \in D : P(x) \wedge \sim Q(x)$$

ultimately, the $\forall$ still negates to $\exists$, and if you consider the composite statement $R(x) = P(x) \to Q(x)$, then $\sim R(x) \equiv \sim(P(x) \to Q(x)) \equiv \sim(\sim P(x) \vee Q(x)) \equiv P(x) \wedge \sim Q(x)$.

Example 2.3.3

Let's negate some more statements!

$$\begin{aligned} A &= \forall x \in \mathbb{Z}, x \geq 1 \to x \in \mathbb{N} && \text{(True)} \\ \therefore \sim A &= \exists x \in \mathbb{Z} : x \geq 1 \wedge x \notin \mathbb{N} && \text{(False)} \\ B &= \forall x \in \mathbb{Z}, (3 \mid x) \to (6 \mid x) && \text{(False)} \\ \therefore \sim B &= \exists x \in \mathbb{Z} : (3 \mid x) \wedge (6 \nmid x) && \text{(True)} \\ C &= \text{“If a rabbit has white fur, then it has long ears”} && \text{(False)} \\ \therefore \sim C &= \text{“There is a rabbit with white fur and short ears”} && \text{(True)} \\ D &= \text{“All parks that have grass, have playgrounds.”} && \text{(False)} \\ \therefore \sim D &= \text{“Some park has grass and not playground.”} && \text{(True)} \end{aligned}$$

Statements with Multiple Quantifiers

Some predicates, for instance $x \leq y$, involve more then one varaible. In such a case, we use the notation $P(x, y)$ to denote such a predicate. Such predicates often appear with more than one quantifier. For example, consider the statement

$$\exists x \in \mathbb{N} : \forall y \in \mathbb{N}, x \leq y.$$

We would read this as “There exists a natural number which is smaller than all natural numbers.” or “There is a smallest natural number.”

Note:-

“Such that”, :, always pairs with the existential quantifier!

It's negation would be

$$\forall y \in \mathbb{N}, \exists x \in \mathbb{N} : x \leq y$$

which is read, “Every natural numbers has some other number which is less then or equal to it.”

Establishing the Truth, when given Multiple Quantifiers

Suppose we want to prove the given the statement

$$\forall x \in D, \exists y \in E : P(x, y).$$

To prove this, we must allow someone to pick any element in D they want, and we must any element in E which makes $P(x, y)$ true.

Example 2.3.4

Let's prove the statement

$$\begin{gathered} \forall x \in \mathbb{Z}, \exists y \in \mathbb{Z} : x + y = 0. \\ \forall x \in \mathbb{Z}, \\ \text{Choose } y = -x, \\ \text{Then } x + y = x - x = 0. \end{gathered}$$

□

No matter what value for x is chosen, I choose $y = -x$, and the predicate $P(x, y)$ always evaluates to true. Because we can do this for all integers x, we know that this statement is true.

Now lets suppose we have the statement

$$\exists x \in D : \forall y \in E, P(x, y).$$

To prove this statement, we need to find one particular $x \in D$ which makes $P(x, y)$ true, no matter what selection is made for $y \in E$.

Example 2.3.5

Let's prove the statement

$$\exists x \in \mathbb{N} : \forall y \in \mathbb{N}, x \leq y.$$

Take $x = 1$.

Now, $\forall y \in \mathbb{Z}, 1 \leq y$. □

Negations of Statements with Multiple Quantifiers

Consider the statement

$$\forall x \in D, \exists y \in E : P(x, y).$$

This statement will negate to

$$\exists x \in D : \forall y \in E, \sim P(x, y).$$

Similarly, consider the statement

$$\exists x \in D : \forall y \in E, P(x, y).$$

This statement will negate to

$$\forall x \in D, \exists y \in E : \not P(x, y).$$

Again, note, that the such that always pairs with the existential quantifier. Let's look at some examples now...

Example 2.3.6

$$\begin{aligned} A &= \forall x \in \mathbb{Z}, \exists y \in \mathbb{Z} : x + y = 0 && \text{(True)} \\ \therefore \sim A &= \exists x \in \mathbb{Z} : \forall y \in \mathbb{Z}, x + y \neq 0 && \text{(False)} \\ B &= \exists x \in \mathbb{R} : \forall y \in \mathbb{R}, |x| \leq |y| && \text{(False)} \\ \therefore \sim B &= \forall x \in \mathbb{R}, \exists y \in \mathbb{R} : |y| < |x| && \text{(True)} \end{aligned}$$

Chapter 3

Week 3

3.1 Lecture 7

Let's consider

Definition 3.1.1: Even and Odd

An integer n is even $\iff \exists k \in \mathbb{Z} : n = 2k$

An integer n is off $\iff \exists k \in \mathbb{Z} : n = 2k + 1$

Definition 3.1.2: Prime and Composite

An integer n is prime $\iff n > 1, \forall r, s \in \mathbb{Z}, n = rs \implies r = 1 \vee s = 1.$

An integer n is composite $\iff n > 1, \exists r, s \in \mathbb{Z} : n = rs, r \neq 1, s \neq 1.$

Direct Proof of Existential Statements

To show $\exists x : P(x)$ is true (for some value x and some predicate $P(x)$), it is enough to find a singe example of an element $x \in D$ for which $P(x)$ is true.

Example 3.1.1

Prove that $\exists x \in \mathbb{N} : x > 30, x$ is composite.

Proof. Suppose $x = 32$. Then $x > 30$ and $x = 2 \cdot 16$ which makes it composite. □

Direct Proof of Universal Statements

One way to prove that $\forall x \in D, P(x)$ is true is by direct proof:

1. Suppose $x \in D$.
2. Show that $P(x)$ is true.

To prove statements like $\forall x \in D, P(x) \to Q(x)$ is true directly:

- Suppose $x \in D$ and $P(x)$.
- Show that the conclusion, $Q(x)$ is true, using definitions, previously established results, and rules of logical inference.

Example 3.1.2

Lemma. For all $n \in \mathbb{Z}, n$ is odd $\implies n^2$ is odd.

Proof. Suppose $n \in \mathbb{Z}$ is odd.
Then $n = 2k + 1$.
$(2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2l + 1$.
Therefore, the square of an odd integer, is odd. □

Disproof by Counterexample

To show that $\forall x \in D, P(x) \to Q(x)$ is false, we only need to find a single example of $x \in D$ for $P(x)$ is true and $Q(x)$ is false. This is called a counterexample.

Example 3.1.3

Lemma. For all $n \in \mathbb{Z}, n$ is even $\implies n/2$ is even

Proof. We will disprove this lemma with a counterexample.
Take $n = 6$.
Then n is even, since $6 = 2 \cdot 3$.
But $n/2$ is odd, since $6/2 = 3 = 2 \cdot 1 + 1$.
Therefore, the statement that all even integers divided by 2 are even, is false. □

Tips for writing proofs

1. Write the theorem to be proved.
2. Clearly mark the beginning of the proof, with *Proof.*
3. Use precise definitions for any mathematical terms.
4. Write the proof using complete sentences.
5. Give reasons for each assertion.
6. Keep the proof self contained.
7. Display equations and inequalities clearly.
8. Conclude by stating what you've proved.

3.2 Lecture 8

Proof by Contradiction of Statements $\forall x \in D, P(x)$

1. Assume the statement to be proved is false.
2. Show that this assumption logically leads to a contradiction.
3. Conclude the statement to be proved is true.

Example 3.2.1

Lemma. There is no greatest integer.

Proof. Suppose the lemma is false.
Then there is a greatest integer, N.
Hence, $\forall n \in \mathbb{Z}, N \geq n$.
Let $M = N + 1$.

Since $N \in \mathbb{Z}$ and $1 \in \mathbb{Z}$, then $M \in \mathbb{Z}$. But $M > N$ ※
Thus, M is an integer that is greater than N.
So N is not the greatest integer.
Therefore, there is no greatest integer. □.

Example 3.2.2

Lemma. $\forall n \in \mathbb{Z}, n$ is not similateously even and odd.

Proof. Suppose the lemma is false.
Then there is some some $n \in \mathbb{Z}$ that is both odd and even.
Thus, $n = 2k$ for some $k \in \mathbb{Z}$.
And, $n = 2l + 1$ for some $l \in \mathbb{Z}$.
Hence, $2k = 2l + 1 \iff 1 = 2(k - l)$.
Therefore, $k - l = 1/2$, which is impossible, since $1/2 \notin \mathbb{Z}$. ※
Therefore, there is no integer which is both even and odd similateously. □

Proof by Contradiction of Statements $\forall x \in D, P(x) \to Q(x)$

1. Assume the statement is false. Therefore the negation of the statement $\exists x \in D : P(x) \wedge \sim Q(x)$.
2. Show that this assumption logically leads to a contradiction.
3. Conclude the statement to be proved is true.

Example 3.2.3

Lemma. For all integers n, if n^2 is odd, then n is odd.

Proof. Suppose that the lemma is false.
Then $\exists n \in \mathbb{Z}, n^2$ is odd and n is even.
Since n is even, $n = 2k$, for some $k \in \mathbb{Z}$
Since n^2 is odd, $n^2 = 2l + 1$, for some $l \in \mathbb{Z}$.
So $n^2 = (2k)^2 = 4k^2 = 2(k^2) = 2l + 1$. ※
n^2 is similateously odd and even, this is a contradiction.
Therefore, the assumption that the lemma is false, is false.
Therefore, the lemma is true. □

3.3 Lecture 9

Proof by Contraposition

Relying on the fact that a statement is logically equivalently to its contrapositive, sometimes it can be easier to prove that contraspositive. Since they are logically equivalent, proving the contrapositive, proves the target statement.

1. Exress the target statement in the form $\forall x \in D, P(x) \to Q(x)$
2. Rewrite the statement in its contrapositive form $\forall x \in D, \sim Q(x) \to \sim P(x)$
3. Prove the contrapositive directly:
   - Suppose $x \in D$ and $Q(x)$ is false.
   - Show that $P(x)$ is false.

Example 3.3.1

Lemma. For all integers n, if n^2 is even, then n is even.
Remark. The lemma is written using notation,

$$\forall n \in \mathbb{Z}, n^2 \text{ is even } \implies n \text{ is even},$$

and is logically equivalent to its contraspositive

$$\forall n \in \mathbb{Z}, n \text{ is odd } \implies n^2 \text{ is odd}.$$

Proof. Suppose $n \in \mathbb{Z}$ and n is odd
n is odd, therefore $n = 2k + 1,\ k \in \mathbb{Z}$
$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2l + 1,\ l \in \mathbb{Z}$
Therefore, n^2 is odd
So, the contrapositive is true.
Then, the lemma is true.
We conclude that, given an even square integer, its root is even. □

Example 3.3.2

Definition (Parity). Two integers have the same parity if they are both even, or both odd. Two integers have opposite parity if one is odd, and the other is even.

Lemma. $\forall m, n \in \mathbb{Z}, m + n$ is even $\implies$ m and n have the same parity.
Remark. The contrapsotive of the lemma is $\forall m, n \in \mathbb{Z}, m$ and n have the opposite parity $\implies$ $m + n$ is odd.

Proof. Suppose $m, n \in \mathbb{Z}$ and have opposite parity.
Then one is odd, and the other is even.
Without loss of generality, suppose that m is odd, and n is even.
Then $m = 2k + 1,\ k \in \mathbb{Z}$ and $n = 2l,\ l \in \mathbb{Z}$.
Hence, $m + n = 2k + 1 + 2l = 2k + 2l + 1 = 2(k + l) + 1$
Therefore, $m + n$ is odd.
So, the contrapositive is true.
Therefore, the lemma is true. □

Example 3.3.3

Lemma. $x, y \in \{z \in \mathbb{R} \mid z > 0\} = D, xy > 25 \implies x > 5 \vee y > 5$.
Remark. The contrapositive of the lemma is $x, y \in \{z \in \mathbb{R} \mid z > 0\}, x \leq 5, y \leq 5 \implies xy \leq 25$.

Proof. Suppose $x, y \in D, x \leq 5, y \leq 5$.
Therfore, $x \cdot y \leq 5 \cdot 5$.
In other words, $xy \leq 25$.
Thus, the contrapositive is true.
Therfore, the lemma is true. □

The Rational Numbers

Definition 3.3.1: The Rational Numbers

A real number is rational if and only if it can be expressed as a quotient of two integers with a nonzero denominator.

$$\forall x \in \mathbb{R}, x \text{ is rational } \iff \exists a, b \in \mathbb{Z} : x = \frac{a}{b}, b \neq 0$$

We denote the set of all rationals $\mathbb{Q}$

$$\mathbb{Q} = \left\{ x \in \mathbb{R} \;\middle|\; \exists a, b \in \mathbb{Z} : x = \frac{a}{b}, b \neq 0 \right\}$$

We can denote the set of all irrational numbers, using $\mathbb{Q}$, namely

$$\mathbb{Q}' = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$$

Claim. The decimal expansion of a rational number either repeats or terminates.

$$\frac{1}{4} = 0.25, \qquad \frac{1}{3} = 0.3333\cdots = 0.\bar{3}$$

Claim. The decimal expansion of an irrational number does not repeat or terminate.

$$\pi = 3.1415\ldots$$

Lemma 3.3.1. $a, b \in \mathbb{Q}, a + b \in \mathbb{Q}$

Proof. Suppose $a, b \in \mathbb{Q}$.

$$\text{Then, } a = \frac{c}{d}, \text{ and } b = \frac{e}{f},\ c, d, e, f \in \mathbb{Z}, d \neq 0, f \neq 0.$$
$$\text{So, } a + b = \frac{c}{d} + \frac{e}{f} = \frac{cf}{df} + \frac{de}{df} = \frac{cf + de}{df}.$$
$$cf + de \in \mathbb{Z},\ df \in \mathbb{Z}, \text{ and } df \neq 0$$
$$\therefore a + b \in \mathbb{Q}$$

Therefore, the sum of any two rational numbers, is rational □

Lemma 3.3.2. For any rational number r, and any nonzero rational s, $\frac{r}{s}$ is rational, or,

$$\forall r, s \in \mathbb{Q}, s \neq 0 \implies \frac{r}{s} \in \mathbb{Q}$$

Proof. Suppose $r, s \in \mathbb{Q}$ and $s \neq 0$

$$\text{Then, } r = \frac{a}{b}, \text{ and } s = \frac{c}{d},\ a, b, c, d \in \mathbb{Z}, b \neq 0, c \neq 0, d \neq 0$$
$$\text{So, } r \div s = \frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{cb}$$
$$ad \in \mathbb{Z},\ cb \in \mathbb{Z},\ \text{and } cb \neq 0$$
$$\therefore \frac{r}{s} \in \mathbb{Q}$$

Therefore, the quotient of any rational and any nonzero rational is a rational. □

Theorem. For all rational numbers, r, s where $r < s$, there exists another rational q such that $r < q < s$, or symbolically,

$$\forall r, s \in \mathbb{Q}, r < s, \exists q \in \mathbb{Q} : r < q < s$$

Proof. Suppose $r, s \in \mathbb{Q}$ and $r < s$

$$\text{Then, } r = \frac{a}{b}, s = \frac{c}{d},\ a, b, c, d \in \mathbb{Z},\ b \neq 0, d \neq 0$$
$$\text{Take } q = \frac{1}{2}(r + s)$$

Since, r and s are rational numbers,

$$r + s \in \mathbb{Q}. \qquad \text{(Lemma 3.3.1)}$$

Since, $r + s \in \mathbb{Q}$ and $2 \in \mathbb{Q}$ and $2 \neq 0$, then

$$q = \frac{r+s}{2} \in \mathbb{Q}. \qquad \text{(Lemma 3.3.2)}$$

Since $r < s$,

$$q = \frac{1}{2}(r + s) < frac12s + s = \frac{1}{2}(2s) = s,$$

and

$$q = \frac{1}{2}(r + s) > \frac{1}{2}(r + r) = \frac{1}{2}(2r) = r,$$
$$\therefore q \in \mathbb{Q} \text{ and } r < q < s.$$ □

Lemma. For every nonzero number r, there exists a nonzero rational s such that $rs = 1$, or symbolically,

$$\forall r \in \mathbb{Q}, r \neq 0, \exists s \in \mathbb{Q} : rs = 1$$

Proof. Suppose $r \in \mathbb{Q}$.
Then,

$$r = \frac{a}{b},\ a, b \in \mathbb{Z},\ a \neq 0, b \neq 0$$

Take $s = \dfrac{b}{a}$

$$\text{Since } r \neq 0 \text{ so } a \neq 0. \text{ Therefore, } q \in \mathbb{Q}$$
$$r \cdot s = \frac{a}{b} \cdot \frac{b}{a}$$
$$= \frac{ab}{ab}$$
$$= 1$$

Therefore, $s \in \mathbb{Q}$ and $rs = 1$. □

Lemma. The sum of any rational number and any irrational number is irrational, $\forall q \in \mathbb{Q}, x \in \mathbb{Q}' \implies q+x \in \mathbb{Q}'$.

Proof. Suppose the lemma is false.
Then, there exists a rational number q and an irrational number x such that $q + x \in \mathbb{Q}$.
So, by definition, $q = \frac{a}{b}$ and $x + q = \frac{c}{d}$, $a, b, c, d \in \mathbb{Z}$ and $b \neq 0, d \neq 0$.
Let's consider $x + q = \frac{c}{d}$. $x + \frac{a}{b} = \frac{c}{d}$, which implies that $x = \frac{c}{d} - \frac{a}{b} = \frac{bc}{bd} - \frac{ad}{bd} = \frac{bc-ad}{bd}$.
Since a, b, c, d are all integers, then bc, ad, and bd are all integers.
And since $b \neq 0$ and $d \neq 0$, then $bd \neq 0$.
Therefore, by definition, x is a rational number ※
x can't be both a rational and an irrational number, this is a contradiction.
Thus, the sum of an irrational and a rational cannot be rational.
Therefore, the lemma is true. □

Chapter 4

Week 4

4.1 Lecture 10

Divisibility

Definition 4.1.1: Divisibility

If $n, d \in \mathbb{Z},\ d \neq 0$ then n is divisible by d iff there exists some $k \in \mathbb{Z}$ such that $n = kd$. In other words

$$d \mid n \iff \exists k \in \mathbb{Z} : n = kd$$

Lemma. $\forall a, b, c \in \mathbb{Z},\ a \mid b,\ b \mid c \implies a \mid c$

Proof. Suppose $a, b, c, \in \mathbb{Z}$ and $a \mid b$ and $b \mid c$

$$\begin{aligned} a \mid b &\iff b = ka,\ k \in \mathbb{Z} \\ b \mid c &\iff c = lb,\ l \in \mathbb{Z} \\ \therefore c = l(ka) = kl(a) &\iff a \mid c \end{aligned}$$

Therefore, the lemma is proved. □

Note:-

Speical Cases:
$d \in \mathbb{Z} \setminus \{0\}$

$$d \mid 0$$

Since, $k = 0$, gives $0 = d \cdot 0$
$n \in \mathbb{Z}$

$$1 \mid n \text{ and } n \mid n, (n \neq 0)$$

Since, $k = n$ gives $n = 1 \cdot n$ and $k = 1$ gives $n = n \cdot 1$.
A new way to think about prime numbers!

$$\forall n \in \mathbb{N}, n \text{ is prime} \iff n > 1, \text{The only positive divisors of } n \text{ are 1 and } n$$

Theorem 4.1.1 Soft Fundamental Theorem of Arithmetic

Every interger $n > 1$ can be written as a product of primes.

Proof. Suppose the theorem is false.
Then there exists an integer $n > 1$ that is not a product of primes.
Choose the smallest such n.
n is either prime, or composite

Case 1: If n is prime, then n is trivially a product of primes.
Case 2: If n is composite, then $n = rs$ for some natural numbers r and s, where $r \neq 0$, and $s \neq 0$.
This implies $1 < r < n$ and $1 < s < n$.
Since n is the smallest number which is not a product of primes, r and s are products of primes.
So therefore, n is a product of primes ※
Thus, assumption that the theorem is false, is false.
Thereore, the theorem is true. □

Theorem 4.1.2 Fundamental Theorem of Arithmetic

Given any integer $n > 1$, there exists: a positive integer k, distinct primes $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$, such that

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k},$$

and any other expression of n as a product of primes is identical to this (commutativity not withstanding).

4.2 Lecture 11

Modular Arithmetic

Definition 4.2.1: Floor and Ceiling

Given $x \in \mathbb{R}$, the floor of x, denoted $\lfloor x \rfloor$, is the unique integer n, such that $n \leq x < n + 1$.

Given $x \in \mathbb{R}$, the ceiling of x, denoted $\lceil x \rceil$, is the unique integer n, such that $n - 1 < x \geq n$.

Theorem 4.2.1 The Quotient-Remainder Theorem

Given an integer n and a positive intger d, there exists unique integers q and r such that

$$n = dq + r, \qquad 0 \leq r < d.$$

q is called the quotient.
r is called the remainder.

Note: $q = \left\lfloor \frac{n}{d} \right\rfloor$.

Definition 4.2.2: Modulo

For integers a and b, we say that a is congruent to b modulo d, where d is a positive intger. This is denoted

$$a \equiv b \bmod d \iff d \mid (a - b).$$

Further, if a and b are not congruent modulo d, we can write

$$a \not\equiv b \bmod d$$

Claim. $n = dq + r \implies n \equiv r \bmod d$
Claim. $n \equiv 0 \bmod d \iff d \mid n$

Lemma. $a \equiv b \bmod d,\ n \equiv m \bmod d \implies an \equiv bm \bmod d$

Proof. Suppose $a, b, n, m \in \mathbb{Z},\ d \in \mathbb{N},\ a \equiv b \bmod d,\ n \equiv m \bmod d$.
Then, $d \mid (a - b)$ and $d \mid (n - m)$.
So, $a - b = dk$ and $n - m = dl$, $d, l \in \mathbb{Z}$.
Hence, $a = dk + b$ and $n = dl + m$.
Now, $an = (dk + b)(dl + m) = d^2kl + dkm + bdl + bm = d(dkl + km + bl) + bm$.

Therefore, $d \mid (an - bm) \iff an \equiv bm \bmod d$. □

Lemma. $a \equiv b \bmod d,\ n \equiv m \bmod d \implies a + n \equiv b + m \bmod d$

Proof. Suppose $a, b, n, m \in \mathbb{Z},\ d \in \mathbb{N},\ a \equiv b \bmod d,\ n \equiv m \bmod d$.
Then, $d \mid (a - b)$ and $d \mid (n - m)$.
So, $a - b = dk$ and $n - m = dl$, $d, l \in \mathbb{Z}$.
Hence, $a = dk + b$ and $n = dl + m$.
Now, $a + n = (dk + b) + (dl + m) = (dk + dl) + (b + m) = d(k + L) + (b + m)$.
Therefpre, $d \mid (a + n) - (b + m) \iff a + n \equiv b + m \bmod d$. □

4.3 Lecture 12

Greatest Common Divisor

Definition 4.3.1: Greatest Common Divisor

For nonzero integers, a, b, the greatest common divisor, denoted $\gcd(a, b)$, is the integer d which satisfies these properties:

- $d \mid a$
- $d \mid b$
- For all $c \in \mathbb{Z}$, $c \mid a$ and $c \mid b \implies c \leq d$.

Thus, d is the largest number which divides both a and b.

Note:-

If $\gcd(a, b) = 1$, then a and b have no common factors, bar ± 1. We call such numbers co-prime or relatively prime.

more interesting properties:

- $\gcd(0, 0)$ is undefined, since $d \mid 0, \forall d \in \mathbb{Z}$, and there is no greatest integer.
- $\gcd(a, a) = a$ since a is trivially it's own greatest divisor.
- $a > 0, \gcd(b, a) = a$, since $d \mid 0, \forall d \in \mathbb{Z}$ and $\gcd(a, a) = a$.
- If $a, b \in \mathbb{Z},\ b \neq 0$, and we apply the Q-R theorem, namely $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

The Euclidean Algorithm

The Euclidean Algorithm brings all of this together to help us compute $\gcd(a, b)$ for any two integers a, b.

Algorithm 1: The Euclidean Algorithm

Input: $a, b \in \mathbb{Z},\ a \geq b > 0$
Output: $d \in \mathbb{Z} : d$ is the greatest common divisor of a and b.

```
/* Apply the quotient-remainder theorem */
q ← ⌊a/b⌋;
r ← a − bq;
if r = 0 then
    /* Terminate, we've found gcd(a, b).  */
    return b;
else
    recurse with arguments (b,r);
end
```

Example 4.3.1

Lets's do an example, to get a feel for the algorithm.

$$\begin{aligned}\gcd(192, 132) &\to 132 \cdot 1 + 60\\ \gcd(132, 60) &\to 60 \cdot 2 + 12\\ \gcd(60, 12) &\to 12 \cdot 5 + 0\\ \gcd(12, 0) &= 12\end{aligned}$$

$\therefore \gcd(192, 132) = 12.$

Note:-

This algorithm will always terminate, because, by the quotient-remainder theorem, $0 \leq r < b$. Therefore, the arguments being recursed are always strcitly smaller.

Example 4.3.2

Find $\gcd(18, 14)$ and $\gcd(175, 63)$.

$$\begin{aligned}\gcd(18, 14) &\to 18 = 14 \cdot 1 + 4\\ \gcd(14, 4) &\to 14 = 4 \cdot 3 + 2\\ \gcd(4, 2) &\to 4 = 2 \cdot 2 + 0\\ \gcd(2, 0) &= 2\end{aligned}$$

$$\begin{aligned}\gcd(175, 63) &\to 175 = 63 \cdot 2 + 49\\ \gcd(175, 49) &\to 175 = 49 \cdot 3 + 28\\ \gcd(49, 28) &\to 49 = 28 \cdot 1 + 21\\ \gcd(28, 21) &\to 28 = 21 \cdot 1 + 7\\ \gcd(21, 7) &\to 21 = 7 \cdot 3 + 0\\ \gcd(7, 0) &= 7\end{aligned}$$

$\therefore \gcd(18, 14) = 2$ and $\gcd(175, 63) = 7$.

Lowest Common Multiple

Definition 4.3.2: Lowest Common Multiple

For nonzero integers, a, b, the lowest common multiple of a and b is the smallest positive integer n such that $a \mid n$ and $b \mid n$.

$$\operatorname{lcm}(a, b) = n \iff a, b \in \mathbb{Z} \setminus \{0\}\,,\ \exists n \in \mathbb{N} : a \mid n,\ b \mid n,\ \forall k \in \mathbb{N}, a \mid k,\ b \mid k,\ n \leq k.$$

Claim. Suppose $a, b \in \mathbb{Z}, 0 < b \leq a$. Then, $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b$.

Chapter 5

Week 5

5.1 Lecture 13

Sequences

A sequence is an ordered list of elements. It can be finite or infinite. Each individual element of a sequence is called a term, an is often denoted with a lowercase letter and a subscript. An explicit or general formula for a sequence is a rule which shows how the value of a_k depends on k.

Consider the infinite sequence: $1, 2, 4, 8, ...$ We could write: $a_k = k^2$.

This same sequence could be denoted in any of the following ways:

$$\{2^k\}_{k\geq 0} \qquad \{2^k\}_{k=0}^{\infty} \qquad (2^k)_{k\geq 0} \qquad (2^k)_{k=0}^{\infty}$$

Example 5.1.1

Given the infinite sequence $a = \left\{(-1)^n \frac{1}{n}\right\}_{n\geq 1}$, write the first 5 terms.

$$a_1 = (-1)^1 \frac{1}{1} = -1$$
$$a_2 = (-1)^2 \frac{1}{2} = \frac{1}{2}$$
$$a_3 = (-1)^3 \frac{1}{3} = -\frac{1}{3}$$
$$a_4 = (-1)^4 \frac{1}{4} = \frac{1}{4}$$
$$a_5 = (-1)^5 \frac{1}{5} = -\frac{1}{5}$$

An alternating sequence is a sequence for which consecutive terms alternate between positive and negative sign. The example sequence above is an example of an alternating sequence.

Summation Notation

We use Greek capital letter Σ to indicate a sum. If $m, n \in \mathbb{Z}$, $m \leq n$, and a is some sequence, then

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + a_{m+2} + \cdots + a_n$$

m is called the lower limit of the summation, and n is caled the upper limit of the summation.
Note that if $m = n$, then the summation will consist of a single term.
i is called a dummy variable. We could use any unused varaible name or symbol here, it only exists exists to illustrate the behaviour of consecutive terms. The dummy varaible only exists inside the sum we're taking.

Product Notatoin

We use Greek capital letter Π to indicate a sum. If $m, n \in \mathbb{Z}$, $m \leq n$, and a is some sequence, then

$$\prod_{i=m}^{n} a_i = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \ldots \cdot a_n$$

m is called the lower limit of the product, and n is caled the upper limit of the product.

Factorial

For all natural numbers n, we define $n!$, read "n factorial" to be

$$\prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n,$$

and $0! = 1$.

Properties of Summations and Products

Suppose we have two real numbers sequences $a = \{a_k\}_{k=m}^{n}$, and $b = \{b_k\}_{k=m}^{n}$, where $m, n \in \mathbb{Z},\ m \leq n$, and c is some real number the following hold:

- $\sum_{i=m}^{n} a_i \pm \sum_{i=m}^{n} b_i = \sum_{i=m}^{n} (a_i \pm b_i)$
- $\sum_{i=m}^{n} ca_i = c \sum_{i=m}^{n} a_i$
- $\left(\prod_{i=m}^{n} a_i\right)\left(\prod_{i=m}^{n} b_i\right) = \prod_{i=m}^{n} a_i b_i$

The Principle of Mathematical Induction

Let $P(n)$ be a predicate that is defined for all integers, n, greater than or equal to some fixed point integer a.

Suppose $P(a)$ is true, and for all integers $k \geq a$, $P(k) \to P(k+1)$.
Then $P(n)$ is true for all integers $n \geq a$.

Think of it as a chain of dominos. $P(1)$ implies $P(2)$ implies $P(3)$ implies ... implies $P(n)$.

Lemma. For all intgers $n \geq a$, $P(n)$.

Proof. By applying the principle of mathematical induction

1. Basis Step: Prove $P(a)$
2. Inductive Step: Prove, for all intgers $k \geq a$, $P(k) \implies P(k+1)$.
   (a) Inductive Hypothesis: Suppose k is an integer, such that $k \geq a$, and $P(k)$ is true.
   (b) Using this, show that $P(k+1)$ is true.
3. Conclude, that therefore, by the principle of mathematical induction, $P(n)$ is true, for all integers $n \geq a$. $\square$

Example 5.1.2

Lemma. For all integers $n \geq 1$, $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

Proof. Let $P(n)$ denote the predicate that the lemma is true for the integer n.
Suppose n is an integer greater than or equal to 1.

Basis Step:

$$P(1) \implies 1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$
$$\therefore P(1) \text{ is true.}$$

Inductive Hypothesis:
Suppose $k \in \mathbb{Z} \geq 1$, $P(k)$ is true.

$$\text{Then, } k = 1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

Let's now consider $k + 1$

$$k + 1 = 1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$$

Therefore, by the inductive hypothesis, the lemma is true. □

5.2 Lecture 14

The Principle of Strong Mathematical Induction

Let $P(n)$ be a predicate that is defined for every integer $n \geq a$, where a is some fixed point integer, and let b be an integer where $b \geq a$.

Basis Step: Suppose $P(a)$, $P(a+1)$, …, $P(b)$ are true.
Inductive Step: Suppose for every integer $k \geq b$, if $P(1), P(2), \ldots, P(k)$ are true, then $P(k+1)$ is true.
Conclusion: Then $P(n)$ is true for all integers $n \geq a$.

Claim. It can be proved that the strong PMI is equivalent to the ordinary PMI.
Strong PMI is advantageous in certain situations, like if we're proving the general form of a recursive sequence.

Example 5.2.1

Let b be a recursive sequence defined as follows:

$$b_1 = 4, \qquad b_2 = 12, \qquad b_n = b_{n-2} + b_{n-1}, \ \forall n \in \mathbb{Z}, n \geq 3.$$

Lemma. $4 \mid b_k, \ \forall k \in \mathbb{Z}, k \geq 1$.
Let $P(n)$ be the predicate: $4 \mid b_n$.

Proof. We will utilise the principle of strong mathematical induction

Basis Case:

$$b_1 = 4, \ 4 \mid 4, \ \therefore P(1).$$
$$b_2 = 12, \ 4 \mid 12, \ \therefore P(2).$$

Inductive Step: Suppose for all intgers $k \geq 3$, $P(1), P(2), \ldots, P(k) \to P(k+1)$.

$$\text{Then, } P(k) \equiv 4 \mid b_k \iff b_k = 4k,\ k \in \mathbb{Z},$$
$$\text{and } P(k-1) \equiv 4 \mid b_{k-1} \iff b_{k-1} = 4l,\ l \in \mathbb{Z}.$$

Let's not consider $P(k+1)$, and the term b_{k+1}.

$$\begin{aligned} b_{k+1} &= b_k + b_{k-1} \\ &= 4k + 4l \\ &= 4(k+l). \\ \therefore 4 \mid b_{k+1} &\equiv P(k+1). \end{aligned}$$

Therefore, by the principle of the lemma is true. □

The Well-Ordering Principle

If S is a non-empty set of integers, all of which are greater then some fixed integer, the S has a least element.

Claim. : It ca be proved that the WOP is equivalent to both the PMI and even the SPMI. All three of these principles are equivalent.

5.3 Lecture 15

Recurrance Relations

Definition 5.3.1: Recurrance Relation

A recurrance relation for a sequence $a = \{a_k\}_{\forall k}$ is a formula which relates some term a_k to some of its predecessors.

The intial conditions for such a recurrance relation specify the values of some inital terms.

Example 5.3.1

For example, the Fibbonacci sequence is defined recursively:

$$\underbrace{F_0 = 1, \qquad F_1 = 1,}_{\text{Inital Conditions}} \qquad \underbrace{F_n = F_{n-1} + F_{n-2},\ \forall n \in \mathbb{Z}, n \geq 2}_{\text{Reccurance Relation}}$$

Ways to Define a Sequence

So far, we've seen sequences defined in 3 ways:

1. **Informally**
   By listing the first few terms of a sequence, until the pattern becomes obvious.
   1, 1, 2, 6, 24, 120, 720 . . . Clearly, this sequence is the factorials of the nonnegative integers.

2. **General Formula**
   By stating the general formula, how a_n depends on n, and stating where the sequence begins.
   $a = \{n!\}_{n \geq 0}$.

3. **Recursively**
   By stating a recurrance relation, how a term a_n depends on some combination of predecessor terms, and

specifying the intial conditions.
$a_0 = 1,\ a_n = n \cdot a_{n-1},\ \forall n \in \mathbb{Z},\ n \geq 1.$

Defining a Set Recursively

We have seen sequences of numbers defined recursively. Many other mathematical objects can also be defined recursively, such as: sets, sums, products, and functions.

A recursive definition of a set requires three things:

I Base: A statement that a certain object belongs in the set.

II Recursion: A collection of rules which show how to form new objects in the set, from the existing objects in the set.

III Restriction: A statement that no objects belong to the set, other then those arising from applications of step **I** and **II**

Example 5.3.2

Let's consider the set of all valid bracketings. Every left bracket, (is matched with a right bracket,). There are always at least as many left brackets as there are right brackets.

(())() is valid.
()()() is valid.
())(() is invalid.

We can define this set recursively, namely

I Base: An empty expression, with no brackets is a valid bracketing.

II Recursion:

(a) If B is a valid bracketing, then (B) is a valid bracketing.

(b) If B and C are valid bracketings, then BC is a valid bracketing.

III Restriction: Any expression not derived from rules **I**, **IIa**, or **IIb** are invalid.

Lemma. (())() is a valid bracketing

Proof.

Let $A =$ An empty expression. Then A is a valid bracketing. (**I**)
Let $B = (A) = ()$. Then B is a valid bracketing. (**IIa**)
Let $C = (B) = (())$. Then C is a valid bracketing. (**IIa**)
Let $D = CB = (())()$. Then D is a valid bracketing. (**IIb**)

Therefore, (())() is a valid bracketing. □

Chapter 6

Week 6

6.1 Lecture 16

Solving Recurrance Relations

Given a sequence defined recursively, we may desire an explicit formula for the sequence. To find this formula, we use the method of itteration.

Method of Itteration

1. Use iteration to record a list of terms of the sequence and guess what the explicit formula is.
2. Use induction to prove the guess is correct.
3. If induction is successful, we've found a general form.
4. If induction is unsuccesful, make a new guess, and try again.

Note:-

It is not always possible to guess an explicit formula, and in fact, some recursively defined sequences do not have an explicit formula at all.

Example 6.1.1

Find an explicit formula for the recursive sequence

$$b_0 = 2, \qquad b_n = b_{n-1} + 5, \text{ for } n \geq 1.$$

We can record some terms in a table:

n	0	1	2	3	4
b_n	2	7	13	19	24

This seem's like an arithmetic sequence. The inital value is 2, and the common difference is 5. So we can guess that $b = \{2 + 5n\}_{n\geq 0}$. Let's set up our proof now:

Lemma. The sequence, b, which was previously defined recursively, is equal to the sequence $\{2 + 5n\}_{n\geq 0}$.

Proof.

Base Case: Consider b_0

$$b_0 = 2$$
$$2 + 5(0) = 2 + 0 = 2 = b_0$$
$$\therefore b_0 \text{ is equal to our guess formula.}$$

Inductive Hypothesis: Suppose $k \in \mathbb{Z} \geq 0, P(k)$

$$\text{Then } b_k = 2 + 5k$$

Let's now consider b_{k+1}

$$b_{k+1} = b_k + 5 = 2 + 5k + 5 = 2 + 5(k+1)$$

Thus, b_{k+1} is equal to our guess formula
Therefore, $\forall k \geq 0,\ b_k = 2 + 5k$.
Therefore, the lemma is true. □

Arithmetic Sequences

A sequence $a_0, a_1, a_2, \ldots$ is an arithmetic sequence if and only if there exists a constant d such that

$$a_k = a_{k-1} + d,$$

for all intgers $k \geq 1$.
It follows from this that a general formula can be expressed as follows:

$$a_n = a_0 + dn,\ \forall n \in \mathbb{Z}, n \geq 0.$$

Geometric Sequences

A sequence $a_0, a_1, a_2, \ldots$ is a geometric sequence if and only if there exists a constant r such that

$$a_k = ra_{k-1},$$

for all intgers $k \geq 1$.
It follows from this that a general formula can be expressed as follows:

$$a_n = a_0 r^n,\ \forall n \in \mathbb{Z}, n \geq 0.$$

6.2 Lecture 17

Defining Sets

A set, S, is a collection of objects, which are called elements of S.
If x, an object, is found in S, we write $x \in S$.
If x is not found in S, we write $x \notin S$.

We can define sets using curly braces,

$$A = \{2, 3, 4\},\ 3 \in A,\ \pi \notin A.$$

Let E be the set of all positive even numbers,

$$E = \{0, 2, 4, 6, 8, \ldots\},\ 20 \in E,\ 21 \notin E,\ -2 \notin E.$$

Note that A is a finite set, and E is an infinite set. Both are fine.

Order does not matter, so $\{1, 2, 3, 4\} = \{2, 3, 1, 4\}$.
Repititions are ignored, so $\{1, 1, 3, 4\} = \{4, 3, 1, 1, 3, 4\} = \{1, 3, 4\}$.

We can define a set by a property $P(x)$ which must be satisfied by it's elements:

$$A = \{x \in S \mid P(x)\}.$$

This is read: "The set A is definied as all the elements, x in the set S, such that the property $P(x)$ is satisfied.". The elements of A are precisely those elements of S for which the predicate $P(x)$ is true. For example,

$$\text{Even Integers} = \{n \in \mathbb{Z} \mid 2 \mid n\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

$$\{x \in \mathbb{Z} \mid 3 < x < 7\} = \{4, 5, 6\}.$$

It's worth noting at this point that set's are mathematical objects, and can therefore also be members of other sets.

$$\text{Let } A = \{1, 2, \{3\}, \{5, 6\}\}$$

$2 \in A,\ 3 \notin A,\ \{2\} \notin A,\ \{3\} \in A,\ 5 \notin A,\ \{5\} \notin A.$

Subsets

If A and B are sets, A is called a subset of B, written $A \subseteq B$, if and only if every element of A is also an element of B.

$$A \subseteq B \iff \forall x \in A \to x \in B.$$

Example 6.2.1

$$X = \{1, 2, 3, 4\}, \qquad Y = \{1, 3, 4\}, \qquad Z = \{1, 2\}$$

$Y \subseteq X$, and $Z \subseteq X$, but $Z \nsubseteq Y$.

Note:-

$$\forall \text{sets, } S,\ S \subseteq S.$$

If A and B are sets, A is called a *proper* subset of B, written $A \subset B$, if and only if, every element of A is also and element of B, but $A \neq B$.

$$A \subset B \iff A \neq B, \forall x \in A \to x \in B$$

This implies that there must be at least a single element of B which is not an element of A.

Properties of Sets

Two sets, A and B, are equal if and only if they contain the same elements,

$$A = B \iff \forall x, x \in A \leftrightarrow x \in B \iff A \subseteq B, B \subseteq A.$$

The empty set, denoted $\varnothing$, is the set which contains no elements.

$$\varnothing = \{\}$$

The empty set is a subset of all sets, so if S is any set, $\varnothing \subseteq S$.

For a finite set, A, the cardinality of A is the number of elements in the set A, which is denoted $|A|$.

$$|\{1, 2, 3, 4, 5\}| = 5, \qquad |\varnothing| = 0$$

Note:-

We mentioned before that sets can contain sets. Consider the following:

$$S = \{A \mid A \text{ is a set}, A \notin A\}.$$

Is $S \in S$?

1. If $S \in S$, then (by definition), $S \notin S$ ※
2. If $S \notin S$, then (by definition), $S \in S$ ※

This is called Russel's Paradox. To avoid this, we can attempt to define all sets recursively, like we did in Lecture 15.

In real life, we ought to study formal set theory, the axiom of choice, the Zermelo-Fraenkel axioms, but we'll get to this in a later course.

Operations on Set

Let A and B be sets.

The union of A and B, denoted $A \cup B$, is the set of all elements in A or in B.

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

The intersection of A and B, denoted $A \cap B$, is the set of all elements in A and also in B.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

The set difference difference of B and A, denoted $B \setminus A$, is the set of elements in B, but not in A.

$$B \setminus A = \{x \mid x \in B \wedge x \notin A\}.$$

If the sets we are considering are all subsets of some set U, called the universal set, then $U \setminus A$ is called the complement of A, and contains all the elements in the "universe of interest", except those in A.

$$A' = U \setminus A = \{x \in U \mid x \notin A\}.$$

Note:-

The definition of U is completely contextual. For example, if we're working in number theory, our universe may be the integers, or the natural numbers. If we're working with calculus, our universal set may be the reals. If we're working with objects in higher dimensional spaces, our universe might be $\mathbb{R}^n$ for some n. The universe can be anything we can think of, as long as it is the totality of what we're considering.

Sequential Operations on Sets

We can do operate on sets sequentially, similar to the product and summation notation we introduced earlier. Given sets, $A_0, A_1, A_2, \ldots, A_n$, and an intger $n \geq 0$,

$$\bigcup_{i=0}^{n} A_i = \left\{ x \;\middle|\; \bigvee_{i=0}^{n} x \in A_i \right\}$$

This set will contain all the elements which are in at least one of the sets $A_0, A_1, A_2, \ldots, A_n$. Of course, we can take this bad boy to infinity to...

$$\bigcup_{i=0}^{\infty} A_i = \left\{ x \;\middle|\; \bigvee_{i=0}^{\infty} x \in A_i \right\}$$

Ultimately, we're still just taking the union of sets, so even though we're considering infinite sets, the union of them will only contain elements which are themselves elements of those sets.

Naturally, we can do the same with intersections

$$\bigcap_{i=0}^{n} A_i = \left\{ x \;\middle|\; \bigwedge_{i=0}^{n} x \in A_i \right\}.$$

We can take this to infinity too,

$$\bigcap_{i=0}^{\infty} A_i = \left\{ x \;\middle|\; \bigwedge_{i=0}^{\infty} x \in A_i \right\}.$$

Imagine a Venn diagram, with infinty circles, and then colour in the central area, which all the circles share.

The Power Set

The power set of a set, S, denoted $\mathcal{P}(S)$, is the set of all subsets of S.

$$\mathcal{P}(S) = \{X \mid X \subseteq S\}.$$

Example 6.2.2

$$\mathcal{P}(\{1,2,3\}) = \left\{ \begin{array}{llll} \varnothing, & \{1\}, & \{1,2\}, & \{1,2,3\} \\ & \{2\}, & \{2,3\}, & \\ & \{3\}, & \{1,3\}, & \end{array} \right\}$$

Note that $\varnothing \in \mathcal{P}(S)$ and $S \in \mathcal{P}(S)$.
Claim. If $|S| = n$, then $|\mathcal{P}(S)| = 2^n$.

Disjoint Sets

Two sets, A, and B are disjoint, if and only if $A \cap B = \varnothing$. That is, A and B share no common elements.

Sets, $A_1, A_2, A_3, \ldots$ are mutually disjoint (or pairwise disjoint, or nonoverlapping) if and only if $A_i \cap A_j = \varnothing$ whenever $i \neq j$. That is to say, given a series of sets, none share common elements.

Set Partitions

A finite or infinite set of nonempty sets, $\{A_1, A_2, A_3, \ldots\}$ is a partition of the set A if and only if $A = \bigcup_{\forall i} A_i$ and $A_1, A_2, A_3, \ldots$ are mutually disjoint.

Example 6.2.3

A partition of $S = \{1,2,3,4,5,6,7\}$ is given by

$$\{\{1\}, \{2,3\}, \{4,5,6\}, \{7\}\}.$$

Note, that there is not necessarily only one partition of S.

Consider $\mathbb{Z}$ and division by 3. By the quotient-remainder theorem, every integer can be expressed uniquely as $n = 3q + r$.

$$\begin{aligned} \text{Let } A_0 &= \{n \in \mathbb{Z} \mid n \equiv 0 \bmod 3\} \\ \text{Let } A_1 &= \{n \in \mathbb{Z} \mid n \equiv 1 \bmod 3\} \\ \text{Let } A_2 &= \{n \in \mathbb{Z} \mid n \equiv 2 \bmod 3\} \end{aligned}$$

Then, $\{A_0, A_1, A_2\}$ is a partition of $\mathbb{Z}$.

Ordered n-Tuple

Let $n \in \mathbb{N}$ and let $x_1, x_2, \ldots, x_n$ be n, not necessarily distinct elements. The ordered n-tuple, denoted $(x_1, x_2, \ldots, x_n)$, consists of n elements with their ordering: first is x_1, then x_2, and so on. x_n is last.

When $n = 2$ is we call (x_1, x_2) an ordered-pair.
When $n = 3$ is we call (x_1, x_2, x_3) an ordered-triple.

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \iff x_i = y_i, \ \forall i, 1 \leq i \leq n.$$

Cartesian Product

The Cartesian product of two sets A and B, denoted $A \times B$,

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Example 6.2.4

If $A = \{a, b\}$ and $B = \{1, 2\}$, then

$$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2)\}.$$

The familiar xy-plane is

$$\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}.$$

In general,

$$A_1 \times A_2 \times \ldots A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i,\ \forall i, 1 \leq i \leq n\}.$$

Intervals

Given $a, b \in \mathbb{R}$ with $a \leq b$,

$$(a, b) = \{x \in \mathbb{R} \mid a < x < b\} \quad \text{(Open Interval)}$$
$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\} \quad \text{(Closed Interval)}$$
$$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$$
$$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$$

The symbols ∞ and $-\infty$ are used to denote intervals which are unbounded on either the left or right side.

$$(a, \infty) = \{x \in \mathbb{R} \mid x > a\}$$
$$(a, \infty] = \{x \in \mathbb{R} \mid x \geq a\}$$
$$(-\infty, a) = \{x \in \mathbb{R} \mid x < a\}$$
$$(-\infty, a] = \{x \in \mathbb{R} \mid x \leq a\}$$

6.3 Lecture 18

More Properties of Sets

Prove that $A \subseteq B$

1. Suppose $x \in A$
2. Show that $x \in B$

Example 6.3.1

Definition (A). Let $A = \{n \in \mathbb{Z} \mid n = 2k + 2, \text{ for some } k \in \mathbb{Z}\}$
Definition (E). Let $E = \{n \in \mathbb{Z} \mid n = 2m, \text{ for some } m \in \mathbb{Z}\}$
Lemma. $A \subseteq E$

Proof. Suppose $n \in A$.
Then $n = 4k + 2,\ k \in \mathbb{Z}$. Hence, $n = 2(2k + 1) = 2m,\ m \in \mathbb{Z}$, so $n \in E$.
Therefore $A \subseteq E$. □
Remark. Suppose $n = 4$. Then $n \in E$, but $n \notin A$. Therefore $A \subset E$.

Theorem 6.3.1 Transitive Property of Subsets

For all sets, A, B, and C, if $A \subseteq B$, and $B \subseteq C$, then $A \subseteq C$.

Proof. Suppose A, B, and C are sets, $A \subseteq B$, and $B \subseteq C$.
Consider $x \in A$.
Since $A \subseteq B$, then $x \in B$.
Since $B \subseteq C$, then $x \in C$.
Therefore, $A \subseteq C$. □

Inclusion For all sets A and B,

$$A \cap B \subseteq A \qquad A \cap B \subseteq B \qquad \text{(Inclusion of Intersection)}$$
$$A \cup B \subseteq A \qquad A \cup B \subseteq B \qquad \text{(Inclusion of Union)}$$

Method for Proving Equality of Sets

1. Prove $A \subseteq B$ (Suppose $x \in A$, show $x \in B$)
2. Prove $B \subseteq A$ (Suppose $x \in B$, show $x \in A$)

Example 6.3.2

Definition (A). Let $A = \{x \in \mathbb{Z} \mid x \equiv 1 \bmod 6\}$
Definition (B). Let $B = \{x \in \mathbb{Z} \mid x \equiv 1 \bmod 2, x \equiv 1 \bmod 3\}$
Lemma. $A = B$

Proof. Suppose $x \in A$
Then $x \equiv 1 \bmod 6 \iff 6 \mid (x-1) \iff x = 6k+1$, for some $k \in \mathbb{Z}$.
$x = 3(2k)+1 \iff 3 \mid (x-1) \iff x \equiv 1 \bmod 3$
$x = 2(3k)+1 \iff 2 \mid (x-1) \iff x \equiv 1 \bmod 2$
$\therefore x \in B$.
$\therefore A \subseteq B$.

Now let's suppose $x \in B$
Then $x \equiv 1 \bmod 2 \iff 2 \mid (x-1) \iff x = 2m+1$, for some $k \in \mathbb{Z}$
And $x \equiv 1 \bmod 3 \iff 3 \mid (x-1) \iff x = 3n+1$, for some $k \in \mathbb{Z}$ Note that $x = 3n+1$ is odd, because $x = 2m+1$, is the definition of odd.
If n is odd, then for some integer l, $x = 3(2l+1)+1 = 6l+4 = 2(3l+2)$ is even ※.
Therefore n is even. $n = 2l$
Hence, $x = 3(2l)+1 = 6l+1 \iff 6 \mid (x-1) \iff x \equiv 1 \bmod 6$.
$\therefore B \subseteq A$.

$\therefore$ The lemma is true, $A = B$. □

Example 6.3.3

Let A and B be subsets of the universal set U. Prove that

$$(A \cap B)' = A' \cup B'$$

Proof. Let $x \in U$

$$\begin{aligned} x \in (A \cap B)' &\iff x \notin A \cap B \\ &\iff \sim(x \in A \cap B) \\ &\iff \sim(x \in A \wedge x \in B) \\ &\iff \sim(x \in A) \vee \sim(x \in B) \\ &\iff x \notin A \vee x \notin B \end{aligned}$$

$$\iff x \in A' \vee x \in B'$$
$$\iff x \in A' \cup B'$$

Therefore, $(A \cap B)' = A' \cup B'$. □

Set Identities

Let A, B, C be any sets. Let U be the universal set.

Commutative Laws
$A \cup B = B \cup A$
$A \cap B = B \cap A$

Associative Laws
$(A \cup B) \cup C = A \cup (B \cup C)$
$(A \cap B) \cap C = A \cap (B \cap C)$

Distributive Laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Absorption Laws
$A \cup (A \cap B) = A$
$A \cap (A \cup B) = A$

Idempotent Laws
$A \cup A = A$
$A \cap A = A$

De Morgan's Laws
$(A \cup B)' = A' \cap B'$
$(A \cap B)' = A' \cup B'$

Set Difference Law
$B \setminus A = A \cap B'$

Double Complement Law
$(A')' = A$

Complements of $\varnothing$ and U
$U' = \varnothing$
$\varnothing' = U$

Complement Laws
$A \cup A' = U$
$A \cap A' = \varnothing$

Identity Laws
$A \cup \varnothing = A$
$A \cap U = A$

Universal Bound Laws
$A \cup U = U$
$A \cap \varnothing = \varnothing$

Functions

Definition 6.3.1: Functions

A function maps, from a set X, to a set Y. Denoted $f : X \to Y$, it is a subset of the Cartesian product, $X \times Y$, such that for all elements $x \in X$, there exists a unique element $y \in Y$, for which $(x, y) \in f$.

We call X the domain of f, $\operatorname{dom} f = X$.
We call Y the co-domain of f.

If $f : X \to Y$ is a function and $(x, y) \in f$, then we write:

$$f(x) = y \qquad \text{or} \qquad f : x \mapsto y.$$

We can call $f(x)$ the value of f at x, or the image of x under f.

For any particular mapping to be a function, every element in the domain, $x \in X$, must map to a single element in the co-domain, $y \in Y$. If an element in X is unmapped, the proposed map is not a function. If an element in X maps to two values in the co-domain, then the proposed map is not a function.

Image and Range

Given a function, $f : X \to Y$, and an element $x \in X$, we call $f(x)$ the image of x. If $A \subseteq X$, then the image of A is

$$f(A) = \{f(x) \mid x \in A\} = \{y \mid f(x) = y \text{ for some } x \in A\}.$$

Note that $f(A) \subseteq Y$.

The set $f(X)$ is called the range of f, $\operatorname{ran} f$.

$$f(X) = \{y \in Y \mid y = f(x) \text{ for some } x \in X\}.$$

Note that $f(X) \subseteq Y$.

Note:-

I honestly had some trouble understanding this, but it's a lot clearer once you take a look at some diagrams which illustrate how these things work. I'm not going to recreate those diagrams here right now.

Inverse Image

Given a function $f : X \to Y$, if $B \subseteq Y$, the inverse image, or preimage of B is

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

Equality of Functions

Suppose $f : X \to Y$ and $G : X \to Y$ are functions. Then

$$f = g \iff f(x) = g(x),\ \forall x \in X.$$

Example 6.3.4

Consider $f : \mathbb{Z} \to \mathbb{Z},\ f(x) = x$ and $g : \mathbb{Z} \to \mathbb{Z},\ g(x) = \sqrt{x^2}$.

Here $f \neq g$ because $f : -1 \mapsto -1$ but $g : -1 \mapsto 1$.

Note that $\operatorname{ran} f = \mathbb{Z}$, but $\operatorname{ran} g = \mathbb{Z}^{\geq 0}$.

Identity Functions

Given a set X, the identity function on X, denoted $\iota_X : X \to X$ is defined by

$$\iota_X : X \to X,\ \iota_X(x) = x,\ \forall x \in X.$$

This function is kind of cute! Given a set, the identity function is a mapping of every element in that set, to itself.

Sequences

An infinite sequence, $a = \{a_n\}_{n \geq k}$ is a function defined on the set of integers greater then some fixed point $k \in \mathbb{Z}$.

$$a = \{a_n\}_{n \geq k} = f : \mathbb{Z}^{\geq k} \to Y,\ f(n) = a_n.$$

Note that $\operatorname{dom} f = \mathbb{Z}^{\geq k}$, where k is the integer fixed point of the sequence.

Chapter 7

Week 7

7.1 Lecture 19

One-to-One (Inejective) Functions

Let f be a function mapping the set X, to the set Y. The function is injective if and only if for all elements $x_1, x_2 \in X$, $f(x_1) = f(x_2) \implies x_1 = x_2$. Or equivalently, if $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$.

Think "Every element in the domain has a different image," or every unique element in the domain maps to a unique element in the co-domain.

A function is not injective if and only if there exists some $x_1, x_2 \in X$, $x_1 \neq x_2$, such that $f(x_1) = f(x_2)$.

To prove injectivity, we use a direct proof:

1. Suppose $x_1, x_2 \in X$ and $f(x_1) = f(x_2)$.
2. Show that $x_1 = x_2$.

To prove that a function is not injective, we only need to present a counterexample of $x_1, x_2 \in X$, $f(x_1) = f(x_2)$, but $x_1 \neq x_2$.

Onto (Surrjective) Functions

Let $f : X \to Y$ be a function, mapping from the set X to the set Y. The function is surrjective if and only if, given any element $y \in Y$, it is possible to find an element $x \in X$ with the property $y = f(x)$. Equivalently,

$$f : X \to Y \text{ is surrjective } \iff \forall y \in Y,\ \exists x \in X : f(x) = y.$$

A function is not surrjective if and only if there exists some element $y \in Y$, the co-domain, that is not mapped onto by f.

To prove surrjectivity, we usually use a direct proof:

1. Suppose that $y \in Y$.
2. Construct an element x of X with $f(x) = y$.

To prove that a funcion is not surrjective, find and present a counterexample of $y \in Y$ such that $\forall x \in X$, $f(x) \neq y$. This is usually done with a proof by contradiction.

One-to-One Correspondance (Bijective) Functions

A function, $f : X \to Y$, is bijective if and only if f is injective and surrjective.

This, effectively means that, every element in the co-domain is an image of an element in the domain, and every unique element in the domain maps to a unique element in the co-domain.

Theorem 7.1.1 Inverse Function

Suppose that a function $f : X \to Y$ is bijective. Then, there exists a function $f^{-1} : Y \to X$ that is defined:

$$\forall y \in Y,\ f^{-1}(y) = x \in X : f(x) = y.$$

The function f^{-1} is called the inverse function of f.

7.2 Lecture 20

Composition of Functions

Definition 7.2.1: Function Composition

Let $f : X \to Y$ and $g : Y \to Z$ be functions. The composition of those functions is defined As

$$(g \circ f)(x) = g(f(x)),\ \forall x \in X.$$

Note that $\operatorname{dom} g \circ f = X$, and its co-domain is Z.
$\operatorname{ran} g \circ f$ is the image (under g) of the range of f.

Theorem 7.2.1 Compositions of Identity Function

If $f : X \to Y$ is a function, and $\iota_X : X \to X$, $\iota_Y : Y \to Y$ are the identity functions on X and Y, respectively, then

$$f \circ \iota_X = f \qquad \text{and} \qquad \iota_Y \circ f = f.$$

Proof. Suppose $f : X \to Y$ is a function, $\iota_X : X \to X$ is the identity function under X and $\iota_Y : Y \to Y$ is the identity function under Y.
Then, by definition, $\iota_X(x) = x,\ \forall x \in X$,
and, $\iota_Y(y) = y,\ \forall y \in Y$.
Now, $\forall x \in X,\ (f \circ \iota_X) = f(\iota_X) = f(x)$. Hence, $f \circ \iota_X = f$.
And, $\forall y \in Y,\ (\iota_Y \circ f) = \iota_Y(f(x)) = f(x)$. Hence, $\iota_Y \circ f = f$.
Therefore, the theorem is proven. □

Theorem 7.2.2 Bijective-Inverse Composition

Let $f : X \to Y$ be a bijective function, and $f^{-1} : Y \to X$ be its inverse. Then

$$f^{-1} \circ f = \iota_X \qquad \text{and} \qquad f \circ f^{-1} = \iota_Y$$

Theorem 7.2.3 Injective Compositions are Injective

If $f : X \to Y$ and $g : X \to Y$ are both injective then the composition $g \circ f$ is injective.

Proof. Suppose $f : X \to Y$ and $g : X \to Y$ are both injective functions.
Suppose $x_1, x_2 \in X$ and $(g \circ f)(x_1) = (g \circ f)(x_2)$.
Then, $g(f(x_1)) = g(f(x_2))$.
Since, g is injective, we have $f(x_1) = f(x_2)$.
Since, f is injective, we have $x_1 = x_2$.
Therefore, $g \circ f$ is injective. □

Theorem 7.2.4 Surjective Compositions are Surjective

If $f : X \to Y$ and $g : Y \to Z$ are both surjective functions, then their composition $g \circ f$ is surjective.

Proof. Suppose $f : X \to Y$ and $g : Y \to Z$ are surjective functions.
Suppose $z \in Z$.
Since g is surjective, $\exists y \in Y : g(y) = z$.
Since f is surjective, $\exists x \in X : f(x) = y$.
Hence, $\exists x \in X : (g \circ f)(x) = g(f(x)) = g(y) = z$.
Therefore $g \circ f$ is surjective. □

Theorem 7.2.5 Bijective Compositions are Bijective

It follows from Theorem 7.2.3 and Theorem 7.2.4 that if $f : X \to Y$ and $g : Y \to Z$ are bijective (injective and surjective), then their composition $g \circ f : X \to Z$ is bijective.

7.3 Lecture 21

Cardinality

The cardinality of a set is a measure of how large it is. We say that two sets X and Y have the same cardinality, $|X| = |Y|$, if and only if there exists a bijection between them.

A finite set is either a set with no elements in it, or one for which there exists a bijection between it and a set of the form $\{1, 2, 3, \ldots, n\}$, where n is some fixed integer.

An infinite set is a nonempty set for which there does not exists a bijection between it and a set of the form $\{1, 2, 3, \ldots, n\}$, where n is some fixed integer.

Finite Sets

Theorem. Suppose X and Y are finite sets

1. If $|X| > |Y|$, then there is no injective $f : X \to Y$. (By pigeonhole principle, there will always be at least 2 $x \in X$ mapping to the same $y \in Y$.)
2. If $|X| < |Y|$, then there is no surjection $f : X \to Y$. ($x \in X$ will map to $|X|$ number of elements in Y, but there will be some left over.)
3. It follows from this that, unless $|X| = |Y|$, there can not exist a bijection $f : X \to Y$.

Corollary. For finite sets, X and Y, with $|X| = |Y|$, the following statements are equivalent:

- $f : X \to Y$ is injective.
- $f : X \to Y$ is surjective.
- $f : X \to Y$ is bijective.

Infinite Sets

Two sets, X and Y, have the same cardinality if and only if there exists a bijection between them.

Lemma. The cardinality of the even integers is equal to the cardinality of all the integers.

Proof. Define a function $f : \mathbb{Z} \to \{n \in \mathbb{Z} \mid n = 2k,\ k \in \mathbb{Z}\}$, $f(x) = 2x,\ \forall x \in \mathbb{Z}$.
First we will show that f is injective:
Suppose $x_1, x_2 \in \mathbb{Z}$ and $f(x_1) = f(x_2)$.
Then $2x_1 = 2x_2$. We divide both sides by 2 and find that $x_1 = x_2$.

Therefore, f is injective.
Next, we'll show that f is surrjective:
Suppose $y \in \{n \in \mathbb{Z} \mid n = 2k,\ k \in \mathbb{Z}\}$.
Then $y = 2x$, for some $x \in \mathbb{Z}$.
Hence $f(x) = 2x = y$.
Thus, f is surrjective.
Therefore, f is injective and surrjective. Therefore, f is a bijection.
Therefore, $|\mathbb{Z}| = |\{n \in \mathbb{Z} \mid n = 2k,\ k \in \mathbb{Z}\}|$. □