MATH 220 Video Notes

Videos from PLP by Prof. Rechnitzer.

V1 Introduction to Sets

- $a \in A$: a is in the set A
- $a \notin A$: a is not in the set A

Describing a set

- $\{1, 2, 3\}$: list out a set
- $\{x \mid x \in \mathbb{R}, x \geq 1\}$: set builder notation
- $\varnothing = \{\}$: empty set
- $|S|$: cardinality of S (number of elements)

V2 Logical Statements

- Statement: either true or false
- Open sentence $P(x)$: can be true or false, depending on the input x

V3 And, Or, Not

- Negation: $\sim P$
- And: $P \wedge Q$. must both be true
- Or: $P \vee Q$. at least one has to be true
- Exclusive Or: $P \operatorname{xor} Q$. exactly one has to be true

V4 Conditional

Conditional/Implication: if P then Q. Written as $P \implies Q$, where P is the hypothesis and Q is the conclusion.

Truth table for the conditional:

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T (vacuously true)
F	F	T (vacuously true)

To prove that $P \implies Q$, we assume that P is true and prove that Q must be true.

V5 Modus Ponens

$(P \implies Q)$ and P are true, so Q must be true.

To prove that $P \implies Q$, we can prove that:

$$\begin{aligned} P &\implies P_1 \\ P_1 &\implies P_2 \\ &\vdots \\ P_n &\implies Q \end{aligned}$$

- When we assume that P is true, we can chain Modus Ponens to conclude that Q must be true, which proves $P \implies Q$.

V6 Converse, Contrapositive, Biconditional

Given the implication $P \implies Q$:

- Converse: $Q \implies P$. Switch order, not the same logically
- Contrapositive: $(\sim Q) \implies (\sim P)$. logically equivalent to $P \implies Q$.
- Biconditional: $P \iff Q$. Equivalent to $(P \implies Q) \wedge (Q \implies P)$

V7 Statement Types and Definitions

Statement Types

- axioms: fundamental statements that are accepted to be true without proof
- facts: statements we accept to be true but don't prove (although they can be proved from axioms)
- theorems: important true statements
- corollaries: true statements that follows from theorems
- lemmas: a true statement that helps us prove a more important result
- results/proposition: true statements that we prove as exercises. Called a proposition if it is more important, otherwise called a result

Number Theory Definitions

- n is even if $n = 2k$ for some $k \in \mathbb{Z}$
- n is odd if $n = 2l + 1$ for some $l \in \mathbb{Z}$
- k divides n if there is $l \in \mathbb{Z}$ so that $n = lk$
  - $k \mid n$: k is a divisor of n, n is a multiple of k
- n is prime if it has exactly two divisors: 1 and itself
- n is composite if it has more than two divisors. Note that 1 is neither prime nor composite.
- $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$: largest/smallest integer that is a divisor/multiple of a and b
- Euclidean division: let $a, b \in \mathbb{Z}$ with $b > 0$. There exists unique $q, r \in \mathbb{Z}$ so that $a = bq + r$ with $0 \le r < b$.
- a congruent to b modulo n when $n \mid (a - b)$. Written as $a \equiv b \pmod{n}$

V8 First Proof

Result 1: n be an integer. If n is even, then n^2 is even.

> *Proof:* Assume that n is an even number. Hence, we know that $n = 2k$ for some $k \in \mathbb{Z}$. It follows that $n^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ is an integer, we conclude that n^2 is even.

V9 More Proofs

Inequality proofs: oftentimes, the actual proof is written in backwards order compared to the natural brainstorming.

For example, to prove $x^2 + y^2 \geq 2xy$, we start from $(x-y)^2 \geq 0$ which we know is true.

V10 Logical Equivalence

- Tautology: statement that is always true
- Contradiction: statement that is always false

R and S are logically equivalent when $R \iff S$ is a tautology. Written as $R \quad \equiv \quad S$.

- Implication: $P \implies Q \quad \equiv \quad (\sim P) \vee Q$
- Contrapositive: $P \implies Q \quad \equiv \quad ((\sim Q) \implies (\sim P))$
- Biconditional: $P \iff Q \quad \equiv \quad ((P \implies Q) \wedge (Q \implies P))$
- Negation: $\sim(\sim P) \quad \equiv \quad P$
- $\wedge$ and $\vee$ are commutative, associative, and distributive
- DeMorgan's Laws:
  - $\sim(P \vee Q) \quad \equiv \quad (\sim P) \wedge (\sim Q)$
  - $\sim(P \wedge Q) \quad \equiv \quad (\sim P) \vee (\sim Q)$

V11 Proof by Contrapositive

Result 1: let $n \in \mathbb{Z}$. If n^2 is even then n is even.

> *Proof:* We prove the contrapositive: if n is odd, then n^2 is odd. Assume that n is odd.
>
> - Hence $n = 2l + 1$ for some $l \in \mathbb{Z}$ and so $n^2 = 4l^2 + 4l + 1 = 2(2l^2 + 2l) + 1$.
> - Since $2l^2 + 2l \in \mathbb{Z}$, it follows that n^2 is odd.
>
> Since the contrapositive is true, the original statement is true.

Result 2: let $n \in \mathbb{Z}$. If $3n + 7$ is odd then n is even.

> *Proof:* We prove the contrapositive. Assume that n is odd, so $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then $3n + 7 = 2(3k + 5)$ and since $3k + 5 \in \mathbb{Z}$ it follows that $3n + 7$ is even. Since the contrapositive is true, the result holds.

V12 Proof by Cases

Relies on $(P \vee Q) \implies R \quad \equiv \quad (P \implies R) \wedge (Q \implies R)$

Result 1: Let $n \in \mathbb{Z}$. Then $n^2 + 5n - 7$ is odd.

> *Proof:* Assume the hypothesis is true, so that $n \in \mathbb{Z}$. Hence n is even or odd.
>
> - *Case 1:* Assume that n is even, so that $n = 2k$ for some $k \in \mathbb{Z}$. Hence $n^2 + 5n - 7 = 4k^2 + 10k - 7 = 2(2k^2 + 5k - 4) + 1$. Thus $n^2 + 5n - 7$ is odd.
> - *Case 2:* Assume that n is odd, so that $n = 2l + 1$ for some $l \in \mathbb{Z}$. Hence

> $n^2 + 5n + 7 = 4l^2 + 4l + 1 + 10l + 5 - 7 = 2(4l^2 + 7l + 1)$. Thus $n^2 + 5n - 7$ is odd.
>
> Since $n^2 + 5n - 7$ is odd in both cases, the result holds.

Result 2: Let $n \in \mathbb{Z}$. If $3 \mid n^2$ then $3 \mid n$.

> *Proof:* We prove the contrapositive, so assume that $3 \nmid n$. By Euclidean division, we know that $n = 3a + 1$ or $n = 3a + 2$.
>
> - *Case 1:* Let $n = 3a + 1$, then $n^2 = 9a^2 + 6a + 1 = 3(3a^2 + 2a) + 1$ and so is not divisible by 3.
> - *Case 2:* Let $n = 3a + 2$, then $n^2 = 9a^2 + 12a + 4 = 3(3a^2 + 4a + 1) + 1$ and so is not divisible by 3.
>
> Since $3 \nmid n^2$ in both cases, the result holds.

V13 Quantifiers

Quantifiers can be used to turn open sentences into statements by adding scope.

- Universal quantifier $\forall$: "for all".
- Existential quantifier $\exists$: "there exists".
- Such that/so that: s.t.

V14 Negating Quantifiers

Let $P(x)$ be an open sentence over the domain A, then

- $\sim(\forall x \in A, P(x)) \equiv \exists x \in A \text{ s.t. } \sim(P(x))$
- $\sim(\exists x \in A \text{ s.t. } P(x)) \equiv \forall x \in A, \sim(P(x))$

Prove or disprove: $\exists n \in \mathbb{N} \text{ s.t. } 4 \mid (n^2 + 1)$

> We show the statement is false by proving its negation is true. We want to show that $\forall n \in \mathbb{N}, 4 \nmid (n^2 + 1)$. Since $n \in \mathbb{N}$ it is either even or odd.
>
> - Assume that n is even, so $n = 2k$ and thus $n^1 + 1 = 4k^1 + 1$.
> - Now assume that n is odd, so $n = 2l + 1$ and thus $n^2 = 4l^2 + 4l + 2$.

V15 Nested Quantifiers

Quantifiers do not commute

Result: $\forall x \in \mathbb{Z}, \exists w \in \mathbb{N}$ s.t. $z^2 < w$.

> *Proof:* Let z be any integer. Now choose $w = z^2 + 1$. We know that $w \in \mathbb{Z}$ and that $w \geq 1$, so $w \in \mathbb{N}$. Further, we know that $w > z^2$ so the statement is true.

V16 Existence Proofs

Constructive proof: give an example that works (do not need to show how we found the value)

Non-constructive proof: proof that it must exist (i.e. using Intermediate Value Theorem). Example is not explicitly given.

Uniqueness proof: First show existence. let x and y be such that both $P(x)$ and $P(y)$ are true. Then show that we must have $x = y$.

V17 Disproofs

- To disprove P, we prove $\sim P$.
- To disprove a universal quantifier, we need to provide a counterexample.
- To disprove an existential quantifier, we need to prove that it is always false.

V18 Induction

Used to proof $\forall n \in \mathbb{N}, P(n)$.

- Base case: prove $P(1)$
- Inductive step: prove $P(k) \implies P(k+1)$

Mathematical Induction

For all $n \in \mathbb{N}$ let $P(n)$ be a statement. Then if

- $P(1)$ is true, and
- $P(k) \implies P(k+1)$ is true for all $k \in \mathbb{N}$

then $P(n)$ is true for all $n \in \mathbb{N}$.

Result 1: for all $n \in \mathbb{N}, n^2 + 5n - 7$ is odd.

> *Proof:* We prove the result by induction.
>
> - Base case: When $n = 1$ we have $1 + 5 - 7 = -1$ which is odd.
> - Inductive step: Assume that $k^2 + 5k - 7$ is odd, so we can write
>
> $k^2 + 5k - 7 = 2l + 1$ for some $l \in \mathbb{Z}$ and so
>
> $(k+1)^2 + 5(k+1) - 7 = 2(l + k + 3) + 1$
>
>   and since $l + k + 3 \in \mathbb{Z}$. it follows that $(k+1)^2 + 5(k+1) - 7$ is odd.
>
> Since the base case and inductive step hold, the result follows by induction.

Result 2: For every natural number n, $3 \mid (4^n - 1)$.

> *Proof:* We prove the result by induction.
>
> - Base case: When $n = 1$ we have $3 \mid (4 - 1)$, so the result holds.
> - Inductive step: Assume that $3 \mid (4^k - 1)$, so $4^k = 3l + 1$ for some $l \in \mathbb{Z}$. Then
>
> $$4^{k+1} - 1 = 4(3l + 1) - 1 = 3(4l + 1)$$
>
>   and so $3 \mid (4^{k+1} - 1)$ as required.
>
> Since the base case and the inductive step hold, the result follows by induction.

V19 Proof of Induction

Sketch of a proof behind why induction works.

V20 More Induction

Result 1: Let $x > -1$, then for all $n \in \mathbb{N}$, $(1+x)^n \geq 1 + nx$.

> *Proof:* We proceed by induction. Assume that $x > -1$.
>
> - Base case: When $n = 1$ we have $1 + x = 1 + x$, as required.
> - Inductive step: Assume the result holds for $n = k$, so $(1+x)^k \geq (1+kx)$. Then
>
> $$\begin{aligned} (1+x)^{k+1} &\geq (1+x)(1+kx) && \text{since } 1+x > 0 \\ &= 1 + (k+1)x + kx^2 \\ &\geq 1 + (k+1)x && \text{since } kx^2 \geq 0 \end{aligned}$$
>
> and so the result holds for $n = k + 1$.
>
> By induction, the result holds for all $n \in \mathbb{N}$.

Result 2: for all $n \in \mathbb{N}$, $1 + 3 + \cdots + (2n-1) = n^2$.

> *Proof:* We prove the result by induction.
>
> - Base case: when $n = 1$ we have $(2-1) = 1^2$.
> - Inductive step: Assume $1 + 3 + \cdots + (2k-1) = k^2$. Then
>
> $1 + 3 + \cdots + (2k-1) + (2k+1) = k^2 + (2k+1) = (k+1)^2$ as required.
>
> By induction, the result holds for all $n \in \mathbb{N}$.

V21 Generalizing Induction

<u>Induction (arbitrary starting point)</u>

Let $l \in \mathbb{Z}$ and $s = \{n \in \mathbb{Z} \text{ s.t. } n \geq l\}$. Let $P(n)$ be a statement for all $n \in S$. Then if

- $P(l)$ is true, and
- $P(k) \implies P(k+1)$ is true for all integers $k \in S$

then $P(n)$ is true for all $n \in S$.

Result 1: For every integer $n \geq 5, 2^n \geq n^2$.

> *Proof:* We prove the result by induction. Since $2^5 = 32 > 25 = 5^2$, the result holds when $n = 5$. Now assume that $k \geq 5$ and that $2^k \geq k^2$. Then
>
> $$\begin{aligned} 2^{k+1} &\geq 2k^2 \\ &= k^2 + k^2 \\ &\geq k^2 + 5k = k^2 + 2k + 3k \\ &\geq k^2 + 2k + 1 \\ &= (k+1)^2 \end{aligned}$$

Theorem: Strong Mathematical Induction

Let $l \in \mathbb{Z}$ and $S = \{n \in \mathbb{Z} \text{ s.t. } n \geq l\}$. Let $P(n)$ be a statement for all $n \in S$. Then if

- $P(l)$ is true, and
- $(P(l) \wedge P(l+1) \wedge P(l+2) \wedge \cdots \wedge P(k)) \implies P(k+1)$ is true for all integer $k \in S$

then $P(n)$ is true for all $n \in S$.

Result 2: Let $\theta \in \mathbb{R}$ be fixed. Let $p_0 = 1$, $p_1 = \cos\theta$, and $p_n = 2p_1p_{n-1} - p_{n-2}$. Then $p_n = \cos(n\theta)$ for all integers $n \geq 0$.

Recall that $\cos(a+b) = \cos a \cos b - \sin a \sin b$ and $\cos(a-b) = \cos a \cos b + \sin a \sin b$.

> *Proof:* We prove the result by strong induction. When $n = 0$ we have $p_0 = \cos 0 = 1$ as required. Now assume that $p_j = \cos j\theta$ for $j = 0, 1, 2, \ldots, k$. Now consider $p_{k+1} = 2p_1p_k - p_{k-1}$.
>
> $$\begin{aligned} p_{k+1} &= 2\cos\theta\cos k\theta - \cos(k-1)\theta \\ &= 2\cos\theta\cos k\theta - (\cos k\theta \cos theta + \sin\theta \sin k\theta) \\ &= \cos\theta\cos k\theta - \sin\theta\sin k\theta \\ &= \cos(k+1)\theta \end{aligned}$$

V22 Subsets and Power Sets

Subset

Let A, B be sets.

- A is a subset of B means every element of A is also an element of B.
- Denoted as $A \subseteq B$. B is a superset of A, written as $B \supseteq A$
- Proper subset $A \subset B$: at least one element of B is not in A

$A = B \iff ((A \subseteq B) \wedge (B \subseteq B))$

Power Set

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

If $|A| = n$ then $|\mathcal{P}(A)| = 2^n$

V23 Set Operations

Let A, B be sets.

Union

The union of A and B is $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

Intersection

The intersection of A and B is $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

If $A \cap B = \varnothing$, then A and B are disjoint.

Difference

The difference $A - B = A \setminus B$ is $A \setminus B = \{x \in A : x \notin B\}$.

<u>Universal</u>

Given a universal set U (depends on context) and $A \subset U$, the complement of A is

$\bar{A} = \{x \in U : x \notin A\}$ or equivalently $x \in \bar{A} \iff x \notin A$.

<u>Ordered Pair</u>

Written as (a, b). Order matters. Do not confuse with interval notation.

<u>Cartesian Product</u>

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

V24 Set Proofs

Let A, B be sets.

<u>Subset and Equality</u>

- $(A \subseteq B) \quad \equiv \quad (\forall x \in A, x \in B) \quad \equiv \quad (x \in A \implies x \in B)$.
- $(A = B) \quad \equiv \quad ((A \subseteq B) \wedge (B \subseteq A)) \quad \equiv \quad ((x \in A) \iff (x \in B))$

<u>Intersection and Union</u>

- $(x \in A \cap B) \quad \equiv \quad (x \in A \wedge x \in B)$
- $(x \in A \cup B) \quad \equiv \quad (x \in A \vee x \in B)$

<u>Complement and Difference</u>

- $(x \in \bar{A}) \quad \equiv \quad (x \notin A) \quad \equiv \quad \sim(x \in A)$
- $(x \in A - B) \quad \equiv \quad ((x \in A) \wedge (x \notin B)) \quad \equiv \quad ((x \in A) \wedge \sim(x \in B))$

Result 1: Let $A = \{n \in \mathbb{Z} : 6 \mid n\}$ and $B = \{n \in \mathbb{Z} : 2 \mid n\}$, then $A \subseteq B$.

> *Proof:* Let the sets A, B as stated and assume that $a \in A$. Hence, we know that $6 \mid a$ and so $a = 6k$. This implies that $a = 2(3k)$ and so $2 \mid a$. By the definition of the set B, $a \in B$. So $A \subseteq B$ as required.

Result 2: Let A, B, C be sets. If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

> *Proof:* Assume that $A \subseteq B$ and $B \subseteq C$. Further, let $x \in A$. Since $A \subseteq B$, we know that $x \in B$. Then similarly, since $B \subseteq C$, we know that $x \in C$. Hence $A \subseteq C$ as required.

Result 3: Let A, B, C be sets, then $A \cup (B \cap C) = (A \cup C) \cap (A \cup B)$.

> *Strategy:* prove LHS is a subset of RHS, then prove that RHS is a subset of LHS.
>
> *Proof:* Let $x \in A \cup (B \cap C)$, so that $x \in A$ or $x \in B \cap C$. We consider each case separately.
>
> - Assume that $x \in A$, then we know that $x \in A \cup B$. Similarly, we have $x \in A \cup C$.
> - Now assume that $x \in B \cap C$, so that $x \in B$ and $x \in C$.

Since $x \in B$ it follows that $x \in B \cup A$. Similarly, because $x \in C$, $x \in C \cup A$.

In both cases, $x \in (A \cup B)$ and $x \in (A \cup C)$. Hence $x \in (A \cup C) \cap (A \cup B)$ as required.

Now let $x \in (A \cup C) \cap (A \cup B)$, so that $x \in A \cup C$ and $x \in A \cup B$.

- If $x \in A$, then $x \in A \cup (B \cap C)$.
- If $x \notin A$, then we must have $x \in B$ and $x \in C$, which implies that $x \in B \cap C$, so $x \in A \cup (B \cap C)$.

In both cases, we have $x \in A \cup (B \cap C)$ as required.

V25 More Set Proofs

Cartesian and Power Set Proofs

Result: Let A, B, C be sets, then $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Proof: First, we will show that $A \times (B \cup C) \supseteq (A \times B) \cup (A \times C)$.

Assume that $(x, y) \in (A \times B) \cup (A \times C)$. Then either $(x, y) \in A \times B$ or $(x, y) \in A \times C$.

- Case 1: When $(x, y) \in A \times B$, we have $x \in A$ and $y \in B$. Hence, $y \in B \cup C$.
- Case 2: When $(x, y) \in A \times C$, we have $x \in A$ and $y \in C$. Hence, $y \in C \cup B$.

In both cases, $x \in A$ and $y \in B \cup C$, so $(x, y) \in A \times (B \cup C)$.

Next, we will show that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.

Assume that $(x, y) \in A \times (B \cup C)$. Then $x \in A$ and $y \in B \cup C$. Either $y \in B$ or $y \in C$.

- Case 1: When $y \in B$, we have $(x, y) \in A \times B$, so $(x, y) \in (A \times B) \cup (A \times C)$.
- Case 2: When $y \in C$, we have $(x, y) \in A \times C$, so $(x, y) \in (A \times C) \cup (A \times B)$.

In both cases, $(x, y) \in (A \times B) \cup (A \times C)$.

Useful Results for Sets

1. $X \subseteq A \implies X \subseteq A \cup B$.
2. $X \subseteq A \cap B \implies X \subseteq A$.
3. $(X \subseteq A) \wedge (X \subseteq B) \iff X \subseteq A \cap B$.

Result 1: Let A, B be sets. Then $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

Proof: Let $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$. Then $X \subseteq A$ or $X \subseteq B$.

- Case 1: If $X \subseteq A$ then $X \subseteq A \cup B$ so $x \in \mathcal{P}(A \cup B)$.
- Case 2: If $X \subseteq B$ then $X \subseteq A \cup B$ so $x \in \mathcal{P}(A \cup B)$.

Disproof of Reverse Inclusion:

Let $A = \{1\}, B = \{2\}$, and $X = \{1, 2\}$. Then $X \in \mathcal{P}(A \cup B)$, however $X \notin \mathcal{P}(A) \cup \mathcal{P}(B)$. Hence $\mathcal{P}(A \cup B) \nsubseteq \mathcal{P}(A) \cup \mathcal{P}(B)$.

Result 2: Let A, B be sets. Then $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

> *Proof:* Assume that $X \in LHS$. Then $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$, and so $X \subseteq A$ and $X \subseteq B$. Hence $X \subseteq A \cap B$, and thus $X \in RHS$.
>
> - Now assume that $Y \in RHS$. Then $Y \in \mathcal{P}(A \cap B)$ and so $Y \subseteq A \cap B$. This means that $Y \subseteq A$ and $Y \subseteq B$. Hence $Y \in \mathcal{P}(A)$ and $Y \in \mathcal{P}(B)$, and thus $Y \in LHS$.

V26 Relations

Relations

Let A be a set.

- A relation, R, on A is a subset $R \subseteq A \times A$.
- If $(x, y) \in R$, we write $x \; R \; y$ and otherwise we write $x \not R \; y$

Special relations

- $R = \varnothing$ is the trivial relation on A
- $S = B \times B$ is the universal relation on A

V27 Properties and Congruence

Properties of Relations

Let R be a relation on a set A. Then R is

- **Reflexive** when $a \; R \; a$.
- **Symmetric** when $a \; R \; b \implies b \; R \; a$.
- **Transitive** when $(a \; R \; b) \wedge (b \; R \; c) \implies a \; R \; c$

Theorem: congruence modulo n is reflexive, symmetric, and transitive.

V28 Equivalence Relations & Classes

Equivalence Relations

R is an equivalence relation when it is reflexive, symmetric, and transitive.

Equivalence Classes

Let R be an equivalence relation on A.

The equivalence class of $x \in A$ (with respect to R) is $[x] = \{a \in A : a \; R \; x\}$.

- We always have $a \in [a]$.
- If $a, b \in A$, then $[a] = [b] \iff a \; R \; b$.

V29 Set Partitions

Properties of equivalence classes

- Equivalence classes are either equal or disjoint (completely separate). Either $[a] = [b]$ or $[a] \cap [b] = \varnothing$.

Partition

A partition of the set A is a set $\mathcal{P}$ of non-empty subsets of A so that

- $\varnothing \notin \mathcal{P}$.
- If $x \in A$ then there is $X \in \mathcal{P}$ such that $x \in X$.
- If $X, Y \in \mathcal{P}$ then either $X \cap Y = \varnothing$ or $X = Y$.

The elements of $\mathcal{P}$ are called parts or pieces.

Theorem: The set of equivalence classes of R form a set partition.

Theorem: Let $\mathcal{P}$ be a set partition of A. Define a relation by $x\ R\ y \iff \exists X \in \mathcal{P}\ \text{s.t.}\ x, y \in X$. Then R is an equivalence relation.

V30 Integers Modulo n

The equivalence relation $\equiv \pmod n$ partitions $\mathbb{Z}$: $\{[0], [1], [2], \ldots, [n-1]\}$.

Theorem: Let $n \in \mathbb{N}$ and let $a, b \in \{0, 1, \ldots, n-1\}$.

If $x \in [a]$ and $y \in [b]$ then $x + y \in [a+b]$ and $x \cdot y \in [a \cdot b]$.

Integers modulo n: $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$

$[a] + [b] = [a+b]$ and $[a] \cdot [b] = [a \cdot b]$.

V31 Functions

A function $f: A \to B$ takes inputs from A and gives outputs in B. $f \subseteq A \times B$.

- Existence: for every $a \in A$, there exists $b \in B$ so that $(a, b) \in f$.
- Uniqueness: If $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.
- Domain is A, codomain is B. $\text{range}(f) \subseteq \text{codomain}(f)$
- If $(a, b) \in f$ we write $f(a) = b$. b is the image of a

V32 Images and Preimages

Let $f: A \to B$ be a function and let $C \subseteq A$ and $D \subseteq B$.

- The image of C in B is $f(C) = \{f(x)\ \text{s.t.}\ x \in C\}$.
- The preimage of D in A is $f^{-1}(D) = \{x \in A\ \text{s.t.}\ f(x) \in D\}$.
  - $x \in f^{-1}(D) \iff f(x) \in D$.

Theorem: Let $f: A \to B$ and $C \subseteq A$ and $D \subseteq B$. Then

- $C \subseteq f^{-1}(f(C))$
- $f(f^{-1}(D)) \subseteq D$.

Let $C_1, C_2 \subseteq A$ and $D_1, D_2 \subseteq B$.

- $f(C_1 \cap C_2) \subseteq f(C_1) \cap f(C_2)$

- $f(C_1 \cup C_2) = f(C_1) \cup f(C_2)$
- $f^{-1}(D_1 \cap D_2) = f^{-1}(D_1) \cap f^{-1}(D_2)$
- $f^{-1}(D_1 \cup D_2) = f^{-1}(D_1) \cup f^{-1}(D_2)$

V33 Injections, Surjections, and Bijections

Let $f: A \to B$ be a function.

- Injective: for all $a_1, a_2 \in A$, if $a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$. Contrapositive: $f(a_1) = f(a_2) \implies a_1 = a_2$.
- Surjective: for all $b \in B$, exists $a \in A$ such that $f(a) = b$.
- Bijective: both injective and surjective.

V34 Compositions

Let $f: A \to B$ and $g: B \to C$. The composition of f and g, denoted by $g \circ f$, defines a new function $g \circ f: A \to C$, where $(g \circ f)(a) = g(f(a))$.

Theorems

- If f and g are injective then so is $g \circ f$.
- If f and g are surjective then so is $g \circ f$.
- If f and g are bijective then so is $g \circ f$.

Theorems

- If $g \circ f$ is an injection then f is an injection
- If $g \circ f$ is a surjection then g is a surjection

V35 Inverse Functions

Let $f: A \to B$ and $g: B \to A$ be functions.

- If $g \circ f = i_A$ then g is a left-inverse of f
- If $f \circ g = i_B$ then we say that g is a right-inverse of f.
- If g is both a left-inverse and right-inverse, then we call it an inverse of f

Inverse is denoted by f^{-1}.

Theorems

- If f has a left-inverse then it is injective
- If f has a right-inverse then it is surjective

Lemma

- If f has a left-inverse g and a right-inverse h, then $g = h$

Theorem: inverse functions

- Let $f: A \to B$. Then f has an inverse if and only if f is bijective. The inverse, if it exists, is unique.

V36 Proof by Contradiction

Warning: Do NOT overuse proof by contradiction. They are often suitable for **not-** results (i.e. non-existence or irrationality).

Relies on law of the excluded middle and modus tollens

- Law of the excluded middle: $P \vee \sim P$ is a tautology.
- Modus tollens: $(P \implies Q)$ is true and Q is false, so P must be false

Proof by contradiction to prove P

- Assume $\sim P$ is true
- Prove a chain of implications

$$\begin{aligned} (\sim P) &\implies P_1 \\ P_1 &\implies P_2 \\ &\vdots \\ P_{n-1} &\implies P_n \\ P_n &\implies \text{contradiction} \end{aligned}$$

- By modus tollens, $(\sim P)$ must be false, and so P is true.

Result: There is no smallest positive real number.

> *Proof:* Assume, to the contrary, that there does exist a smallest real number q. Then the number $r = q/2$ satisfies $0 < r < q$. Hence, r is a positive real number that is smaller than q, which contradicts our assumption that q is the smallest positive real. Thus, there is no smallest positive real number.

V37 Proof by Contradiction - Examples

Result 1: There are no integers a, b so that $2a + 4b = 1$.

> *Proof:* Assume, to the contrary, that the result is false. So there are $a, b \in \mathbb{Z}$ so that $2a + 4b = 1$. Dividing by 2 gives $a + 2b = \frac{1}{2}$. However, this cannot happen since the sum of integers is an integer. Hence there cannot be such integers a, b and so the result holds.

Result 2: There are no integers a, b so that $a^2 - 4b = 3$.

> *Proof:* Assume, to the contrary, that we can find $a, b \in \mathbb{Z}$ with $a^2 - 4b = 3$. Rewrite as $a^2 = 3 + 4b$ and notice that RHS is odd, so the LHS must also be odd, which means that a is odd (which we have shown previously). Hence we can write $a = 2k + 1$ for some $k \in \mathbb{Z}$ and so we have
>
> $3 = a^2 - 4b = (2k+1)^2 - 4b = 4k^2 + 4k + 1 - 4b = 4(k^2 + k - b) + 1$
>
> which means that $3 \equiv 1 \pmod 4$, a contradiction. Thus, the result follows.

Rational and Irrational

Let q be a real number.

- Rational: q is rational if we can write $q = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $b \neq 0$.

$\exists a \in \mathbb{Z}$ s.t. $\exists b \in \mathbb{Z} - \{0\}$ s.t. $q = \frac{a}{b}$.

- Irrational: q is irrational if it is not rational.

  $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z} - \{0\}, q \neq \frac{a}{b}$.

  Denoted as $\mathbb{I} = \mathbb{R} - \mathbb{Q}$

Result 3: If $x \in \mathbb{Q}$ and $y \in \mathbb{I}$ then $x + y \in \mathbb{I}$.

> *Proof:* Assume, to the contrary, that there is $x \in \mathbb{Q}$ and $y \in \mathbb{I}$ so that $x + y \in \mathbb{Q}$. This implies that $x = \frac{a}{b}$ and $(x + y) = \frac{c}{d}$ with $a, b, c, d \in \mathbb{Z}$ and $b, d \neq 0$. From this we see that $y = (x + y) - x = \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd}$ and hence $y \in \mathbb{Q}$. This contradicts our assumption that $y \in \mathbb{I}$, and so the result follows.

V38 Proof by Contradiction - Famous Proofs

Lemma 1: let $n \in \mathbb{N}$, then n is even if and only if n^2 is even.

> Forward implication is easy to prove, reverse implication can be proven with contrapositive

Result 1: $\sqrt{2}$ is irrational.

> *Proof:* Assume, to the contrary, that $\sqrt{2} \in \mathbb{Q}$. Hence we can write $\sqrt{2} = \frac{a}{b}$ so that $b \neq 0$ and $\gcd(a, b) = 1$. Since $\sqrt{2} = \frac{a}{b}$, we have $a^2 = 2b^2$. Thus a^2 is even, and so a is even. Hence write $a = 2c$ where $c \in \mathbb{Z}$. But now, since $a^2 = 2b^2$, we know that $4c^2 = 2b^2$ and so $b^2 = 2c^2$. Hence b^2 is even, and so b is even. This gives a contradiction since we assumed that $\gcd(a, b) = 1$. Thus, $\sqrt{2}$ is irrational.

Lemma 2: let $n \in \mathbb{N}$. If $n \geq 2$ then n is divisible by a prime.

> *Proof:* We prove this by strong induction.
>
> - Base case: since 2 is prime and $2 \mid 2$, the result holds when $n = 2$
> - Inductive step: let $k \in \mathbb{N}$ with $k \geq 2$ and assume that the result holds for all integers $2, 3, \ldots, k$.
>   - If $k + 1$ is not prime then since $(k + 1) \mid (k + 1)$, the result holds at $n = k + 1$.
>   - If $k + 1$ is not prime, then $(k + 1) = ab$ for integers $a, b \geq 2$. But by assumption, both a, b have prime divisors, ands o $a = pc, b = qd$ where $c, d \in \mathbb{N}$ and p, q are prime. Hence $(k + 1) = pqcd$ and so the result holds at $n = k + 1$.
>
> The result follows by strong induction.

Result 2: there are an infinite number of primes.

> *Proof:* Assume, to the contrary, that there is a finite list of primes: $\{p_1, p_2, \ldots, p_n\}$.
>
> Use this list to construct $N = p_1 \cdot p_2 \cdot p_3 \cdots p_n \in \mathbb{N}$, and then consider $(N + 1)$.
>
> - If $(N + 1)$ is prime, then we have found a new prime larger than all on our list, which is a contradiction.
> - If it is not prime, then by Lemma 2, $(N + 1)$ has some p_k as a divisor. But then $p_k \mid N$ and $p_k \mid (N + 1)$ so
>
> $1 = (N + 1) - N = p_k b - p_k a = p_k(b - a)$ for some $a, b \in \mathbb{N}$
>
>   which implies that $p_k \mid 1$, which is a contradiction.
>
> So the list of primes cannot be finite.

V39 Cardinality of Finite Sets

Cardinality: $|A|$ is the number of elements in A.

- $|A| = n$ means there is a bijection from A to $\{1, 2, \ldots, n\}$.
- If $|A| = |B|$ then A and B are equinumerous.

Let A, B be sets. They have the same cardinality if $A = B = \varnothing$ or if there is a bijection from A to B.

Pigeonhole Principle: If n objects are placed in k boxes then:

- If $n < k$ then at least one box has zero objects in it.
- If $n > k$ then at least one box has at least two (or more refined $\lceil n/k \rceil$) objects in it.

Corollaries of Pigeonhole

Let A, B be finite sets and let $f: A \to B$. Then

- If f is an injection then $|A| \leq |B|$.
- If f is a surjection then $|A| \geq |B|$.

Result 1: there exist two pwoers of 3 whose difference is divisible by 220.

> *Proof:* Consider the sequence of 221 numbers $3^0, 3^1, 3^2, 3^3, \ldots, 3^{219}, 3^{220}$. There are at most 220 possible remainders, but 221 numbers in the sequence. Hence two numbers have the same remainder: $3^i = 220k + r$ and $3^j = 220l + r$ for some i, j. So their difference is a multiple of 220 as required.
>
> We can check that $220 \mid (3^{20} - 3^0)$.

Result 2: place 5 points in an equilateral triangle of side-length 1. There is a pair at distance no greater than 0.5.

> *Proof:* Split the triangle into 4 sub-triangles as shown. The subtriangle side-length is $\frac{1}{2}$.
>
> One sub-triangle must contain 2 points, so those points are at distance $\leq \frac{1}{2}$.

V40 Towards Infinite Sets

Equinumerous: same size. "Being equinumerous" is an equivalence relation.

Result: Let $\mathcal{E} = \{n \in \mathbb{N},\ \text{s.t. } n \text{ is even}\}$ and $\mathcal{O} = \{n \in \mathbb{N}\, \text{s.t. } n \text{ is odd}\}$, then $|\mathcal{O}| = |\mathcal{E}|$. Furthermore, $|\mathbb{N}| = |\mathcal{E}|$.

> The function $f : \mathcal{O} \to \mathcal{E}$ defined by $f(n) = n + 1$ is a bijection.
>
> The function $g : \mathbb{N} \to \mathcal{E}$ defined by $g(n) = 2n$ is a bijection.

Let A, B with $A \subset B$.

- If A, B are finite then PHP tells us $|A| \neq |B|$.
- If A, B are infinite then a bijection maybe possible.

Infinite Set: a set A is infinite if there is a bijection from A to a proper subset of A.

The First Infinity:

- A set A is denumerable if there is a bijection $f: \mathbb{N} \to A$.
- Cardinality of denumerable set is $\aleph_0$ - "aleph-null
- Countable: either finite or denumerable

V41 Denumerable Sets

A set B is denumerable when we can "list out" its elements $\iff$ there exists a bijection $g: \mathbb{N} \to B$.

- Elements in list do not repeat - injective
- Any given element $y \in B$ appears at a finite position - surjective

Result 1: The set of all integers is denumerable.

> *Proof:* List the elements $z \in \mathbb{Z}$ as $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$ so that
>
> - If $z \geq 1$, then z appears at position $2z$;
> - If $z \leq 0$, then z appears at position $1 - 2z$.
>
> The list does not repeat and any given $z \in \mathbb{Z}$ appears at some finite position. Hence the list defines a bijection between $\mathbb{N}$ and $\mathbb{Z}$.

Theorem: Let A, B be sets with $A \subseteq B$. If B is denumerable then A is countable; there is no smaller infinity.

> *Proof Sketch:* If A is finite then A is countable.
>
> If A is not finite, then list out B nicely, and then delete the elements in the list that are not in A. The resulting list does not repeat, and also every element in A appears at some finite position in the list. Hence A is denumerable and is thus countable.

Result 2: Let $k \in \mathbb{N}$, then the following sets are denumerable.

$$k\mathbb{Z} = \{kn : n \in \mathbb{Z}\} \quad \text{and} \quad k\mathbb{N} = \{k\mathbb{m} : n \in \mathbb{N}\}$$

> We can use the previous theorem. These sets are subset of $\mathbb{Z}$, which is denumerable. Since the sets are not finite, they must be denumerable.

Let A, B be countable sets, then:

- $A \cap B$ and $A \cup B$ are all countable.
- $A \times B$ is countable.

Result 3: The set of all rational numbers $\mathbb{Q}$ is denumerable.

> *Proof Sketch:*
>
> - Note that any $q \in \mathbb{Q}$ can be written uniquely as $q = \frac{a}{b}$ with $a \in \mathbb{Z}, b \in \mathbb{N}$ and $\gcd(a, b) = 1$.
> - We can rewrite rationals as $P = \{(a, b) \in \mathbb{Z} \times \mathbb{N} \, \text{s.t.} \, \gcd(a, b) = 1\}$.
> - There is a bijection $f: \mathbb{Q} \to P$ given by $f(a/b) = (a, b)$, where a/b is the reduced fraction.
> - Since $P \subseteq \mathbb{Z} \times \mathbb{N}$, we know that P is denumerable.
> - Since $|P| = |\mathbb{Q}|$, we have that Q is also denumerable.

V42 Uncountable Sets

Facts:

- Every rational number has a repeating decimal expansion
- Some rationals have two repeating expansions. For example, $1/2 = 0.500000\ldots = 0.499999\ldots$ This only happens when the reduced fraction a/b is a product of 2s and 5s.
- Every irrational number has a unique non-repeating decimal expansion

Result 1 (Cantor 1891): The open interval $(0,1) = \{x \in \mathbb{R} \text{ s.t. } 0 < x < 1\}$ is uncountable.

> Assume, to the contrary, that $(0,1)$ is countable. Since it is infinite, it is denumerable, and so there is a bijection $f\colon N \to (0,1)$.
>
> We can use this bijection to list all the numbers in $(0,1)$, and if there are two decimal expansions then choose the expansion that ends in 0s.
>
> Denote the k^{th} digit of $f(n)$ as $f_{n,k}$. The diagonal is $\Delta = 0.d_1d_2d_3d_4\ldots$, and the n^{th} digit of the diagonal as $d_n = f_{n,n}$.
>
> Create a new number $z = 0.z_1z_2z_3z_4\ldots$ via $z_n = \begin{cases} 1 & \text{if } d_n \neq 1 \\ 2 & \text{if } d_n = 1 \end{cases}$, chosen so that for all $n \in \mathbb{N}$, $z_n \neq d_n = f_{n,n}$.
>
> Since $0.11111\ldots \leq z \leq 0.22222\ldots$, we have $z \in (0,1)$ so z must be somewhere in the table. If $z = f(k)$ then we must have $z_k = f_{k,k}$, but $f_{k,k} = d_k \neq z_k$ be construction, which is a contradiction.
>
> Hence z is not in the table, so $(0,1)$ is uncountable.

Result 2: The set of all real numbers is uncountable. Additionally $|(0,1)| = |\mathbb{R}| = c$.

> Contrapositive of a previous theorem: if A is uncountable then its superset B is uncountable. Hence $\mathbb{R}$ is uncountable.
>
> To show that $|(0,1)| = |\mathbb{R}|$, we can show that $g\colon (0,1) \to \mathbb{R}$ defined by $g(x) = \frac{1}{1-x} - \frac{1}{x}$ is a bijection.

V43 More Infinities

Comparing Infinite Sets

- $|A| \leq |B|$ means there is an injection from A to B.
- $|A| < |B|$ means there is an injection from A to B but no bijection. $|A| < |B| \iff (|A| \leq |B|) \wedge (|A| \neq |B|)$.

Continuum Hypothesis: There is no set A so that $\aleph_0 < |A| < c$.

Cantor's Theorem: Let A be a set. Then $|A| < |\mathcal{P}(A)|$.

> *Proof Sketch:*
>
> First we show that $|A| \leq |\mathcal{P}(A)|$. Consider $f\colon A \to \mathcal{P}(A)$ defined by $f(a) = \{a\}$, which is an injection from A to $\mathcal{P}(A)$. Hence, $|A| \leq |\mathcal{P}(A)|$.
>
> To show that $|A| \neq |\mathcal{P}(A)|$, it suffices to show that there cannot be a surjection from A to $\mathcal{P}(A)$.
>
> Assume, to the contrary, that there exists a surjection $g\colon A \to \mathcal{P}(A)$, and define $B = \{x \in A \text{ s.t. } x \notin g(x)\}$. Since g is a surjection, there must exist some $b \in A$ so that $g(b) = B$.

> We must either have $b \in B$ or $b \notin B$.
>
> - If $b \in B$, then by definition, $b \notin g(b) = B$, a contradiction.
> - If $b \notin B$, then by definition, $b \in g(b) = B$, also a contradiction.
>
> Hence g is not surjective, so g is not bijective, which means $|A| \neq |\mathcal{P}(A)|$.
>
> We conclude that $|A| < |\mathcal{P}(A)|$.

Cantor-Schröder-Bernstein Theorem: $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$.

Corollary of Cantor's Theorem: there are an infinite number of different infinities.

> $$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| < \cdots$$
>
> We can create larger and larger infinite sets by repeatedly taking power sets.