MATH 220 Class Notes

W1b 9/6

MATH 220: logic and set theory + presentation and communication

Sets

- $\{\} = \emptyset$: empty set
- $\{2, 3\}$: finite set
- $\{1, 2, 3, 4, \ldots\}$: infinite set
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$: shorthand infinite sets
- $\{n^2 \mid n \in \mathbb{Z}\}$: set builder notation

W1c 9/8

Claim: $A := \{4x + 3y \mid x, y \in \mathbb{Z}\} = \mathbb{Z}$.

Proof:

First, let $a \in A$ so that $a = 4x + 3y$ for some integers x and y. Since products and sums of integers are integers, $a \in \mathbb{Z}$.

Second, let $n \in \mathbb{Z}$, and observe that $n = 4n + 3 \cdot (-n)$. Letting $x = n$ and $y = -n$, we see that $n \in A$.

We conclude that $A \in \mathbb{Z}$.

W2a 9/11

Logic

- Logical statement: can be evaluated to be true or false.
- Open sentence: not well-defined statement. Avoid.

Logical operators

- and: $\wedge$
- or: $\vee$
- negative: $\sim$
- implication: $\implies$

Implication:

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

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

W2b 9/13

Claim: If n is even, then $n^2 + 4n + 5$ is odd.

Proof:

Since n is even, we can write $n = 2x$ for some integer x. It follows that $n^2 + 4n + 5 = 4x^2 + 8x + 5 = 2(2x^2 + 4x + 2) + 1$, which is odd.

W2c 9/15

Claim: for all $n \in \mathbb{Z}$, if $2 \mid n$ and $3 \mid n$, then $6 \mid n$.

Proof:

Assume that $2 \mid n$ so $n = 2x$ and $3 \mid n$ so $n = 3y$ for some integers x, y. Then $6(x - y) = 3n - 2n = n$, and since $x - y$ is an integer, we conclude that $6 \mid n$.

Claim: for all $x \in \mathbb{R}$, if $x > 0$, then $x + \frac{2}{x} > 2$.

Proof 1:

Let $x \in \mathbb{R}$ and assume that $x > 0$. We know that $(x - 1)^2 + 1 > 0$. It follows that $x^2 - 2x + 1 + 1 > 0$, which implies that $x^2 + 2 > 2x$. Since $x > 0$, we can divide by x to get $x + \frac{2}{x} > 2$.

Proof 2:

Let $x \in \mathbb{R}$ and assume that $x > 0$. We proceed with casework.

- *Case 1:* $0 < x \leq 1$. Then $\frac{2}{x} \geq 2$ and $x > 0$, so $x + \frac{2}{x} > 2$.
- *Case 2:* $1 < x \leq 2$. Then $\frac{2}{x} \geq 1$ and $x > 1$, so $x + \frac{2}{x} > 2$.
- *Case 3:* $x > 2$. Then $x > 2$ and $\frac{2}{x} > 0$, so $x + \frac{2}{x} > 2$.

W3a 9/18

- **Style**: <u>avoid symbolic logic notation in proofs</u>
- Proving a biconditional $P \iff Q$: we prove $P \implies Q$ and $Q \implies P$.

Claim: Let $n \in \mathbb{Z}$, then $n \equiv 3 \pmod 5$ if and only if $5 \mid 2n + 1$.

Proof: continued next class

W3b 9/20

Claim: Let $n \in \mathbb{Z}$. Show that $n \equiv 3 \pmod 5$ if and only if $5 \mid (3n + 1)$.

Proof:

- Forward direction: Let $n \in \mathbb{Z}$. Assume that $n \equiv 3 \pmod 5$, so we can write $n = 5x + 3$ for some integer x. It follows that $3n + 1 = 3(5x + 3) + 1 = 15x + 10 = 5(3x + 2)$. Since $3x + 2$ is an integer, we obtain that $5 \mid 3n + 1$.
- Reverse direction: Let $n \in \mathbb{Z}$. We prove the contrapositive. Assume that

Claim: for all $n \in \mathbb{Z}$,

1. $n^2 + 3n + 8$ is even
2. $2n^2 + n + 1$ is not a multiple of 3

Proof of 1:

Let $n \in \mathbb{Z}$. We consider two cases.

- *Case 1:* assume that n is even, so we can write $n = 2x$ for some integer x. It follows that $n^2 + 3n + 8 = 4x^2 + 6x + 8 = 2(2x^2 + 3x + 4)$, which is even.
- *Case 2:* assume that n is odd, so we can write $n = 2y + 1$ for some integer y. It follows that $n^2 + 3n + 8 = (2y + 1)^2 + 3(2y + 1) + 8 = 4y^2 + 10y + 12 = 2(2y^2 + 5y + 6)$, which is even.

Since we have covered all cases, we conclude that $n^2 + 3n + 8$ is even.

Proof of 2:

Let $n \in Z$. We consider three cases.

- *Case 1:* assume that $n \equiv 0 \pmod 3$, so we can write $n = 3x$ for some integer x. It follows that $2n^2 + n + 1 = 18x^2 + 3x + 1 = 3(6x^2 + 1) + 1$, which is not a multiple of 3.
- *Case 2:* assume that $n \equiv 1 \pmod 3$, so we can write $n = 3y + 1$ for some integer y. It follows that $2n^2 + n + 1 = 2(3y + 1)^2 + (3y + 1) + 1 = 18y^2 + 15y + 4 = 3(6y^2 + 5y + 1) + 1$, which is not a multiple of 3.
- *Case 3:* assume that $n \equiv 2 \pmod 3$, so we can write $n = 3z + 2$ for some integer z. It follows that $2n^2 + n + 1 = 2(3z + 2)^2 + (3z + 2) + 1 = 18z^2 + 27z + 11 = 3(6z^2 + 9z + 3) + 2$, which is not a multiple of 3.

Since we have covered all cases, we conclude that $2n^2 + n + 1$ is not a multiple of 3.

W3c 9/22

Definition: A rational number is any number of the form $\frac{a}{b}$ for $a, b \in \mathbb{Z}$ and $b \neq 0$. Any real number which is not rational is irrational.

Claim: Let $a, b \in \mathbb{R}$. Then if $a \neq b$, then $\frac{a+b}{2} > a$ or $\frac{a+b}{2} > b$.

Proof: If $a \neq b$, then either $a > b$ or $a < b$.

- If $a > b$, then $a + b > 2b$ and so $\frac{a+b}{2} > b$.
- If $b > a$, then $a + b > 2a$ and so $\frac{a+b}{2} > a$.

In both cases, one of the inequalities is true.

Claim: Let $x \in \mathbb{R}$. If x is irrational, then $x^{1/3}$ is irrational.

Proof: We prove the contrapositive. Assume that $x^{1/3}$ is rational, so $x^{1/3} = \frac{a}{b}$ for some integers a and $b \neq 0$. It follows that $x = (x^{1/3})^3 = \frac{a^3}{b^3}$, and since $b^3 \neq 0$, x is rational.

Claim: Prove that for all $n \in \mathbb{Z}$, if $3 \mid n^2$, then $3 \mid n$.

Proof: We prove the contrapositive. Assume that $3 \nmid n$, so either $n \equiv 1 \pmod 3$ or $n \equiv 2 \pmod 3$.

- *Case 1:* $n \equiv 1 \pmod 3$. Then $n^2 \equiv 1 \pmod 3$, so n^2 is not a multiple of 3.
- *Case 2:* $n \equiv 2 \pmod 3$. Then $n^2 \equiv 4 \equiv 1 \pmod 3$, so n^2 is not a multiple of 3.

We conclude that n^2 is not a multiple of 3.

W4a 9/25

- Missed class

W4b 9/27

Claim: For all $x, y \in \mathbb{R}$, $(\forall z > 0, |x - y| < z) \implies x = y$.

Proof:

We prove the contrapositive: suppose $x \neq y$, and we want to prove that there exists $z > 0$ so that $|x - y| \geq z$.

- If $x > y$, then $x - y > 0$. Let $z = x - y$. Then $|x - y| = x - y = z \geq z$.
- If $x < y$, then $x - y < 0$. Let $z = -(x - y)$. Then $|x - y| = -(x - y) = y - x = z \geq z$.

Claim: (1) Prove that $\forall x \in \mathbb{I}$, $(k \in \mathbb{Q} \text{ and } k \neq 0) \implies \frac{x}{k} \in \mathbb{I}$.

Scratchwork:

$P \implies (Q \implies R)$

- P : $x \in \mathbb{I}$
- Q : $k \in \mathbb{Q} \text{ and } k \neq 0$
- R : $\frac{x}{k} \in \mathbb{I}$

$\equiv \sim(Q \implies R) \implies \sim P$

$\equiv (Q \wedge \sim R) \implies \sim P$

Which is: $(k \in \mathbb{Q} \text{ and } k \neq 0 \text{ and } \frac{x}{k} \in \mathbb{Q}) \implies x \in \mathbb{Q}$

Much easier to prove.

My Proof:

We prove the contrapositive. Choose an arbitrary $x \in \mathbb{I}$, and suppose that $\frac{x}{k} \in \mathbb{Q}$. We want to prove that $k \in \mathbb{I}$ or $k = 0$.

Since $\frac{x}{k}$ is rational, we can write $\frac{x}{k} = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ with $b \neq 0$. In particular, $a \neq 0$ because that would result in $x = 0$, which contradicts the assumption that $x \in \mathbb{I}$.

Then $k = \frac{b}{a}x$. To show that $k \in \mathbb{I}$, we prove the contrapositive: assume that $x \in \mathbb{Q}$, and we want to show that $k \in \mathbb{Q}$. Since $x \in \mathbb{Q}$, we have $x = \frac{c}{d}$ for $c, d \in \mathbb{Z}$ with $d \neq 0$. Then $k = \frac{b}{a} \cdot \frac{c}{d} = \frac{bc}{cd}$, which is rational. Since the contrapositive is true, we obtain that k is irrational.

Since we have shown that $k \in \mathbb{I}$, we know that $k \in \mathbb{I}$ or $k = 0$, as desired.

W4c 9/29

Bounded: a function $f : \mathbb{R} \to \mathbb{R}$ is bounded if $\exists M \in \mathbb{R}$ so that $\forall x \in \mathbb{R}$, $|f(x)| \leq M$.

Claim: Show that $f(x) = 2\sin(x) + 1$ is bounded.

Proof: we know that $-1 \leq \sin(x) \leq 1$ for all $x \in \mathbb{R}$. Therefore, $-2 \leq 2\sin(x) \leq 2$ and $-1 \leq 2\sin(x) + 1 \leq 3$ for all x. In particular, if we choose $M = 3$, then $-M \leq 2\sin(x) + 1 \leq M$ for all $x \in \mathbb{R}$. Therefore, $f(x)$ is bounded.

Claim: Show that $f(x) = 2x + 5$ is not bounded.

Proof:

We prove the negation: $\forall M \in \mathbb{R}, \exists x \in \mathbb{R} \text{ so that } |f(x)| > M$.

Let $M \in \mathbb{R}$. Choose $x = |M|$, so $f(x) = 2x + 5 = 2|M| + 5 \geq M$.

Continuity: A function $f : \mathbb{R} \to \mathbb{R}$ is continuous if $\forall \varepsilon > 0$, $\exists \delta > 0$ so that for all $x_1, x_2 \in \mathbb{R}$,
$|x_1 - x_2| < \delta \implies |f(x_1) - f(x_2)| < \varepsilon$.

Claim: $\forall \varepsilon > 0, \exists N \in \mathbb{N} \text{ so that } \forall n \in \mathbb{N}, (n > N) \implies \left(\frac{1}{n} < \varepsilon\right)$.

Proof: Let $\varepsilon > 0$ be arbitrary. Take $N = \lceil \frac{1}{\varepsilon} \rceil > 0$.

For all $n > N$, we have $\frac{1}{n} < \frac{1}{N} = \frac{1}{\lceil \frac{1}{\varepsilon} \rceil} \leq \frac{1}{\frac{1}{\varepsilon}} = \varepsilon$ as required.

W5b 10/4

Limit of a sequence: given a sequence $\{x_n\}$ of real numbers, we say $\{x_n\}$ converges to L for some $L \in \mathbb{R}$, if $\forall \varepsilon > 0, \exists N \in \mathbb{N}$ so that $\forall n \in \mathbb{N}$ with $n \geq N$, $|x_n - L| \leq \varepsilon$.

Claim: Show that $\lim_{n \to \infty} \dfrac{n}{n^2 + 1} = 0$.

> Let ε be arbitrary. Take $N = \lceil \frac{1}{\varepsilon} \rceil$, and let n be an arbitrary natural number greater than N. Then
>
> $\left| \frac{n}{n^2+1} - 0 \right| = \frac{n}{n^2+1} < \frac{n}{n^2} = \frac{1}{n} \leq \frac{1}{N} \leq \frac{1}{\frac{1}{\varepsilon}} = \varepsilon$.
>
> Therefore, $\lim_{n \to \infty} \dfrac{n}{n^2 + 1} = 0$.

Claim: Show that $\lim_{n \to \infty} \dfrac{n}{\sqrt{n^2 + 1}} \neq 0$.

> We first negate the definition of convergence. To show that $\{x_n\}$ does not converge to L, we need to show that $\exists \varepsilon > 0$ such that $\forall N \in \mathbb{N}$, $\exists n \in \mathbb{N}$ with $n \geq N$ such that $|x_n - L| > \varepsilon$.
>
> Take $\varepsilon = \frac{1}{2}$, and let $N \in \mathbb{N}$ be arbitrary. Now, take $n = N$. In particular, $n \geq 1$. Then
>
> $\left| \frac{n}{\sqrt{n^2+1}} - 0 \right| = \frac{n}{\sqrt{n^2+1}} = \frac{1}{\sqrt{1+\frac{1}{n^2}}} > \frac{1}{\sqrt{1+\frac{1}{1^2}}} = \sqrt{\frac{1}{2}} > \frac{1}{2} = \varepsilon$.
>
> Therefore, $\lim_{n \to \infty} \dfrac{n}{\sqrt{n^2 + 1}} \neq 0$.

W5c 10/6

Limit of a function: $\lim_{x \to a} f(x) = L$ means that $\forall \varepsilon > 0, \exists \delta > 0$ such that $\forall x \in \mathbb{R}, 0 < |x - a| < \delta \implies |f(x) - L| < \varepsilon$.

Claim: show that $\lim_{x \to 2} \frac{1}{x} = \frac{1}{2}$.

Scratch work: we want $\left|\frac{1}{x} - \frac{1}{2}\right| < \varepsilon$. We want $|2 - x| < 2x\varepsilon$. Idea: choose $\delta = \min(1, 2\varepsilon)$.

If $\delta \leq 1$, then $1 \leq x \leq 3$. Then $1 \leq x \implies 2\varepsilon \leq 2x\varepsilon$ and so $|2 - x| < \delta \leq 2\varepsilon \leq 2x\varepsilon$.

> Let $\varepsilon > 0$, and let $\delta = \min(1, 2\varepsilon)$. Let $x \in \mathbb{R}$, and suppose that $0 < |x - 2| < \delta$. Note that since $\delta \leq 1$, $|x - 2| < 1$, and so $x > 1$. Thus, $2\varepsilon < 2x\varepsilon$.
>
> We then see that $|x - 2| < \delta \leq 2\varepsilon$, since $\delta \leq 2\varepsilon$. Hence $|x - 2| < 2\varepsilon \leq 2x\varepsilon$, so that $\frac{|x-2|}{2x} < \varepsilon$, since $x > 1 > 0$.
>
> Hence, $\left|\frac{1}{x} - \frac{1}{2}\right| < \varepsilon$.

Limit Not Equal: $\exists \varepsilon > 0$ so that $\forall \delta > 0$, $\exists x \in \mathbb{R}$ so that $0 < |x - a| < \delta$ and $|f(x) - L| \geq \varepsilon$.

Claim: show that $\lim_{x \to 1} \neq 0$.

> Choose $\varepsilon = \frac{1}{2}$ and let $\delta > 0$ be arbitrary. Choose $x = 1 + \frac{\delta}{2}$, which satisfies $0 < |x - 1| < \delta$.
>
> Additionally, $x > 1$ implies that $x^2 > 1 > \frac{1}{2}$ so $|x^2 - 0| \geq \frac{1}{2}$.

W6a 10/11

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 $n \in \mathbb{N}$.

W6b 10/12

Claim: Let $F_1 = 1, F_2 = 1, F_n = F_{n-1} + F_{n-2}$ for $n > 2$. Prove that $3 \mid F_{4n}$ for all $n \in \mathbb{N}$.

> We proceed with induction.
>
> - For the base case, consider $n = 1$ in which case $F_{4n} = F_4 = F_3 + F_2 = F_2 + F_1 + F_2 = 3$. Then $F_{4n} = 3 \cdot 1$ and since $1 \in \mathbb{Z}$, $3 \mid F_{4n}$.
> - For the inductive step, let $k \in \mathbb{N}$ and assume that $3 \mid F_{4k}$. We will show that $3 \mid F_{4(k+1)}$.
>
> 1. If $F_{4k+1} \equiv 0 \pmod 3$, then $F_{4k+2} \equiv 0 + 0 \equiv 0 \pmod 3$ so $F_{4k+3} \equiv 0 + 0 \equiv 0 \pmod 3$ and $F_{4k+4} \equiv 0 + 0 \equiv 0 \pmod 3$.
> 2. If $F_{4k+1} \equiv 1 \pmod 3$, then $F_{4k+2} \equiv 1 + 0 \equiv 1 \pmod 3$ so $F_{4k+3} \equiv 1 + 1 \equiv 2 \pmod 3$ and $F_{4k+4} \equiv 2 + 1 \equiv 3 \equiv 0 \pmod 3$.
> 3. If $F_{4k+1} \equiv 2 \pmod 3$, then $F_{4k+2} \equiv 2 + 0 \equiv 2 \pmod 3$ so $F_{4k+3} \equiv 2 + 2 \equiv 4 \equiv 1 \pmod 3$ and $F_{4k+4} \equiv 1 + 2 \equiv 3 \equiv 0 \pmod 3$.

> In all cases, we have $F_{4k+4} \equiv 0 \pmod 3$, so $3 \mid F_{4k+4}$ as desired.

W7b 10/18

Exercise 1

a) Consider the set $A_a = \{(x, x^2 - ax), x \in \mathbb{R}\}$ for $a = 0, 1, 2$. Draw these sets.

b) Consider $B = \bigcap_{a \in \mathbb{R}} A_a$ Prove that $B = \{(0, 0)\}$.

> First, to show that $\{(0, 0)\} \subseteq B$, let $x = 0$, so that $(0, 0) \in A_a$ for all $a \in \mathbb{R}$.
>
> Second, to show that $B \subseteq \{(0, 0)\}$, consider A_0 and A_1.
>
> Then $A_0 = \{(x, x^2) \in \mathbb{R}\}$ and $A_1 = \{(x, x^2 - x), x \in \mathbb{R}\}$. Note that $A_0 \cap A_1 = \{(x, x^2) \mid x^2 = x^2 - x, x \in \mathbb{R}\}$.
>
> Since $x^2 = x^2 - x$ implies $x = 0$, $A_0 \cap A_1 = \{(0, 0)\}$. Thus $\bigcap_{a \in \mathbb{R}} A_a \subseteq A_0 \cap A_1 \subseteq \{(0, 0)\}$, so $B \subseteq \{(0, 0)\}$.
>
> Thus, $B = \{(0, 0)\}$.

Exercise 2

Let $\{p_1, p_2, \ldots, p_n, \ldots\}$ be the set of primes listed in increasing order. For $k \in \mathbb{N}$, let $A_k = \{a \in \mathbb{N} \mid a \geq 2, p_k \nmid a\}$.

For $n \in \mathbb{N}$, let $B_n = \bigcap_{k=1}^{n} A_k$

a) Find $\min(B_4)$

> B_4 is the set of numbers that are not divisible by $2, 3, 5, 7$. $\min(B_4) = 11$.

b) Find $\bigcap_{k=1}^{\infty} A_k$

> $\bigcap_{k=1}^{\infty} A_k = \varnothing$.

W8a 10/23

Exercise 1

Let U be a set, and $A, B, C \subseteq U$.

a) Prove that $(U - A) \subseteq B$ if and only if $A \cup B = U$.

> *Scratchwork:*
>
> $A \cup B = U$ means that $A \cup B \subseteq U$ and $U \subseteq A \cup B$.
>
> *Proof:*
>
> First, suppose $U - A \subseteq B$. So for all $x \in U - A$, $x \in B$. Hence if $x \in U$ and $x \notin A$, then $x \in B$.

- Now let $y \in U$. If $y \in A$, then $y \in A \cup B$. If $y \notin A$, then be our assumption, $y \in B$ so that $y \in A \cup B$. Hence, $U \subseteq A \cup B$
- Also, since $A \subseteq U$ and $B \subseteq U$, then $A \cup B \subseteq U$.

  Therefore $A \cup B = U$.

Second, suppose that $A \cup B = U$. Then $U \subseteq A \cup B$.

Let $x \in U$ so that $x \in A \cup B$. Then either $x \in A$ or $x \in B$.

Let $y \in U - A$, so that $y \in U$ and $y \notin A$. Since $y \in U$, we have $y \in A$ or $y \in B$. Since $y \notin A$, we have $y \in B$. Hence $(U - A) \subseteq B$.

Since we have proven both implications, we are done.

b) Prove that $(U - A) \subseteq B$ implies that $(C - B) \cup A = A$.

Suppose that $(U - A) \subseteq B$. Then by part (a), $A \cup B = U$. Now since $C \subseteq U$, we have $C \subseteq A \cup B$.

- Let $x \in (C - B) \cup A$. Then either $x \in A$ or $x \in C - B$. If $x \in C - B$, then $x \in C$ and $x \notin B$. Since $C \subseteq U$, we have $x \in A \cup B$. Furthermore, since $x \notin B$, we have $x \in A$. On the other hand, if $x \in A$, then we are done.

  So $(C - B) \cup A \subseteq A$ as needed.
- Also, clearly $A \subseteq (C - B) \cup A$.

We conclude that $(C - B) \cup A = A$.

W8b 10/25 Midterm

W8c 10/27

Exercise 1

Prove or disprove: for all sets A, B, C:

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

True.

Proof: First, we will show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

Suppose $x \in A \cap (B \cup C)$. Then $x \in A$, and either $x \in B$ or $x \in C$.

Case 1: $x \in B$. Then $x \in (A \cap B)$, so $x \in (A \cap B) \cup (A \cap C)$.

Case 2: $x \in C$. Then $x \in (A \cap C)$, so $x \in (A \cap B) \cup (A \cap C)$.

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

Suppose that $x \in (A \cap B) \cup (A \cap C)$.

Case 1: $x \in A \cap B$. Then $x \in A$. Furthermore, $x \in B$, and so $x \in (B \cup C)$. Thus, $x \in A \cap (B \cup C)$.

> Case 2: $x \in A \cap C$. Then $x \in A$. Furthermore, $x \in C$, and so $x \in (B \cup C)$. Thus, $x \in A \cap (B \cup C)$.
>
> We conclude that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

2. $A - (B - C) = (A - B) - C$

> False.
>
> *Proof:* Consider the sets $A = B = C = \{1\}$.
>
> Then $A - (B - C) = A - \varnothing = \{1\}$.
>
> On the other hand, $(A - B) - C = \varnothing - C = \varnothing$.
>
> Notice that $1 \in A - (B - C)$ but $1 \notin (A - B) - C$.
>
> Hence, $A - (B - C) \nsubseteq (A - B) - C$. so $A - (B - C) \neq (A - B) - C$

Exercise 2

Prove or disprove: $(A \subseteq B) \implies (\mathcal{P}(A) \subseteq \mathcal{P}(B))$.

> True.
>
> Assume that $A \subseteq B$. Thus, for all $x \in A$, we have $x \in B$.
>
> Let $X \in \mathcal{P}(A)$ be arbitrary. By the definition of the power set, we know that $X \subseteq A$. Thus, for any $x \in X$, we have $x \in A$.
>
> By assumption, $A \subseteq B$, and thus for any $x \in X$, we also have $x \in B$. Therefore, $X \subseteq B$.
>
> Lastly, by the definition of the power set, we know that $X \in \mathcal{P}(B)$. We conclude that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

W9a 10/30

Equivalence relation

Consider $R \subseteq A \times A$. R is an equivalence relation if:

1. **Reflexive:** all $x \in A, (x, x) \in R$.
2. **Symmetric:** all $x, y \in A$, if $(x, y) \in R$ then $(y, x) \in R$.
3. **Transitive:** all $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$.

Theorem: equivalent mod n is an equivalence relation. (Also proven in Video 27)

Exercise 1:

Determine, with proof, which of the following are equivalence relations.

a) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$

> Not an equivalence relation.
>
> *Proof:* Notice that $2 \neq 2^2$, so $(2, 2) \notin R$. Since $2 \in \mathbb{R}$, the relation is not reflexive, so it is not an equivalence relation.

b) $R = \{(1,1),(2,2),(3,3),(1,2),(2,1),(1,3),(3,1)\}$ on $\{1,2,3\}$

> Not an equivalence relation.
>
> *Proof:* Consider $x = 2, y = 1$, and $x = 3$, so that $x, y, z \in \{1,2,3\}$. Then $(2,1) \in R$ and $(1,3) \in R$ but $(2,3) \notin R$. Hence, the relation is not transitive, so it is not an equivalence relation.

c) $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid 3 \mid (a-b)\}$

> Is an equivalence relation.
>
> *Proof:*
>
> Let $a \in \mathbb{Z}$ be arbitrary. Then $a - a = 0$ and $3 \mid 0$, which means that $(a,a) \in R$ and so the relation is reflexive.
>
> Assume that $(a,b) \in R$. Then $a - b = 3k$ for some $k \in \mathbb{Z}$. Thus, $b - a = 3(-k)$, so $3 \mid (b-a)$ which means that $(b,a) \in R$ and so the relation is symmetric.
>
> Assume that $(a,b) \in R$ and $(b,c) \in R$. Then $a - b = 3k$ and $b - c = 3l$ for some $k, l \in \mathbb{Z}$. Adding gives $a - c = 3(k+l)$, so $3 \mid (a-c)$ which means that $(a,c) \in R$ and so the relation is transitive.

W9b 11/1

Exercise 1: Let A, B be sets. Prove or disprove: $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

> We claim that the statement is true.
>
> *Proof:*
>
> First, let $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Then for all $x \in X, x \in A$ and $x \in B$. Hence, $x \in A \cap B$ and so $X \subseteq A \cap B$ and $X \in \mathcal{P}(A \cap B)$. Thus, $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.
>
> Next, let $X \in \mathcal{P}(A \cap B)$. Then for all $x \in X$, $x \in A$ and $x \in B$. Thus $X \subseteq A$ and $X \subseteq B$, and so $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$. Therefore, $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Thus, $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.
>
> We conclude that $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

Exercise 2: Let $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid 3 \mid (2a - 5b)\}$. Is R reflexive, symmetric, transitive?

> *Proof:*
>
> - R is reflexive. Let $n \in \mathbb{Z}$. Then $2n - 5n = -3n = 3 \cdot (-n)$. Since $-n \in \mathbb{Z}$, $3 \mid (2n - 5n)$ and $n \; R \; n$.
> - R is symmetric. Let $a, b \in \mathbb{Z}$. Suppose that $a \; R \; b$. Then $2a - 5b = 3x$ for some $x \in \mathbb{Z}$. Adding $3a + 3b$, we have $5a - 2b = 3(x + a + b)$ and so $2b - 5a = 3(-x - a - b)$. Since $-x - a - b \in \mathbb{Z}$, we have $3 \mid (2b - 5a)$ and so $b \; R \; a$.
> - R is transitive. Let $a, b, c \in \mathbb{Z}$. Suppose that $a \; R \; c$ and $b \; R \; c$. Then $2a - 5b = 3x$ and $2b - 5c = 3y$ for some $x, y \in \mathbb{Z}$. Adding these, we have $2a - 3b - 5c = 3x + 3y$, so $2a - 5c = 3(x + y + b)$. Since $x + y + b \in \mathbb{Z}$, we have $3 \mid (2a - 5c)$ and so $b \; R \; c$.
>
> R is an equivalence relation.

W9c 11/3

Exercise 1:

Let $A = \{1, 2, 3, 4, 5, 6\}$. Let $R \subseteq A \times A$ be the relation $a \; R \; b \iff a \nmid b$.

Write out the elements of R:

> $\{(2,1), (2,3), (2,5), (3,1), (3,2), (3,4), (3,5), (4,1), (4,2), (4,3), (4,5), (4,6), (5,1), (5,2), (5,3), (5,4), (5,6), (6,1), (6,2),$

Is R reflexive, symmetric, transitive?

> Not reflexive: Consider $3 \in A$. Then $3 \mid 3$, so $(3,3) \nmid R$.
>
> Not symmetric: Consider $2, 4 \in A$. Then $2 \mid 4$ but $4 \nmid 2$ so that $(2,4) \notin R$ but $(4,2) \in R$.
>
> Not transitive: Consider $2, 3, 4 \in A$. Then $2 \mid 4$ but $2 \nmid 3$ and $3 \nmid 4$. Hence $(2,4) \in R$ and $(3,4) \in R$, but $(2,4) \notin R$.

What if we extend A to $\mathbb{Z}$?

> Same examples apply

What if we restrict A to $\{1, 3\}$?

> Not reflexive, not symmetric.
>
> It is transitive (vacuously true because there is only one element in the relation, so the assumption for transitivity which requires two elements in the relation is false)

Exercise 2:

Let A be the set of functions $f: \mathbb{R} \to \mathbb{R}$. Define R on A by $R = \{(f, g) \in A \times A \mid f - g = c, \text{ for some } c \in \mathbb{R}\}$. Is R reflexive, symmetric, transitive?

> It is reflexive: Consider $f \in A$, then $f - f = 0 \in \mathbb{R}$ so $(f, f) \in R$.
>
> It is symmetric: Consider $f, g \in A$, and assume that $(f, g) \in R$ so $f - g = c$ for some $c \in \mathbb{R}$. Then $g - f = -c$ and since $-c \in \mathbb{R}$, we have $(g, f) \in R$ as desired.
>
> It is transitive: Consider $f, g, h \in A$, and assume that $(f, g) \in R$ and $(g, h) \in R$. Thus $f - g = c$ and $g - h = d$ for some $c, d \in \mathbb{R}$. Adding gives $f - h = c + d$ and since $c + d \in R$, we have $(g, h) \in R$ as desired.

W10a 11/6

Exercise 1: Let p be prime, and let $a, b \in \mathbb{Z}$. Prove that $p \mid (a \cdot b)$ if and only if $p \mid a$ or $p \mid b$.

> Assume that $p \mid a$ or $p \mid b$. WLOG $p \mid a$. Then $a = p \cdot c$. This means that $a \cdot b = p \cdot (bc)$. Therefore, $p \mid (a \cdot b)$.

> Assume that $p \mid a \cdot b$, so that $\exists k \in \mathbb{Z}$ so that $a \cdot b = p \cdot k$. We have two cases:
>
> If $p \mid a$, then $p \mid a$ or $p \mid b$ and we are done.
>
> If $p \nmid a$, then $\gcd(a, p) = 1$ since $\gcd(a, p) = p$ would imply $p \mid a$. By Bézout's lemma, $\exists x, y \in \mathbb{Z}$ so that $ax + py = 1$. Multiplying by b, we have $abx + pby = b$. Since $ab = pk$, we have $pkx + pby = p(kx + by) = b$. Since $kx + by \in \mathbb{Z}$, we have $p \mid b$ and so $p \mid a$ or $p \mid b$ and we are done.

Exercise 2: A relation R on $\mathbb{Z}$ is defined by $a \; R \; b$ if $7a^2 \equiv 2b^2 \pmod 5$.

a) Prove R is an equivalence relation.

> Let $a \in \mathbb{Z}$. Notice that $7 \equiv 2 \pmod 5$ so $7a^2 \equiv 2a^2 \pmod 5$, so $a \ R \ a$ and R is reflexive.
>
> Suppose that $7a^2 \equiv 2b^2 \pmod 5$ which means that $2a^2 \equiv 2b^2 \pmod 5$. Then $2b^2 \equiv 2a^2 \pmod 5$ and so $2b^2 \equiv 7a^2 \pmod 5$. Thus $b \ R \ a$ and R is symmetric.
>
> Suppose that $a \ R \ b$ and $b \ R \ c$. Then $7a^2 \equiv 2b^2 \pmod 5$ and $7b^2 \equiv 2c^2 \pmod 5$. Thus $7a^2 \equiv 2b^2 \equiv 7b^2 \equiv 2c^2 \pmod 5$. Hence, $a \ R \ c$ and R is transitive.

b) Write $[0]$ and $[1]$ as simply as possible.

> $[0] = \{n \in \mathbb{Z} \mid n \equiv 0 \pmod 5\}$
>
> $[1] = \{n \in \mathbb{Z} \mid n \equiv 1 \pmod 5 \text{ or } n \equiv 4 \pmod 5\}$

W12a 11/20

Consider $f\colon A \to B$.

- Injective: if $f(a_1) = f(a_2)$ then $a_1 = a_2$
- Surjective: for all $b \in B$, there exists $a \in A$ such that $f(a) = B$

Note: f is injective and surjective (i.e. bijective) if and only if f has an inverse function

Exercise 1

Let $f\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be given by $f(n) = (2n+1, n+2)$.

a) is f injective?

> Yes. Assume that $n_1, n_2 \in \mathbb{Z}$, and suppose $f(n_1) = f(n_2)$. Then $(2n_1+1, n_1+2) = (2n_2+1, n_2+2)$. In particular, $2n_1 + 1 = 2n_2 + 1$ implies that $n_1 = n_2$. Likewise, $n_1 + 2 = n_2 + 2$ also implies that $n_1 = n_2$.

b) is f surjective?

> No. Consider $(0,0) \in \mathbb{Z} \times \mathbb{Z}$. Then for all $n \in \mathbb{Z}$, $f(n) = (2n+1, n+2) \neq (0,0)$ since $2n+1$ is odd and 0 is even.

Exercise 2

Let $f\colon \mathbb{R} \setminus \{2/5\} \to \mathbb{R} \setminus \{-3/5\}$ be given by $f(x) = \frac{3x}{2-5x}$. Prove that f is bijective.

> First, we prove that f is injective.
>
> Let $x_1, x_2 \in \mathbb{R} \setminus \{2/5\}$, and assume that $f(x_1) = f(x_2)$. Then $\frac{3x_1}{2-5x_1} = \frac{3x_2}{2-5x_2}$. Since $x_1 \neq \frac{2}{5}$ and $x_2 \neq \frac{2}{5}$, we may cross multiply to obtain $6x_1 - 15x_1x_2 = 6x_2 - 15x_1x_2$, which implies that $6x_1 = 6x_2$ and so $x_1 = x_2$. Therefore, f is injective.
>
> Let $y \in R \setminus \{-3/5\}$, and take $x = \frac{2y}{5y+3}$, which is defined because $y \neq -\frac{3}{5}$. Then $f(x) = \dfrac{3 \cdot \frac{2y}{5y+3}}{2 - 5 \cdot \frac{2y}{5y+3}} = \dfrac{6y}{2(5y+3) - 10y} = \dfrac{6y}{6} = y$. Therefore, f is surjective.
>
> Since f is both injective and surjective, we conclude that f is bijective.

W12b 11/22

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

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

f^{-1} refers to the preimage. Usually, f^{-1} is not a function (when it is a function, it is the inverse function).

Technically speaking, the preimage is applied on sets and produces sets.

Exercise 1

Let $f: A \to B$. Prove that $X = f^{-1}(f(X))$ for all $X \subseteq A$ if and only if f is injective.

> First, suppose that $X = f^{-1}(f(X))$ for all $X \subseteq A$. Let $a_1, a_2 \in A$ and suppose $f(a_1) = f(a_2)$. Then $\{a_1\} = f^{-1}(f(\{a_1\}))$ and $\{a_2\} = f^{-1}(f(\{a_2\}))$. Since $f(\{a_1\}) = f(\{a_2\})$, we know that $f^{-1}(f(\{a_1\})) = f^{-1}(f(\{a_2\}))$, and so $a_1 = a_2$.
>
> Second, suppose f is injective. Let $X \subseteq A$.
>
> 1. We will show that $X \subseteq f^{-1}(f(X))$. Let $x \in X$. Then $f(x) \in f(X)$. Hence $x \in f^{-1}(f(X))$.
> 2. We will show that $f^{-1}(f(X)) \subseteq X$. Let $x \in f^{-1}(f(X))$. Then $f(x) \in f(X)$. So there exists $\bar{x} \in X$ with $f(\bar{x}) = f(x)$. Since f is injective, $\bar{x} = x$, so $x \in X$.

Exercise 2

Consider for $a, b, c, d \in \mathbb{R}$ the matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Let $f: \{2 \times 2 \text{ matrices}\} \to \{2 \times 2 \text{ matrices}\}$ given by $f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

a) Find $f \circ f$.

> $f \circ f = \text{identity}$.

b) Is f invertible? If so, what is f^{-1}?

W12c

Theorems

1. If $g \circ f$ is an injection then f is an injection
2. If $g \circ f$ is a surjection then g is a surjection
3. If f, g are bijective, so is $f \circ g$
4. If f is bijective then f^{-1} is a bijective function

Exercise 1

Let E, F, G be non-empty sets. Let $f: E \to F, g: F \to G, h: G \to E$ be functions. Prove that if $g \circ f$ and $h \circ g$ are bijective, then so are f, g, h.

> *Proof:* By (1), g is injective since $h \circ g$ is injective. By (2), g is surjective since $g \circ f$ is surjective. Then g is bijective and has a bijective inverse g^{-1}.

> Then $g^{-1} \circ g \circ f = f$ is bijective (composition of two bijective functions). Also, $h \circ g \circ g^{-1} = h$ is bijective.

Proof by Contradiction

1. Proofs that a number is irrational

Exercise 1

Prove that if $x^2 = 2$, then $x \notin \mathbb{Q}$. Correct approach is a proof by contradiction.

> *Proof:* Suppose $x \in \mathbb{Q}$ and $x^2 = 2$. Then $x = \frac{m}{n}$ for $m, n \in \mathbb{Z}$ and $\gcd(m, n) = 1$. Hence $\left(\frac{m}{n}\right)^2 = \frac{m^2}{n^2} = 2$ and so $m^2 = 2n^2$. Then $2 \mid m^2$ and so $2 \mid m$. Hence $4 \mid m^2$, so $4 \mid 2n^2$, then $2 \mid n^2$ and so $2 \mid n$. Hence $\gcd(m, n) \geq 2$ which contradicts $\gcd(m, n) = 1$. Thus either $x \neq \mathbb{Q}$ or $x^2 \neq 2$.

W13a

Exercise 1

Let $x \in \mathbb{R}$ and suppose that $x^7 + 5x^2 - 3 = 0$. Prove that x is irrational.

> *Proof:* Suppose for contradiction that $x \in \mathbb{Q}$ and $x^7 + 5x - 3 = 0$. Then there exists $a, b \in \mathbb{Z}$ so that $x = \frac{a}{b}$ and $\gcd(a, b) = 1$.
>
> Then $(\frac{a}{b})^7 + 5(\frac{a}{b})^2 - 3 = 0$ and $a^7 + 5a^2b^5 - 3b^7 = 0$. Reducing $\mod b$, we have $a^7 \equiv 0 \pmod b$, so $b \mid a^7$. We consider two cases:
>
> If $b \neq 1$, then there exists a prime $p \mid b$. Then $p \mid a^7$ so $p \mid a$, so $\gcd(a, b) \geq p$ which contradicts $\gcd(a, b) = 1$.
>
> If $b = 1$ or $b = -1$, then $\frac{a}{b} \in \mathbb{Z}$. Reducing $\mod x$, we have $3 \equiv 0 \pmod x$, so $x = \pm 1, \pm 3$.
>
> Check cases

Rational Root Theorem

W13b

Exercise 1: Let $n \in \mathbb{N}, n \geq 2$, and $a, b, c \geq \mathbb{Z}$. Prove that if $ab \equiv 1 \pmod n$, then $\forall c \not\equiv 0 \pmod n$, we have $ac \not\equiv 0 \pmod n$.

> *Proof:* Let $c \in \mathbb{Z}$, and suppose $ac \equiv 0 \pmod n$. Then $a \cdot b \cdot c \equiv 1 \cdot c \equiv 0$, so that $1 \cdot c \equiv 0 \pmod n$. Then $c \equiv 0 \pmod n$, which proves the contrapositive.

Exercise 2: Let $(x_n), n \in \mathbb{N}$ be a sequence of real numbers. Prove that if $\lim x_n = L_1$ and $\lim x_n = L_2$ then $L_1 = L_2$.

Definition: $\lim x_n = L$ means $\forall \varepsilon > 0, \exists N \in \mathbb{N}, \text{ s.t. } \forall n \geq N, |x_n - L| < \varepsilon$.

> *Proof:* Suppose that $\lim x_n = L_1$ and $\lim x_n = L_2$, but $L_1 \neq L_2$. Then consider $\varepsilon = \frac{|L_1 - L_2|}{2}$. Note that $\varepsilon > 0$ as needed. Now observe that since $\lim x_n = L_1$, we know that there exists $N_1 \in \mathbb{N}$ so that for all $n > N_1$, we have $|x_n - L_1| < \frac{|L_1 - L_2|}{2}$.

W14c

Exercise: Let $\mathbb{Z}(\sqrt{2}) = \{x \in \mathbb{R} \mid x = a + b\sqrt{2}, \text{ for } a, b \in \mathbb{Z}\}$.

a) Prove that $\mathbb{Z}(\sqrt{2}) \cap \mathbb{Q} = \mathbb{Z}$.

> *Proof:* Let $x \in \mathbb{Z}(\sqrt{2}) \cap \mathbb{Q}$. Then $\exists a, b \in \mathbb{Z}$ so that $x = a + b\sqrt{2}$, and $\exists p, q \in \mathbb{Z}, q \neq 0$, so that $x = \frac{p}{q}$. Then $\frac{p}{q} = a + b\sqrt{2}$, so either $\sqrt{2} = \frac{p - aq}{bq}$, or $b = 0$.
>
> Since $\sqrt{2}$ is irrational, we must have $b = 0$, which implies that $x = a \in \mathbb{Z}$.
>
> Now, let $n \in \mathbb{Z}$. Then $n = \frac{n}{1} \in \mathbb{Q}$. Also, $n = n + 0\sqrt{2}$ so $n \in \mathbb{Z}(\sqrt{2})$.

b) Prove that $\forall x \in \mathbb{Z}(\sqrt{2})$ and $n \in \mathbb{N}, x^n \in \mathbb{Z}(\sqrt{2})$.

> *Proof:* Let $x = a + b\sqrt{2}$. We claim that $x^n \in \mathbb{Z}(\sqrt{2})$ for all $n \in \mathbb{N}$. We proceed with induction.
>
> Base case: $x^1 = (a + b\sqrt{2})^1 = x \in \mathbb{Z}(\sqrt{2})$.
>
> Inductive step: for some $k \in \mathbb{Z}$ assume that $x^k \in \mathbb{Z}(\sqrt{2})$. We want to show that $x^{k+1} \in \mathbb{Z}(\sqrt{2})$. By assumption, we may write $x^k = c + d\sqrt{2}$ for $c, d \in \mathbb{Z}$. Then
>
> $$\begin{aligned} x^{k+1} &= x^k \cdot x \\ &= (c + d\sqrt{2})(a + b\sqrt{2}) \\ &= (ac + 2bd) + (ad + bc)\sqrt{2} \end{aligned}$$
>
> so $x^{k+1} \in \mathbb{Z}(\sqrt{2})$ because $ac + 2bd \in \mathbb{Z}$ and $ad + bc \in \mathbb{Z}$.
>
> By induction, $x^n \in \mathbb{Z}(\sqrt{2})$ for all $n \in \mathbb{N}$.

c) Prove $\mathbb{Z}(\sqrt{2})$ is denumerable.

> We need to show $|\mathbb{Z}(\sqrt{2})| = |\mathbb{N}|$, we will show that $|\mathbb{Z}(\sqrt{2})| = |\mathbb{Z} \times \mathbb{Z}|$ and we already know that $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$.
>
> Consider $f: \mathbb{Z}(\sqrt{2}) \to \mathbb{Z} \times \mathbb{Z}$ given by $f(a + b\sqrt{2}) = (a, b)$ and $g: \mathbb{Z}(\sqrt{2}) \to \mathbb{Z}(\sqrt{2})$ given by $g(a, b) = a + b\sqrt{2}$.
>
> To see that f is a function, suppose $a + b\sqrt{2} = c + d\sqrt{2}$ for some $a, b, c, d \in \mathbb{Z}$. Then $\sqrt{2} = \frac{a - c}{d - b}$ or $d - b = 0$. Since $\sqrt{2}$ is irrational, $d - b = 0$, so $d = b$ and hence $a = c$.
>
> Note that g is clearly a function.
>
> Finally, we compute $f \circ g(a, b) = f(a + b\sqrt{2}) = (a, b)$, and $g \circ f(a, b) = g(a, b) = a + b\sqrt{2}$. Thus $g \circ f = i_{\mathbb{Z}(\sqrt{2})}$ and $f \circ g = i_{\mathbb{Z} \times \mathbb{Z}}$. Hence, f and g are inverses, so f is a bijection and $|\mathbb{Z}(\sqrt{2})| = |\mathbb{Z} \times \mathbb{Z}$.